DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION PARA EL AREA TI DE LA ESE HOSPITAL UNIVERSITARIO ERASMO MEOZ DE CÚCUTA BASADO EN LA NORMA ISO27001:2013

CHERLY LILIANA LEAL SANDOVAL
JAVIER RICARDO TARAZONA ANTELIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN DE SEGURIDAD INFORMATICA
FEBRERO DE 2018

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL AREA TI PARA LA ESE HOSPITAL UNIVERSITARIO ERASMO MEOZ DE CÚCUTA BASADO EN LA NORMA ISO27001:2013

CHERLY LILIANA LEAL SANDOVAL
JAVIER RICARDO TARAZONA ANTELIZ

PROYECTO PARA OPTAR A TITULO
ESPECIALISTA SEGURIDAD INFORMÁTICA

DIRECTOR DE PROYECTO
ING. FRANCISCO JAVIER HILARION NOVOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN DE SEGURIDAD INFORMATICA
FEBRERO DE 2018

Nota de aceptación

_____

_____

_____

_____

_____

_____
Firma de Jurado

Cúcuta, 26 de febrero de 2018

DEDICATORIA

Dedico este proyecto inicialmente a Dios, que nos da su aliento para seguir adelante y salud para poder desarrollar cada actividad que emprendemos.

A mis padres que son un ejemplo de honestidad, amor a su familia, lucha diaria en donde a pesar de los problemas y limitaciones demuestran que se puede avanzar para cumplir las metas que nos trazamos.

A mi esposo e hijos, por su apoyo incondicional y fortaleza, por todo el tiempo que me regalaron para estudiar y sacar adelante este fabuloso proyecto; ellos son mi inspiración para escalar y ser cada día mejor. Los amo con todas mis fuerzas.

Cherly Liliana

DEDICATORIA

Dedico este trabajo a Dios que es quien nos regala la vida y la fuerza para seguir adelante siempre.

A mis padres quienes con su incansable cariño y enseñanzas me han inculcado el deseo por superarme día a día y han sido claves para poder construir y forjar la persona ahora soy.

A mi hermano Julián Orlando quien siempre ha estado pendiente de mis pasos, cumpliendo a cabalidad su labor de hermano mayor con su gran ejemplo y consejo amoroso.

A mi sobrino amado Julian David quien es el motorsito que me impulsa a seguir adelante todos los días en la búsqueda de ser cada día una persona con una mayor calidad humana.

Javier Ricardo

AGRADECIMIENTOS

Este proyecto es resultado de nuestro esfuerzo y apoyo que hemos recibido de personas muy especiales, como la Ing. Tatiana Cáceres, Asesora de Planeación y Calidad de la ESE HUEM, el Dr. Juan Agustín Ramírez Montoya, Gerente de la ESE HUEM y el Ing. Lucas Liendo, Coordinador de la Oficina de TIC en la ESE HUEM, quienes gracias a su gestión han mejorado considerablemente las condiciones físicas, financieras, humanas y de infraestructura en el hospital, logrando que proyectos de este tipo le interesen a la administración y logren implementarse pasando de la teoría a la práctica.

De igual manera, agradecemos a nuestro Director de proyecto en la UNAD, Ing. Francisco Hilarion, quien acertadamente nos ha colaborado para enriquecer este trabajo y entregar un producto de calidad a la institución.

Agradecemos a todos nuestros tutores y compañeros en la UNAD y de la oficina TIC de la ESE HUEM, amigos y familiares que nos han apoyado y no dudaron que cumpliríamos este reto de la mejor manera.

CONTENIDO

Pág.

INTRODUCCION 13

1. EL PROBLEMA 14
1.1 DESCRIPCION DEL PROBLEMA 14

2. JUSTIFICACION 15

3. OBJETIVOS 16
3.1 OBJETIVO GENERAL 16
3.2 OBJETIVOS ESPECIFICOS 16

4. ALCANCE Y DELIMITACIÓN 17

5. MARCO REFERENCIAL 18
5.1 MARCO TEORICO 18
5.1.1 ISO 27001:2013 18
5.1.2 Fases ciclo PHVA. 23
5.1.3 ISO 27002. 24
5.1.4 ISO 27003. 25
5.1.5 Política general de seguridad y privacidad de la información. 26
5.1.6 Metodología de análisis de riesgos 27
5.2 MARCO CONTEXTUAL 30
5.2.1 Acerca de la empresa. 30
5.2.2 Plataforma estratégica. 30
5.2.3 Organigrama institucional. 31
5.2.4 Mapa de procesos. 32
5.3 MARCO DE ANTECEDENTES 32
5.4 MARCO CONCEPTUAL 33
5.5 MARCO LEGAL 35

6. DISEÑO METODOLOGICO 40

6.1 METODOLOGIA DE LA INVESTIGACION 40
6.2 METODOLOGIA DE DESARROLLO 40

7. ESTADO ACTUAL DE LA SEGURIDAD 42

8. IDENTIFICACION DE ACTIVOS 57
8.1 ACTIVOS DATOS / INFORMACION 57
8.2 SERVICIOS 57
8.3 ACTIVOS DE SOFTWARE – APLICACIONES INFORMATICAS 57
8.4 ACTIVOS DE HARDWARE 59
8.5 ACTIVOS DE REDES Y COMUNICACIONES 60
8.6 EQUIPAMIENTO AUXILIAR 60
8.7 INSTALACIONES 60
8.8 ACTIVOS DE PERSONAL 61

9. INVENTARIO DE ACTIVOS DE LA ENTIDAD 62

10. DIMENSIONES DE VALORACIÓN 78
10.1 DISPONIBILIDAD [D] 78
10.2 INTEGRIDAD [I] 78
10.3 CONFIDENCIALIDAD [C] 78
10.4 AUTENTICIDAD [A] 78
10.5 TRAZABILIDAD [T] 78

11. VALORACION DE ACTIVOS 80

12. AMENAZAS 85
12.1 DESASTRES NATURALES [N] 85
12.2 DE ORIGEN INDUSTRIAL [I] 85
12.3 ERRORES Y FALLO NO INTENCIONADOS [E] 86
12.4 ATAQUES INTENCIONADOS 87

13. IDENTIFICACION DE AMENAZAS Y VALORACION DE RIESGOS 89
13.1 ANALISIS 91

14. SISTEMA DE CONTROL INTERNO SEGÚN ISO 27001 93
14.1 DECLARACION DE APLICABILIDAD - SoA 94

15. MANUAL DE POLÍTICAS 130

16. PLAN DE CONTINUIDAD DEL NEGOCIO 140

16.1 FASE I. ANALISIS DEL NEGOCIO Y EVALUACION DE RIESGOS 140
16.2 FASE II– SELECCIÓN DE ESTRATEGIAS 143
16.3 FASE III- DESARROLLO DEL PLAN 144
16.4 FASE IV- PRUEBAS Y MANTENIMIENTO 147

17. DIVULGACIÓN 148

18. RECOMENDACIONES 149

19. CONCLUSIONES 150

20. BIBLIOGRAFIA 151

LISTADO DE FIGURAS

Pág.

Figura 1. Ciclo PHVA 23

Figura 2. Organigrama ESE HUEM..... 31

Figura 3. Mapa de Procesos ESE HUEM..... 32

LISTADO DE TABLAS

Pág.

Tabla 1. Escala de Valoración de Controles 42

Tabla 2. Lista de chequeo cumplimiento estándar ISO 270011:2013 43

Tabla 3. Evaluación de Efectividad de controles Actual 55

Tabla 4. Inventario activos del Hospital Universitario Erasmo Meoz 62

Tabla 5. Valoración activos 79

Tabla 6. Valoración de activos - Estimación del impacto 80

Tabla 7. Valoración de la frecuencia de las amenazas 89

Tabla 8. Valoración del impacto 89

Tabla 9. Valoración del riesgo potencial y residual 90

Tabla 10. Análisis de Riesgo 91

Tabla 11. Declaración de aplicabilidad SoA 95

Tabla 12. Procesos de la entidad 140

ANEXOS

Pág.

Anexo A Carta de aval de la entidad 153

Anexo B Matriz Análisis de Riesgos 154

Anexo C Resumen Analítico Especializado – RAE 417

INTRODUCCION

En los inicios de la seguridad, ésta se orientaba principalmente a la protección de propiedades físicas, almacenes, bodegas, productos, ya que era el mayor activo de las organizaciones. Sin embargo, hoy por hoy, la mayoría de actividades realizadas tanto a nivel empresarial como personal están envueltas en redes de datos administradas por sistemas de información computarizados que requieren un funcionamiento correcto garantizando su seguridad. En la actualidad, las organizaciones han tomado conciencia que el mayor activo de las mismas es la INFORMACIÓN, por ello, están tomando las precauciones necesarias para evitar fugas de datos o funcionamientos inadecuados en ellos.

Debido a la preocupación de contar con sistemas seguros, surge la Seguridad informática como medidas (estándares, normas, protocolos) tendientes a controlar e impedir el desarrollo de actividades no autorizadas sobre los activos de los sistemas de información (hardware – software – firmware – información), cumpliendo normas organizacionales o legales, que impidan el daño en los datos o acceso no autorizado, dejando al descubierto información confidencial, disminuyendo autenticidad o integridad u ocasionando el bloqueo a usuarios o equipos y/o disminución en el rendimiento en los mismos.

Múltiples factores influyen en un sistema de seguridad informática, entre los que se mencionan: Apoyo del personal responsable de la dirección de la empresa, conocimiento del área de sistemas sobre tecnología, amenazas y riesgos, sentido de pertenencia de los usuarios, correcta administración de los equipos informáticos, establecimiento de políticas para limitar el acceso y establecer privilegios, soporte de los fabricantes de hardware y software, mapa de riesgos, políticas y procedimientos acordes a la realidad institucional.

De esta manera la seguridad informática debe ser visualizada como un proceso más no como un bien o producto, de tal manera que aplicando las recomendaciones del estándar ISO 27001:2013, el cual es una norma internacional que describe cómo gestionar la seguridad de la información en una empresa, garantizamos tener un sistema de gestión de calidad óptimo disminuyendo riesgos detectados.

1. EL PROBLEMA

1.1 DESCRIPCION DEL PROBLEMA

La seguridad de las Tecnologías de la Información, en adelante TI, es fundamental para las organizaciones, a medida que la computación en la nube y los dispositivos móviles han cambiado la forma en que hacemos negocios. Con las enormes cantidades de datos que se transmiten y almacenan en redes en todo el mundo, es esencial tener implementado prácticas de seguridad efectivas.

La ESE Hospital Universitario Erasmo Meoz, como entidad pública prestadora de servicios de salud, custodia información privada de pacientes, almacenada en diferentes medios físicos y digitales; de sus procesos de atención en salud y de apoyo, procesa gran cantidad de datos que son susceptibles de control por entidades externas y al mismo tiempo son insumo para la toma de decisiones gerenciales.

En la ejecución de sus actividades diarias está expuesta a diferentes amenazas que ocasionan lentitud en algunas labores como la consecución de historias clínicas y generación de informes, inexactitud en reportes presentados, fallas en el registro de documentos, incumplimiento de normas, filtrado de información, uso inadecuado de los recursos informáticos, entre otros, problemas que al persistir, exponen a la entidad a ser blanco de multas por el no cumplimiento de la normatividad legal, perdiendo credibilidad, acabando con la buena posición que tiene en el mercado y con la confianza que sus usuarios han depositado en ella, causando daños irreparables en el funcionamiento e imagen del hospital.

Como alternativa de solución, se plantea la necesidad de diseñar un Sistema de Gestión de Seguridad Informática – SGSI, generando el siguiente interrogante:

¿Qué debe hacer la ESE Hospital Universitario Erasmo Meoz para asegurar que su información sea confidencial, íntegra y se encuentre disponible?

2. JUSTIFICACION

Son muchas las formas por las que nuestra información puede verse comprometida, resultando como necesidad la de evaluar esos riesgos, aplicar los controles necesarios y establecer planes que aseguren la custodia de la información de la entidad, así como la preservación de los activos y la continuidad del negocio.

La ESE HUEM maneja mucha información, entre la que se destaca información clínica de pacientes, datos epidemiológicos, información contractual, de proveedores, de servicios prestados, de inventarios, financiera: presupuestal, contable, pagos, tesorería, nómina.

Para garantizar la custodia y contar con información confidencial, íntegra y disponible, se debe contar con un SGSI, que permita analizar y ordenar la estructura de los sistemas de información, esto conlleva a una serie de ventajas como la mejora de imagen y relaciones con los usuarios, mejora en el control de los funcionarios, mejora en el registro de incidencias y debilidades, y mejora en la gestión de continuidad del negocio.

Al realizar la propuesta del SGSI teniendo como marco la norma ISO 27001:2013, tendremos ventajas como:

1. Cumplir con los requerimientos legales: Desde la norma nacional, así como los requerimientos contractuales de nuestros clientes (Aseguradoras en salud) relacionadas con la seguridad de la información, implementando ISO 27001 proporciona una metodología adecuada para cumplir con ellos.
2. Obtener una ventaja comercial: dado que aseguraremos la información de manera adecuada generando confianza en nuestros clientes tanto empresas como usuarios, pacientes, contratistas.
3. Disminución de costos: Un incidente de seguridad siempre genera costos, al evitarlos y propender por su disminución, la entidad obtendrá un ahorro en dinero y tiempo y maximizará el rendimiento de los funcionarios.
4. Mejora en la organización, ya que los empleados tendrán claro los procedimientos establecidos, definiendo que hacer, cuándo y quién debe hacerlo.
5. Reducción de riesgos que se produzcan pérdidas de información
6. Implantación de medidas de seguridad para que los usuarios puedan acceder a la información de manera segura, disponible, autentica y con niveles de confidencialidad que correspondan a su necesidad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información para el área TIC de la ESE Hospital Universitario Erasmo Meoz de Cúcuta basado en la norma IS0 27001:2013.

3.2 OBJETIVOS ESPECIFICOS

- Recolectar información que sirva de insumo para realizar la evaluación de riesgos.
-
- Realizar el análisis de riesgos para la ESE Hospital Universitario Erasmo Meoz usando la metodología MAGERIT.
-
- Identificar los controles para mitigar los riesgos en la gestión de seguridad de la información para la empresa ESE Hospital Universitario Erasmo Meoz basados en la ISO 27001:2013 mediante una declaración de aplicabilidad.
-
- Diseñar las políticas de seguridad de la información tomando como base la ISO 27001:2013.

4. ALCANCE Y DELIMITACIÓN

El proyecto desarrollará una propuesta de solución para la implementación de un SGSI bajo la norma ISO 27001:2013 en su fase de planear y que corresponde las siguientes actividades:

- Definir el alcance del SGSI
- Definir la política de seguridad
- Metodología para la evaluación de riesgos
- Inventario de Activos
- Identificar amenazas y vulnerabilidades
- Identificar el impacto
- Análisis y evaluación de riesgos
- Selección de Controles y SOA

Se ejecutará en el área de TICS de la ESE Hospital Universitario Erasmo Meoz en la ciudad de Cúcuta teniendo en cuenta activos informáticos tales como Información, Software, Recurso Humano, hardware e infraestructura; la implementación de la propuesta de solución del SGSI estará a cargo de la entidad.

5. MARCO REFERENCIAL

5.1 MARCO TEORICO

Para el éxito de un SGSI es necesario contar con el apoyo de la Gerencia y las directivas de la entidad. Para su diseño se debe tener en cuenta el alcance y los objetivos que se pretenden, incluirá el diseño de la política de seguridad de la empresa, realización de un inventario de los activos de la información a custodiar y un análisis de riesgos de cada tipo de estos activos. Así, se podrá detectar las amenazas, vulnerabilidades e impacto de una intrusión en la información de la empresa, gestionando el riesgo permitiendo seleccionar los controles necesarios para minimizar su ocurrencia.

5.1.1 ISO 27001:2013. Para poder gestionar todo esto, se cuenta con una serie de estándares internacionales que funcionan como modelo para realizar una propuesta de solución acorde a las necesidades detectadas, en este caso, se eligió la ISO/IEC 27001:2013, en su versión más reciente, toda vez que da directrices para gestionar la seguridad de la información en una empresa, ofrece un valor añadido a las organizaciones, pues permite hacer mejor las cosas, de una forma más económica y rápida, también permite optimizar las áreas relacionadas con la información que más le importa a la alta dirección, además que también permite anticiparse para no dejar que se produzcan incidentes contra su información por no tener el suficiente control.

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su Confidencialidad – Integridad – Disponibilidad (CID):

- *Confidencialidad*: Corresponde a aquella característica en la que se garantiza el acceso a la información solo por aquellos individuos o procesos autorizados, de tal manera que no sea conocida por aquellos no autorizados.
- *Integridad*: Cualidad de la información que garantiza que no ha sido modificada y es exacta por lo tanto completa, válida y consistente.
- *Disponibilidad*: Hace referencia al acceso y uso de la información en el instante en que los usuarios o procesos lo requieran.

Según el Portal ISO 2700 en español: “Con base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.”[1]

[1]Portal ISO 27000 en español. [En línea] http://www.iso27000.es/sgsi.html

Garantizar un nivel de protección total, es un tanto ambicioso y utópico, aun cuando se cuente con una inversión ilimitada; por ello, el objetivo de un Sistema de Gestión de Seguridad de la Información es tender a que los riesgos a los que está expuesta la información sean conocidos, estableciendo procedimientos y políticas adecuadas para implementar controles de seguridad, revisando periódicamente el impacto de éstos para medir su eficacia y de ser necesario hacer ajustes en los mismos.

En las empresas generalmente se cuenta con el hardware y software requerido, pero se usa de una forma no segura, por ello, al implementar ISO27001 se deben determinar reglas organizacionales (políticas, procedimientos) para prevenir violaciones de seguridad en donde se involucra la gestión de procesos, recursos humanos, protección física, jurídica entre otras.

La norma ISO 27001:2013 es un documento que se divide en once partes, de las cuales de la sección 4 a la 10 son obligatorias implementarlas si se desea contar con la certificación.

- Introducción: Aporta orientaciones sobre su uso y su compatibilidad con otros estándares
- Objeto y campo de aplicación: En esta parte explica el objetivo y campo de aplicación de la norma.
- Referencia normativa: Se hacen relaciones a otras normas aplicables.
- Términos y definiciones.
- Contexto de la organización: En este capítulo la organización debe determinar los requisitos que son relevantes de acuerdo a su propósito y que afecten para lograr el resultado esperado en la gestión de seguridad de la información. Comprende las necesidades y expectativas de las partes interesadas. Determina el alcance del sistema de gestión de seguridad de la información. Sistema de gestión de seguridad de la información, de acuerdo a los requerimientos de la norma la organización establece, implementa y mantiene el SGSI.
- Liderazgo: demostración y establecimiento del compromiso de la dirección en apoyo al SGSI, estipula políticas, asigna roles y responsabilidades para el desarrollo del mismo.
- Planificación: establece un plan con las actividades para evaluar los riesgos, analizando su impacto y definir si se deben prevenir, reducir o asumir sus efectos.
- Soporte: La organización determina y asegura los recursos necesarios para establecer, implementar y mantener el SGSI.
- Operación: La organización aplica e implementa las modificaciones a procesos para cumplir con los requisitos de seguridad de la información y las acciones determinadas.
- Evaluación de desempeño: La organización monitorea y evalúa el desarrollo del plan del SGSI.

- Mejora: Al encontrar resultados no esperados, se deberán realizar los ajustes necesarios para cumplir con los requisitos de la organización.

Anexo A, proporciona un catálogo de 114 controles de seguridad distribuidos en 14 dominios. Dentro de los 14 dominios encontramos:

A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN. Objetivo: Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes

A.6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.
A.6.1 Organización interna. Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.
A.6.2 Dispositivos para movilidad y teletrabajo. Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

A.7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
A.7.1 Antes de la contratación. Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran
A.7.2 Durante la ejecución del empleo. Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.3 Cese o cambio de puesto de trabajo. Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

A.8. GESTIÓN DE ACTIVOS.
A.8.1 Responsabilidad sobre los activos. Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.
A.8.2 Clasificación de la información. Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.
A.8.3 Manejo de los soportes de almacenamiento. Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

A.9. CONTROL DE ACCESO.
A.9.1 Requisitos del negocio para el control de acceso. Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.2 Gestión del acceso de usuarios. Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.
A.9.3 Responsabilidades del usuario. Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.

A.9.4 Control de acceso a sistemas y aplicaciones. Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.

A.10. CRIPTOGRAFÍA.
A.10.1 Controles criptográficos. Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.

A.11. SEGURIDAD FISICA Y AMBIENTAL.
A.11.1 Áreas seguras. Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
A.11.2 Seguridad de los equipos. Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

A.12. SEGURIDAD EN LAS OPERACIONES.
A.12.1. Procedimientos operacionales y responsabilidades. Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.2. Protección contra códigos maliciosos Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos
A.12.3. Copias de Respaldo. Objetivo. Proteger contra la pérdida de datos
A.12.4. Registro y Seguimiento. Objetivo. Registrar eventos y generar evidencia
A.12.5. Control de Software Operacional. Objetivo. Asegurarse de la integridad de los sistemas operacionales.
A.12.6. Gestión de vulnerabilidad técnica. Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnica
A.12.7. Consideraciones sobre auditorías de sistemas de información. Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos

A.13. SEGURIDAD EN LAS TELECOMUNICACIONES.
A.13.1. Gestión de Seguridad de Redes. Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.13.2. Transferencia de información. Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

A.14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SITEMAS DE INFORMACIÓN.
A.14.1. Requisitos de seguridad de los sistemas de información. Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.

A.14.2. Seguridad en los procesos de desarrollo y de soporte. Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información
A.14.3. Datos de ensayo. Objetivo. Asegurar la protección delos datos usados para ensayos

A.15. RELACIONES CON LOS PROVEEDORES.
A.15.1. Seguridad de la información en las relaciones con los proveedores. Objetivo. Asegurar la protección delos activos de la organización quesean accesibles a los proveedores
A.15.2. Gestión de la prestación de servicios de proveedores. Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores

A.16. GESTIÓN DE INCIDENTES.
A.16.1. Gestión de incidentes y mejoras en la seguridad de la información. Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad

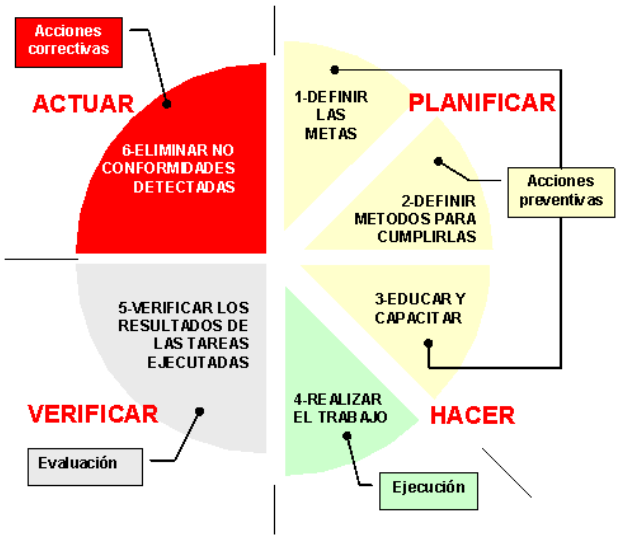
A.17. ASPECTOS DE LA SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.
A.17.1. Continuidad de seguridad dela información. Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización
A.17.2. Redundancia. Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información

A.18. CUMPLIMIENTO.
A.18.1. Cumplimiento de requisitos legales y contractuales. Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.
A.18.2. Revisiones de seguridad de la información. Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales

Esta norma por corresponder a los estándares ISO, se basa en los cuatro pasos del ciclo de Deming: Planear, Hacer, Verificar y Actuar.

5.1.2 Fases ciclo PHVA. La utilización continua del ciclo PHVA (Planear – Hacer – Verificar – Actuar) brinda una solución que permite mantener un ciclo de mejoramiento continuo en las organizaciones, utilizado ampliamente por los sistemas de gestión de calidad, mejorando permanentemente la calidad, facilitando una mayor participación en el mercado, optimizando costos, obteniendo una mejor rentabilidad. Por su dinamismo puede ser utilizado en todos los procesos de la organización y por su simple aplicación, que si se hace una forma adecuada, aporta en la realización de actividades de forma organizada y eficaz.(Moreno, 2014)

Figura 1. Ciclo PHVA



Fuente http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

Planear: En esta etapa se identifican los objetivos y las actividades necesarias para lograrlos, así como identificar los procesos involucrados para conseguir los resultados de acuerdo a las necesidades de la organización. Esta fase es muy importante ya que permite organizar el desarrollo de los otros pasos, es decir, si no planeamos bien, los resultados en las otras tres fases no serán los esperados.

- Definir el alcance del SGSI
- Definir la política de seguridad
- Metodología para la evaluación de riesgos
- Inventario de Activos
- Identificar amenazas y vulnerabilidades
- Identificar el impacto
- Análisis y evaluación de riesgos
- Selección de Controles y SOA

Hacer: En esta fase se ejecutan las actividades planeadas, se realizan cambios para implantar la mejora propuesta. En su desarrollo se puede evidenciar los problemas que se tienen en la implementación, se identifican las oportunidades de mejora y su puesta en marcha.

- Definir el plan de tratamiento de riesgos
- Implementar el plan de tratamiento de riesgos
- Implementar los controles
- Formar y concientizar
- Aplicar el SGSI

Verificar: Una vez implantada la mejora, en esta fase se realiza la comprobación del cumplimiento de los objetivos propuestos a través del seguimiento y medición, confirmando que estén acorde con las políticas y planeación inicial.

- Revisar el SGSI
- Medir la eficacia de los controles
- Revisar los riesgos residuales
- Realizar auditorías internas del SGSI
- Registrar eventos y acciones

Actuar: En esta etapa que puede llamarse de mejora continua, se realiza las acciones que mejoren el ejercicio de los procesos, se difunden los resultados obtenidos para hacer las recomendaciones a que haya lugar si se encuentre un resultado no esperado o se desea mejorar aún más el desempeño obtenido.

- Implementar mejoras al SGSI
- Aplicar acciones correctivas
- Aplicar acciones preventivas
- Comprobar la eficacia de las acciones
- Revisión de los resultados de los indicadores

5.1.3 ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información, esta norma recomienda las medidas que se deben implementar para asegurar los sistemas de información de las organizaciones (Portilla, 2015)en la que pueden encontrar una guía que sirva para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionar la seguridad de la información.

Fue publicada originalmente como un cambio de nombre de la norma ISO 17799. Fue en el 2000 cuando se publicó por primera vez como ISO 17799, y en 2005

aparece una nueva versión, junto con la publicación de la norma ISO 27001. No debe olvidarse que estos dos documentos están destinados a ser utilizados de forma complementaria. (Ministerio de Hacienda y Administraciones Públicas - Secretaría de Estado de Administraciones Públicas)

Esta norma contiene 39 objetivos de control y 133 controles, todos estos agrupados en 11 dominios. Los dominios son: Política de seguridad, aspectos organizativos de la seguridad de la información, gestión de activos, seguridad ligada a los recursos humanos, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de acceso, adquisición, desarrollo y mantenimiento de sistemas de información, gestión de incidentes en la seguridad de la información, gestión de la continuidad del negocio y cumplimiento.

5.1.4 ISO 27003. Proporciona métricas para la gestión de la seguridad de la información, da las directrices para la implementación de un SGSI, esta norma sirve de soporte a la ISO 27001. En esta norma describe el proceso de especificación del SGSI y el diseño desde el inicio hasta la elaboración de planes de ejecución. Además incluye el proceso para obtener la aprobación de la Dirección para implementar un SGSI, y da pautas sobre cómo planificar el proyecto del SGSI, resultando un proyecto final de ejecución del plan. (riesgoscontrolinformatico)

Está compuesta por: (Cepeda, 2016)

a. Alcance
b. Referencias normativas
c. Términos y definiciones
d. Estructura de la norma
e. Obteniendo la aprobación de la alta dirección para iniciar un SGSI
f. Definir el alcance del SGSI, límites y políticas
g. Evaluación de los requerimientos de seguridad de la información
h. Evaluación de riesgos y plan de tratamiento de riesgos
i. Diseño del SGSI

Y como anexos:

a. Anexo A. Lista de chequeo para la implementación de un SGSI
b. Anexo B. Roles y responsabilidades en seguridad de la información
c. Anexo C. Información sobre auditorías internas
d. Anexo D. Estructura de las políticas de seguridad
e. Anexo E. Monitoreo y seguimiento del SGSI

5.1.5 Política general de seguridad y privacidad de la información. La necesidad de la implementación de un SGSI queda consignada en la política general de seguridad y privacidad de la información, en ella se plantea la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de este proceso. De esta manera, la entidad define las necesidades de sus grupos de interés, la valoración de los controles para mantener la seguridad, establece una política que tenga en cuenta el marco general del funcionamiento de la entidad, objetivos institucionales, procesos misionales para que sea aprobada y guida por la Gerencia.

La política es concisa, fácil de leer y comprender, fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Es corta, y enmarca los principios que guían las actividades dentro de la entidad.

Según el MINTIC, en su guía Elaboración de la política general de seguridad y privacidad de la información (SGSI) – Guía No.2, sugiere la estructura típica del documento de las políticas que podría tener:

- Resumen. Política resumen- Visión general de una extensión breve
- Introducción. Breve explicación del asunto principal de la política
- Ámbito de aplicación. Descripción de las áreas y/o procesos de la organización a las que afecta y aplica la política.
- Objetivos. Descripción de la intención de la política
- Principios. Descripción de las reglas que conciernen a acciones o decisiones para alcanzar los objetivos.
- Responsabilidades. Descripción de responsabilidades de las personas con roles designados para el cumplimiento de la política.
- Políticas relacionadas. Descripción de actividades y controles necesarios para el cumplimiento de los objetivos, dentro de estas políticas se deben incluir detalles específicos como control de acceso, control en la seguridad física, uso de equipos, copias de seguridad, uso de los recursos entre otras.

La gerencia debe establecer de forma clara las líneas de las políticas de actuación y compromiso a la seguridad de la información, publicando y manteniendo políticas de seguridad en toda la organización.

Las políticas para la seguridad de la información se deben planificar y revisar con regularidad por si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad.

5.1.6 Metodología de análisis de riesgos. El primer paso para la gestión del riesgo es el análisis de riesgo que tiene como objetivo establecer los componentes de un sistema que requieren mayor protección a partir de las vulnerabilidades y amenazas que lo puedan poner en peligro con el fin de encontrar su grado de riesgo. Existen diversidad de metodologías para evaluar los riesgos, pero antes de llevar a cabo esta evaluación se deben tener identificados todos los activos de información que estén involucrados en la gestión de la información.

De la adecuada gestión de riesgos por intermedio de la juiciosa identificación de vulnerabilidades y las posibles amenazas que puedan explotar estas es de donde se podrán establecer las medidas preventivas y correctivas viables que puedan garantizar un mayor nivel de seguridad de la información.

- MAGERIT

Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, actualizada en 2012, que divide los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas para evitar cualquier inconveniente.

MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, persigue una aproximación metódica que deja lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Esta metodología persigue los siguientes objetivos:

- Sensibilizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de reducirlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación.

Se estructura de la siguiente forma: (Ministerio de Hacienda y Administraciones Públicas - Secretaría de Estado de Administraciones Públicas, s.f.)

- El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.
- El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.
- El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.

- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.
- El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.
- El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.
- El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.
-

Dentro de las fases que se debe cumplir para seguir esta metodología de análisis de riesgos tenemos:

- Determinar los activos relevantes para la organización su inter-relación y su valor en el sentido de que perjuicios o costos supondrían su degradación. Dentro de los activos informáticos se incluyen aquellos:
    - Activos Datos / Información: Agrupa los activos referentes a los soportes físicos y digitales usados dentro de la empresa para el desarrollo de las actividades diarias de los usuarios.
    - Servicios: Función que satisface una necesidad de los usuarios (del servicio). Contempla servicios prestados por el sistema
    - Activos de Software – Aplicaciones Informáticas: Agrupa los activos referentes a los programas o aplicativos usados dentro de la empresa para el desarrollo de las actividades diarias de los usuarios.
    - Activos de Hardware: El hardware de cómputo provee el fundamento físico básico para el desarrollo TI de la empresa, son los medios físicos destinados a dar soporte de los servicios que presta la oficina de TICS.
    - Activos de Redes y Comunicaciones: Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
    - Equipamiento Auxiliar: Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con los datos.
    - Instalaciones: Lugares donde se hospedan los sistemas de información y comunicaciones
    - Activos de Personal: Personas relacionadas con los sistemas de información.

- Determinar a qué amenazas están expuestos los activos informáticos: Las amenazas son cosas que ocurren o pueden ocurrir y que puede causar daño, entre ellas están: accidentes naturales, terremotos, inundaciones, desastres industriales, contaminación, fallos eléctricos, ante los cuales el sistema de información es víctima; otras amenazas son las personas, ya que por errores o fallos intencionados pueden causar daño. No todas las amenazas causan daño a todos los activos, por ejemplo, las inundaciones pueden causar daño a las instalaciones, pero al software no.
- Para realizar la valoración de las amenazas en los activos, se debe tener en cuenta las dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) que son afectadas y otorgarles un costo de afectación en dos sentidos: degradación (valoración del impacto potencial) mide el daño causado en el activo en el caso que ocurriera la amenaza, frecuencia mide cada cuanto se materializa la amenaza, brindando con esto la valoración del riesgo potencial, es decir, una amenaza puede ser de consecuencias nefastas pero es muy improbable que ocurra, mientras que otra amenaza puede ser de muy baja consecuencias pero de ocurrencia tan frecuente que puede terminar en un daño considerable.
- Determinar que salvaguardas o controles hay dispuestos y que tan eficaces son frente al riesgo. Los controles son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, como por ejemplo elementos técnicos: programas o equipos, seguridad física o política de personal. Entran en el cálculo de riesgo de dos maneras: reduciendo la frecuencia de amenazas (salvaguardas preventivas) o bajando las consecuencias de afectación.
- Estimar el impacto, definido como el daño sobre el activo derivado sobre la materialización de la amenaza, conociendo la valoración de los activos y la degradación que causan las amenazas es directo derivar el impacto que éstas tendrán sobre el sistema.
- Estimar los riesgos, definido como el impacto ponderado con la tasa de ocurrencia o expectativa de materialización de la amenaza. Se denomina riesgo a la medida del daño probable sobre un sistema, conociendo el impacto de las amenazas sobre los activos, el riesgo crece con el impacto y con la frecuencia.
- Elegir una estrategia para mitigar el impacto de riesgo, se determinan las salvaguardas oportunas para el objetivo anterior, se determina la calidad necesaria para dichas salvaguardas y se diseña un plan de seguridad para llevar el impacto y riesgo a niveles aceptables y por último se lleva a cabo el plan de seguridad.

5.2 MARCO CONTEXTUAL

5.2.1 Acerca de la empresa. Según el sitio web institucional de la empresa. www.herasmomeoz.gov.co), el hospital inicia sus labores en forma escalonada a partir del 15 de octubre de 1987, atendiendo primero la demanda en medicina general en 36 centros y puestos de salud de su entonces denominada área de influencia. El día 19 de noviembre de 1987, se dio al servicio el departamento de ginecobstetricia con 65 camas, luego en enero 04 de 1988 el departamento de pediatría inició su atención con 63 camas, el 28 de marzo de 1988 inició labores medicina interna con 42 camas y el 30 de marzo del mismo año el servicio de cirugía general con 105 camas; a mediados de 1988 quedaron habilitadas 325 camas.

Un año después de su entrada en funcionamiento (1988) la planta de personal del hospital, ascendía a 1100 funcionarios, siendo la mayor parte de sus trabajadores los que laboraban en el antiguo hospital San Juan de Dios, también se vinculó al personal de la clínica infantil Teresa Briceño de Andressen y del hospital sanatorio Amelia.

La estructura organizativa y órganos de dirección de la entidad están distribuidos de la siguiente forma:

- Dirección: Conformada por la Junta Directiva, compuesta por seis miembros de diferentes estamentos del departamento y el Gerente de la ESE.
- Atención al usuario: Conformado por la Sub-Gerencia de Servicios de Salud y cuatro secciones: Apoyo a la Atención, Servicios Hospitalarios, Servicios Quirúrgicos y Servicios Ambulatorios
- Logística Comprende la Sub Gerencia Administrativa la cual tiene a cargo tres secciones: Talento Humano, Recursos Físicos y Financiera.

5.2.2 Plataforma estratégica. Según el Acuerdo 014 de 12 de mayo de 2016, en el que se actualiza la plataforma estratégica de la institución:

Misión. Somos una Empresa Social del Estado, que produce y presta servicios de salud de mediana y alta complejidad, actuando como centro de referencia de la región, mejorando la calidad de vida de sus usuarios y generando desarrollo del conocimiento mediante docencia.[2]

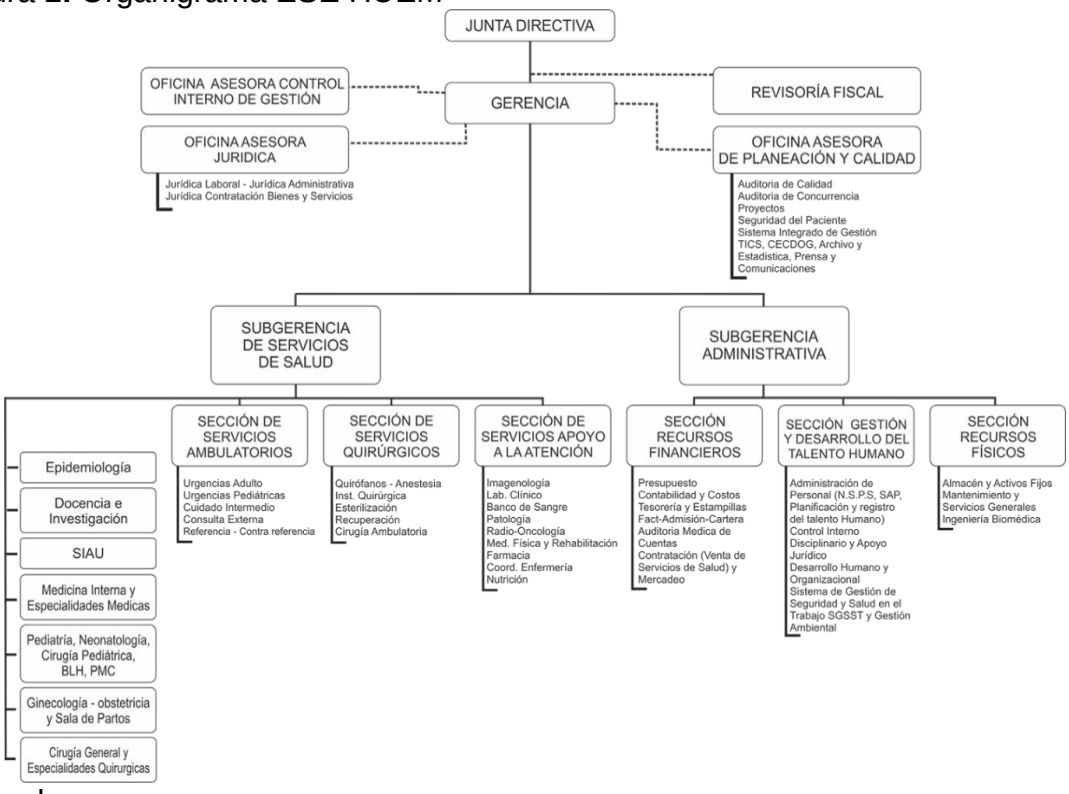
[2] Acuerdo 014 de 12 de mayo de 2016. Recuperado de http://www.herasmomeoz.gov.co/index.php/nuestra-empresa/plataforma-estrategica

Visión. Ser la institución Norte Santandereana prestadora de servicios de salud, posicionada y preferida por su atención humana, segura, alto enfoque investigativo, con rentabilidad social y económica.[3]

Objetivos Estratégicos. Servir bajo los lineamientos de seguridad del paciente
Eficiencia en la gestión de recursos públicos
Respeto por la dignidad humana en todas nuestras acciones
Mantener relaciones de confianza con los diferentes actores del sistema en salud
Ejecutar acciones en el marco del respeto y protección del medio ambiente
Jalonar servicios innovadores en salud
Orientar el trabajo en equipo para el logro de resultados
Reconocer al usuario como centro de la atención, satisfaciendo sus necesidades y expectativas.

5.2.3 Organigrama institucional. En la figura 2, se observa la estructura orgánica actual de la institución.

Figura 2. Organigrama ESE HUEM

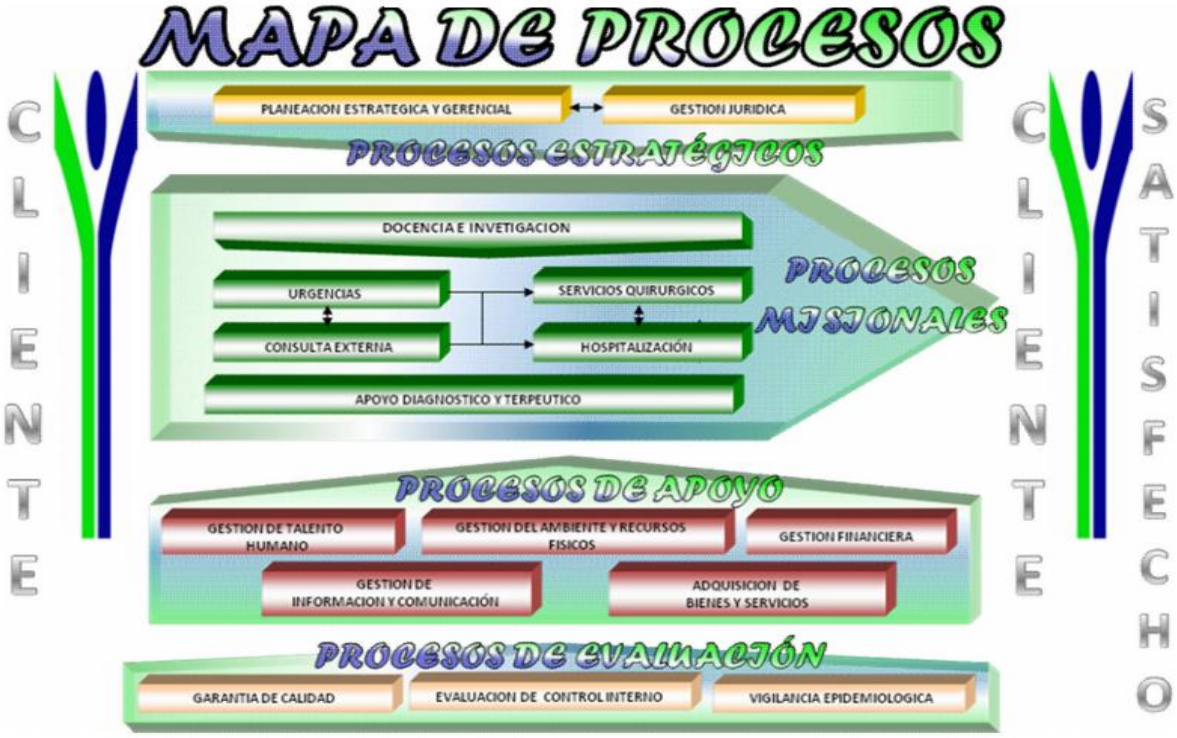


Tomado de: http://www.herasmomeoz.gov.co/images/planeacion/ORGANIGRAMAJULIO292016ESEHUEM.jpg

[3] Acuerdo 014 de 12 de mayo de 2016. Recuperado de http://www.herasmomeoz.gov.co/index.php/nuestra-empresa/plataforma-estrategica

5.2.4 Mapa de procesos. En la figura 3, se visualiza la estructura de procesos desarrollada por el Sistema Integrado de Gestión de la institución.

Figura 3. Mapa de Procesos ESE HUEM



Fuente: http://www.herasmomeoz.gov.co/

5.3 MARCO DE ANTECEDENTES

A continuación, se presentan algunos estudios con experiencias documentadas con las etapas abarcadas en la fase del diseño de un SGSI. No se presenta por secciones ya que la mayoría de trabajos documentados ofrecen un cubrimiento general sobre todos los aspectos de los SGSI relacionados. Por otra parte, se muestra un resumen contextual con las generalidades de planeación estratégica y el esquema de procesos que presenta actualmente la ESE Hospital Universitario Erasmo Meoz.

Modelo para la Implementación del Sistema General de Seguridad Informática y Protocolos de Seguridad Informática en la Oficina TIC de La Alcaldía Municipal De Fusagasugá, Basados En La Gestión Del Riesgo Informático. Trabajo de grado propuesto por Ana Milena Pulido y Jenith Marsella Mantilla en el presente año en el cual se presenta una propuesta de SGSI basado en el análisis de unos riesgos ya previamente identificados y de acuerdo a los lineamientos

establecidos por el ministerio de las tecnologías de la información y de las comunicaciones dentro de la ley 1341 de 2009, entre ellos los relacionados con trámites y servicios en línea, así como también lo señala la estrategia de gobierno en línea.

A través de este estudio desarrollan un documento con los pasos con los pasos para la implementación del modelo de Sistema de Gestión de Seguridad de la información, de acuerdo a los riesgos encontrados en la oficina de TIC, aplicando las fases del ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como dando aplicación a los lineamientos del estándar NTC:ISO/IEC 27001 para una posible certificación en este estándar.

Análisis de Riesgos y Recomendaciones de Seguridad de la Información al Área de Información y Tecnología del Hospital SUSANA LÓPEZ DE VALENCIA de la Ciudad de Popayán. Trabajo de grado presentado en el año 2014 por Henry Eduardo Bastidas, Iván Arturo López y Hernando José Peña donde a través de un análisis de riesgos y vulnerabilidades basados en la metodología MAGERIT se realizan una serie de propuestas de mecanismos de control y gestión de información para minimizarlos y se propone también un documento complementario donde se incentiva al desarrollo de buenas prácticas en el manejo de los recursos con el fin de apoyar el aseguramiento de la información. Todo esto basado en los lineamientos del estándar ISO 27001 y las fases del ciclo PHVA.

Diseñar un Sistema de Gestión de Seguridad de la Información Mediante la Norma ISO 27001 en el Instituto Colombiano de Bienestar Familiar Centro Zonal Virgen y Turístico de la Región Bolívar. Trabajo de grado presentado por Shirley Sandra Bueno Bustos en el año 2015. Este proyecto realiza el diseño de un SGSI usando la norma ISO 27001:2013 y la metodología MAGERIT para la gestión del riesgo en los activos de información presentes en el ICBF Centro Zonal Virgen y Turístico en búsqueda de garantizar la seguridad de la información y tener un nivel de riesgo aceptable. Identifica vulnerabilidades y riesgos, define las políticas de seguridad informática, establece los procedimientos documentados basándose en el estándar y establece los controles para la eficacia del SGSI.

5.4 MARCO CONCEPTUAL

Un adecuado Sistema de Gestión de la Seguridad de la Información representa un punto de partida para el diseño de controles que conllevan a mitigar los principales riesgos encontrados dentro de la organización para de esta manera gestionarlos y reducir al máximo su probabilidad de ocurrencia. A través de metodologías como MAGERIT o normas como la ISO 27001 se puede abordar esta realidad que debe preocupar hoy por hoy a todas las organizaciones independientemente de su tamaño y/o campo de acción principal.

Para el desarrollo del diseño hay que tener en cuenta que la seguridad de la información como el conjunto de los procedimientos, estrategias y herramientas que permiten garantizar la integridad, la disponibilidad y confidencialidad de la información de una entidad. A menudo este concepto se confunde con el de seguridad informática, pero hay que destacar que este concepto solo se refiere a la seguridad en medios informáticos, mientras que la seguridad de la información hace referencia a diferentes medios o formas en que se puedan encontrar los datos. A raíz del gran valor que ha tomado la información y su reconocimiento como el principal activo de las organizaciones han surgido diferentes estándares y/o herramientas que ayudan a identificar cuáles son los puntos en los cuales una organización debe tener mayor atención a través de la identificación de problemas, análisis de riesgos, entre otras y a partir de allí generar controles que permitan mitigarlos y disminuir las probabilidades de que alguno(s) de los riesgos detectados la impacte, con lo cual la afectaría en alguna medida.

Para hablar de seguridad de la información se hace necesario conocer sus principales características, con lo cual se tienen las bases para comenzar a edificar el sistema en un orden correcto. Estos pilares son confidencialidad, integridad y disponibilidad, las cuales se describen a continuación:

Confidencialidad: Capacidad de no divulgar o publicar información sensible de una empresa a personas no autorizadas. Como ejemplo tenemos los accesos no autorizados, fugas y filtraciones de información. Al tener fallo en esa característica de la información, supone el incumplimiento de leyes y compromisos en relación a la custodia de datos, además que la organización evidenciaría que no es competente para el manejo de datos.

Integridad: Característica de mantener la información de manera intacta sin tener modificaciones. Al fallar este elemento afecta directamente el correcto funcionamiento de la organización.

Disponibilidad: Consiste en tener los activos disponibles cuando se requiere su uso. La falta de este atributo evidencia una interrupción del servicio y afecta la productividad de la organización.

El desarrollo de un Sistema de gestión de seguridad de la información es un proceso sistemático, documentado que se realiza para garantizar que la seguridad de la información es gestionada correctamente, buscando mantener la confidencialidad, integridad y disponibilidad para contrarrestar los riesgos a los cuales puede estar expuesta la entidad, lo cual es precisamente el objeto de aplicar la seguridad de la información y la seguridad informática.

Información: Datos que maneja la empresa ya sea en forma digital o impresa.

Activos de la información: Elementos de valor que posee la empresa como son, datos, software, hardware, elementos de redes y comunicaciones, infraestructura y recursos humanos.

Riesgo: Aquella eventualidad que imposibilita el cumplimiento de un objetivo.

Amenazas: Cualquier situación que se puede presentar en la entidad dañando un activo de información, mediante la explotación de una vulnerabilidad.

Vulnerabilidad: Es toda debilidad del sistema informático que puede ser utilizada para causar un daño. Corresponde a las ausencias o fallas en los controles para proteger un activo.

Impacto: Es el alcance del daño que se produce en un activo cuando sucede una amenaza.

Análisis de riesgos: Es un elemento fundamental dentro del proceso de implantación de un SGSI debido a que es en esta fase donde se cuantifica la importancia de los activos para la seguridad de la organización.

Controles: Medida de protección que se implementa para minimizar los riesgos.

5.5 MARCO LEGAL

Resolución 1995 de 1999. Por la cual se establece normas para el manejo de la historia clínica y se establecen la organización y manejo del archivo de historias clínicas, custodia, acceso y seguridad[4]. La entidad como prestadora de servicios de salud, tiene bajo su custodia la información de historia clínica de los pacientes, siendo esta norma de obligatorio cumplimiento para el hospital ya que indica los registros que debe contener, quienes pueden tener acceso a ella, la custodia, la seguridad y condiciones de almacenamiento.

Ley 1266 de 2008. Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Tiene por objeto desarrollar el derecho constitucional de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, además de los derechos, libertades y garantías relacionadas con la recolección, tratamiento y circulación de datos

[4]Resolución 1995 de 199. Recuperado de https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

personales, así como el derecho a la información[5]. La entidad como Operador de información, por recibir información de datos personales directamente del titular, tiene la administración de los mismos, por tanto, está obligado a garantizar la protección de estos datos.

Ley 1431 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Reglamentada por el decreto 2693 de 2012 y 2573 de 2014[6]. A través de esta ley se facilita el libre acceso y sin discriminación a los habitantes del territorio nacional a la Sociedad de la información y establece el régimen de protección al usuario entre otras cosas.

Ley 1273 de 2009. Por el cual se modifica el código Penal, creando u nuevo bien jurídico tutelado llamado de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones[7]. En esta norma, tipifica y protege la información de los datos, sentando en el código penal algunos delitos informáticos con sus respectivas penas. A nivel general tenemos:

- Suplantación de sitios web para capturar datos personales.
- Violación de datos personales.
- Uso de software malicioso.
- Daño informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Acceso abusivo a un sistema informático.

Cuya pena en prisión puede ir de 48 a 96 meses y multa de 100 a mil salarios mínimos mensuales legales vigentes.

- Interceptación de datos informáticos.

Incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- Transferencia no consentida de activos.

Incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes

- Hurto por medios informáticos y semejantes

Se aplicará las penas establecidas en el art.240 del código Penal. La pena será de 5 a 12 años de prisión.

---

[5]Ley 1266 de 2008. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

[6]Ley 1431 de 2009. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

[7]Ley 1273 de 2009. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

También define aquellos agravantes que aumentarán las penas dispuestas, como por ejemplo: aquellos cometidos sobre redes oficiales o del sector financiero, por servidor público en ejercicio de sus funciones, aprovechando la confianza depositada por el poseedor de la información, publicando información en perjuicio de otro, obteniendo provecho para sí mismo o para un tercero, con fines terroristas, generando riesgo para la seguridad nacional, si quien cometiere estos delitos es el responsable de la administración, manejo o control, se le impondrá pena de inhabilitación hasta por tres años para el ejercicio de su profesión relacionada con los sistemas de información.

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales, cuyo objeto es desarrollar el derecho constitucional a conocer, actualizar y rectificar informaciones que se hayan recogido en bases de datos o archivos, así como el derecho a la información consagrado[8]. Sobre el tratamiento de datos personales se aplican diferentes principios, entre ellos, el de transparencia, acceso y circulación restringida, de seguridad y confidencialidad.

Resolución 2003 de 2014. Por la cual se define los estándares de habilitación para las instituciones prestadoras de servicios de salud, dentro de ellos Historia Clínica y Registros, que busca la existencia y cumplimiento de procesos que garanticen la historia clínica por paciente y las condiciones técnicas de su manejo y el de los registros de procesos clínicos que se relacionan directamente con los principales riesgos propios de la prestación de servicios, estableciendo que para la gestión de las historias en medios electrónicos, se debe garantizar la confidencialidad y seguridad, sin que se puedan modificar los datos una vez se guarden los registros, garantizando la confidencialidad del documento protegido legalmente por reserva .[9]

Decreto 903 de 2014. Por el cual se dictan disposiciones en relación con el Sistema Único de Acreditación en salud. Dicta disposiciones y realiza ajustes al sistema único de acreditación en Salud, como componente del Sistema Obligatorio de Garantía de Calidad de la Atención de salud. [10] El sistema de acreditación es voluntario, y las entidades que deciden implementarlo, deben comprobar el cumplimiento de niveles de calidad superiores a los requisitos mínimos obligatorios (habilitación).

---

[8]Ley estatutaria 1581 de 2012. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[9] Resolución 2003 de 2014. Recuperado de https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%202003%20de%202014.pdf

[10] Decreto 903 de 2014. Recuperado de http://www.acreditacionensalud.org.co/userfiles/file/2015/Decreto%200903%20de%202014.pdf

Manual de Acreditación en salud. El Ministerio de Salud y Protección Social adoptará los manuales, los cuales serán de uso libre, podrán ser ajustados periódicamente y de manera progresiva. El Manual de Acreditación está dividido en Grupos de estándares que a su vez contienen criterio y estándares, así como el estándar de mejoramiento por cada grupo. Los estándares que aplican para la institución son estándares del proceso de atención al cliente asistencial, estándares de direccionamiento, estándares de gerencia, estándares de gerencia del talento humano, estándares de gerencia del ambiente físico, estándares de gestión de tecnología, estándares de gerencia de la información, estándares de mejoramiento de la calidad.

Para el presente proyecto aplicado, se realiza especial énfasis en el Grupo de estándares de Gerencia de la Información, el cual busca la integración de las áreas asistenciales y administrativas en relación con la información clínica y administrativa buscando que los procesos tengan información adecuada para la toma de decisiones y obliga a la implementación de mecanismos y estrategias para garantizar la seguridad y confidencialidad de la información, desarrollando un plan de gerencia de la información, con fundamento en el ciclo de mejoramiento continuo.[11]

La organización debe cumplir con criterios como el estándar 144. Existen mecanismos estandarizados, implementados y evaluados para garantizar la seguridad y confidencialidad de la información, cuyos criterios son: la seguridad y confidencialidad; acceso no autorizado; pérdida de información; manipulación; mal uso de los equipos y de la información, para fines distintos a los legalmente contemplados por la organización; deterioro, de todo tipo, de los archivos; los registros médicos no pueden dejarse o archivarse en sitios físicos donde no esté restringido el acceso a visitantes o personal no autorizado; existe un procedimiento para la asignación de claves de acceso; existencia de backups y copias redundantes de información; control documental y de registros; indicadores de seguridad de la información.

Decreto 2573 de 2014. Por el cual se establecen los lineamientos generales (lineamientos, instrumentos y plazos) de la Estrategia de Gobierno en línea, para garantizar el aprovechamiento de las Tecnologías de la Información y Comunicaciones y se reglamenta parcialmente la Ley 1341 de 2009[12].

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública nacional y se dictan otras

[11] Manual de Acreditación en salud. Recuperado de http://www.acreditacionensalud.org.co/Documents/Manual%20AcreditSalud%20AmbulyHosp2012.pdf

[12] Decreto 2573 de 2014. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596#14

disposiciones. Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.[13]

Resolución 3564 de 2015. Tiene por objeto establecer los lineamientos respecto de los estándares para publicación y divulgación de la información, accesibilidad en medios electrónicos para población en situación de discapacidad, formulario electrónico para la recepción de solicitudes de acceso a información pública, condiciones técnicas para la publicación de datos abiertos y condiciones de seguridad de los medios electrónicos, que se establecen en los artículos 2.1.1.2.1.1, 2.1.1.2.1.11, y el parágrafo 2 del artículo 2.1.1.3.1.1 del Decreto N° 1081 de 2015. [14]

[13] Ley 1712 de 2014. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882

[14] Res.3564 de 2015. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=66249

6. DISEÑO METODOLOGICO

6.1 METODOLOGIA DE LA INVESTIGACION

Se realizará un estudio descriptivo de la seguridad informática en la ESE Hospital Universitario Erasmo Meoz, recolectando información a través de entrevistas, observación y lista de chequeo para obtener un panorama general de la situación actual.

Se procederá a realizar investigación en diferentes fuentes de información como libros, proyectos de grado e internet para seleccionar la metodología ideal para realizar el análisis de riesgos.

Basados en la experiencia adquirida, y teniendo en cuenta los dominios de la norma y recomendaciones de otros profesionales relacionados con el tema se establecerán los controles a implementar.

6.2 METODOLOGIA DE DESARROLLO

Para el desarrollo del presente trabajo de grado se usará para recolección y análisis de datos la entrevista y la observación directa de los escenarios en los que aplicaremos las actividades a ejecutar. La entrevista como método más efectivo para lograr conseguir la información solicitada, además que con ella se obtiene contacto directo con las personas involucradas en el proceso y de esta manera identificar inmediatamente su adherencia y colaboración a este proyecto.

La población será la oficina de TICS de la ESE Hospital Universitario Erasmo Meoz y se tomará una muestra de los activos informáticos más importantes de ésta área.

Pasos a seguir para el cumplimiento de los objetivos propuestos:

En primer lugar, para *realizar el diagnóstico del estado actual de la seguridad informática en la entidad aplicando la norma ISO 27001:2013*, se tiene planeado realizar lo siguiente:

- Recolección de información a través de la observación y entrevistas a los funcionarios involucrados.
- Consulta de la normatividad vigente aplicable a la seguridad informática y relacionada con el sector salud al cual pertenece la entidad.
- Consulta de información y selección de la metodología adecuada para realizar el análisis de riesgos
- Realización de un diagnóstico inicial del estado de la seguridad de la información en la entidad.
- Realización del inventario de activos de la información

- Identificar amenazas, vulnerabilidades, y el impacto
- Aplicación de la metodología seleccionada para desarrollar la gestión de riesgos

Como actividades para el cumplimiento del segundo objetivo *Establecer un modelo de Sistema de Gestión de seguridad informática, teniendo en cuenta lo establecido en la fase de planear del ciclo PDCA según lo indica la norma ISO27001:2013*, se tiene prevista la ejecución de:

- Definir el alcance del SGSI
- Documentar el establecimiento de la política de seguridad de la información y revisar si está acorde a las necesidades institucionales, estableciendo responsabilidades para la aplicación, con un alcance determinando la población, áreas, procesos para su cumplimiento.
- Realizar el Inventario de Activos de la Información
- Aplicar la metodología para la gestión de riesgos; Identificar amenazas y vulnerabilidades e impacto
- Análisis y evaluación de riesgos
- Selección de Controles y SOA, verificando controles existentes que aplican la norma 27002 mediante un checklist
- Declaración de aplicabilidad, selección de los dominios y controles de la norma para contrarrestar las amenazas encontradas.

Finalmente, con la información obtenida de las actividades anteriores se procederá a realizar el *Diseño de la propuesta de solución planificada y de mejora continua bajo la norma ISO 27001*.

7. ESTADO ACTUAL DE LA SEGURIDAD

La lista de chequeo del Estado Actual de la Seguridad se realiza basada en los estándares de la norma ISO27001:2013, asignando una calificación de valoración de cumplimiento y esperado, de acuerdo a la recolección de evidencias proporcionadas, entrevista con el coordinador de sistemas y la observación realizada.

La escalada de valoración sobre la que se realiza es la siguiente:

Tabla 1. Escala de Valoración de Controles

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. *No hay procesos estandarizados*. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	*Los procesos y los controles siguen un patrón regular.* Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	*Los procesos y los controles se documentan y se comunican.* Los controles *son efectivos y se aplican casi siempre*. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: Instrumento de identificación de la línea base de seguridad MINTIC

Se obtiene el siguiente resultado:

ESE HOSPITAL UNIVERSITARIO ERASMO MEOZ

LISTA DE CHEQUEO CUMPLIMIENTO ESTANDAR ISO 27001:2013

Fecha de revisión: Agosto de 2017

Tabla 2. Lista de chequeo cumplimiento estándar ISO 27001

CONTROLES	SELECCIÓN DE RESPUESTA		
5. POLÍTICAS DE SEGURIDAD			
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN. Objetivo: Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
La empresa cuenta con un conjunto de políticas para la seguridad de la información aprobadas por la dirección, publicadas y comunicadas a los empleados y partes interesadas?	20	80	La entidad cuenta con la política de seguridad de la información aprobada por la gerencia, sin embargo esta no es conocida por los empleados ni partes interesadas.
La empresa realiza revisión a intervalos planificados o si ocurren cambios significativos de las políticas para la seguridad de la información?	0	80	Se realizan cambios en las políticas pero estos no son documentados.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION			
A. 6.1 Organización interna. Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
La empresa define y asigna las responsabilidades para la seguridad de la información?	40	80	
La empresa separa las tareas y áreas de responsabilidad en conflicto para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización?	40	80	
La empresa mantiene contactos apropiados con las autoridades pertinentes?	20	80	
La empresa mantiene controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad?	40	80	
La seguridad de la información se debe trata en la gestión de proyectos, independiente del tipo de proyecto?	0	80	
A.6.2 Dispositivos para movilidad y teletrabajo. Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
Se adoptan políticas o medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles?	20	80	Se toman algunas medidas por la experiencia o eventos sucedidos pero no son tomadas por un análisis de riesgos.

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo	40	80	En la institución no se aplica teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
A.7.1 Antes de la contratación. Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
7.1.1. Antes de la contratación del personal, son investigados y validados los antecedentes disciplinarios y judiciales?	80	80	
7.1.2 Se aceptan y firman los términos y condiciones del contrato del empleo, el cual contiene las funciones y demás información referente al cargo y en cuanto a la seguridad de la información?	20	80	No existen acuerdos de confidencialidad de la información dentro del contrato firmado
A.7.2 Durante la ejecución del empleo. Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
7.2.1 La Dirección exige en el momento de la contratación aplicar la seguridad en concordancia con las políticas y procedimientos?	20	80	
7.2.2. Todos los empleados reciben capacitación sobre la concientización e información sobre aspectos de la seguridad de la información?	60	80	
7.2.3 Existe un proceso formal disciplinario comunicado a empleados sobre la seguridad?	40	80	Se encuentra conformado un comité interno disciplinario pero actualmente no se encuentran documentadas las faltas y sanciones referentes a la seguridad
7.3 Cese o cambio de puesto de trabajo. Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
7.3.1 Se tiene claro en el momento de fin de contrato o cambio de puesto de trabajo, que acciones para proteger la seguridad de la información se deben seguir y se ejecutan?	0	80	Por el volumen de contratistas, en ocasiones no informan de los cambios ni de los retiros de los empleados.
8. GESTIÓN DE ACTIVOS			
8.1 Responsabilidad sobre los activos. Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
8.1.1 Existe un inventario de los activos, donde se encuentren claramente identificados?	60	80	Se tiene una hoja de vida de los equipos informáticos

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
8.1.2 Toda la información y activos del inventario están asociados a un responsable de la empresa para su conservación y seguridad?	60	80	
8.1.3 Se implantan regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información?	40	80	
8.1.4 Terminado el contrato del empleado, existe un procedimiento para la devolución y revisión de los activos asignados durante su tiempo laborado?	80	80	Existe un formato de paz y salvo, donde tos los líderes de área verifica si el empleado tiene cosas pendientes con cada área, en el caso de los activos entregados hay un formato adicional de entrega de equipos informáticos con su respectivas observaciones de estado del activo.
8.2 Clasificación de la información. Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
8.2.1 La información se clasifica en relación a su valor, requisitos legales, sensibilidad e importancia para la empresa?	40	80	La empresa cuenta con TRD aprobadas y publicadas, pero su aplicación en cuanto al resguardo de las copias de seguridad no ha sido el adecuado.
8.2.2 Se tiene un procedimiento para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la empresa?	40	80	
8.2.3 Se tiene procedimientos para el manejo de los activos de acuerdo con el esquema de clasificación de información adoptado por la organización?	20	80	
8.3 Manejo de los soportes de almacenamiento. Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
8.3.1 Se establecen procedimientos para la gestión de los medios informáticos extraíbles?	40	80	A través del antivirus se pueden analizar pero el usuario a veces desconoce su uso.
8.3.2 Se eliminan información de los medios cuando ya no sean requeridos?	40	80	En la actualidad se elimina de acuerdo al criterio del usuario.

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
8.3.3 Se protegen los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte?	40	80	
9. CONTROL DE ACCESO			
9.1 Requisitos del negocio para el control de acceso. Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
9.1.1 Se establece, documenta y revisa una política para el control de acceso?	60	80	No se encuentra documentada.
9.1.2 Existen controles para el acceso a redes y a servicios en red?	60	80	
9.2 Gestión del acceso de usuarios. Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
9.2.1 Existe un proceso para el registro y/o cancelación de los usuarios nuevos o salientes?	60	80	Existe un formato de creación / cancelación de usuarios
9.2.2. Existe algún proceso que permita identificar que usuarios pueden acceder a los diferentes sistemas y sus respectivos privilegios?	60	80	
9.2.3 Existe algún proceso para la gestión de derechos de acceso con privilegios especiales?	40	80	El jefe solicita los permisos adicionales o privilegios especiales, pero no se encuentra documentado en un procedimiento.
9.2.4 Existen políticas para la creación de contraseñas de usuarios?	20	80	Solo para el correo institucional.
9.2.5 Existe un proceso de revisión periódica de los derechos de accesos de los usuarios?	20	80	
9.2.6 Existe algún tipo de control para establecer la retirada o adaptación de los derechos de acceso?	20	80	
9.3 Responsabilidades del usuario. Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
9.3.1 Existen acuerdos de confidencialidad?	20	80	
9.4 Control de acceso a sistemas y aplicaciones. Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
9.4.1 Existen restricciones del acceso a la información?	80	80	
9.4.2. Existen procedimientos seguros de inicio de sesión?	80	80	
9.4.3 Existen métodos de gestión de contraseñas?	20	80	
9.4.4 Se restringe y controla el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones	60	80	
9.4.5 Existen algún control sobre el acceso a códigos fuente de programas?	40	80	
10. CRIPTOGRAFÍA			
10.1 Controles criptográficos. Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger	CUMPLIMIENTO	ESPERADO	OBSERVACIONES

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
la confiabilidad, la autenticidad y/o la integridad de la información.			
10.1.1. Se desarrolla o implementa una política que regule el uso de controles criptográficos para la protección de la información?	0	60	
10.1.2 Se desarrolla o implementa una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida?	0	60	
11. SEGURIDAD FISICA Y AMBIENTAL			
11.1 Áreas seguras. Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
11.1.1 Se utilizan perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica?	20	80	
11.1.2 Las áreas seguras están protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso?	40	80	
11.1.3 Se aplica un sistema de seguridad física a las oficinas, salas e instalaciones de la organización?	40	80	
11.1.4 se aplica una protección física contra desastres naturales, ataques maliciosos o accidentes?	20	80	
11.1.5 Existen y se aplican procedimientos para trabajo en áreas seguras?	40	80	
11.1.6 Se controlan puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información?	40	80	
11.2 Seguridad de los equipos. Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
11.2.1 Los equipos se ubican de manera que se reduzcan los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado?	40	80	
11.2.2 Los equipos se protegen contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo?	60	80	
11.2.3 Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se protegen contra la intercepción, interferencia o posibles daños?	20	80	
11.2.4 Se cumple con el cronograma de mantenimiento a los equipos con el fin de asegurar su disponibilidad e integridad?	80	80	
11.2.5 Los equipos, la información o el software se retiran del sitio sin previa autorización?	60	80	
11.2.6 Se aplica la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos?	20	80	

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
11.2.7 Antes de dar de baja o reubicar algún equipo que contenga cualquier tipo de dato sensible y/o software con licencia se verifica que dicha información se hayan extraído o se haya sobrescrito de manera segura?	80	80	
11.2.8 Los equipos sin supervisión de usuarios cuentan con la protección adecuada?	60	80	
11.2.9 Se adopta una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información?	40	80	
12. SEGURIDAD DE LAS OPERACIONES			
12.1 Procedimientos operacionales y responsabilidades. Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
12.1.1 Existe documentación de los procedimientos de operación?	40	80	
12.1.2 Existe proceso de gestión de cambios?	40	80	
12.1.3 Se realiza seguimiento al uso de recursos, ajustes y proyecciones de capacidad futura?	20	80	
12.1.4 Los entornos de prueba y desarrollo están separados?	0	80	
12.2 Protección contra códigos maliciosos. Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
12.2.1 Existen controles contra código malicioso?	60	80	Los equipos cuentan con software antivirus debidamente licenciado y actualizado
12.3 Copias de Seguridad. Objetivo. Proteger contra la perdida de datos	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
12.3.1 Existen copias de seguridad de la información?	80	80	Se realizan copias de seguridad que se almacenan dentro y fuera de la organización
12.4 Registro y Seguimiento. Objetivo. Registrar eventos y generar evidencia	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
12.4.1 Existen registros de eventos?	20	80	Se utiliza el log de auditoria de la aplicación
12.4.2 Los registros de información están debidamente protegidos?	20	80	
12.4.3 Existe un log de actividades del administrador y/o operador del sistema?	60	80	Log de actividades del sistema operativo
12.4.4 Existe sincronización de relojes?	60	80	
12.5 Control de software operacional. Objetivo. Asegurarse de la integridad de los sistemas operacionales	CUMPLIMIENTO	ESPERADO	OBSERVACIONES

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
12.5.1 Se realiza monitoreo y control de los equipos en los cuales es instalado el software de la organización?	60	80	
12.6 Gestión de vulnerabilidad técnica. Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
12.6.1 Se realiza un diagnóstico de las vulnerabilidades técnicas?	40	80	
12.6.2 Existen restricciones para la instalación de software?	80	80	
12.7 Consideraciones sobre auditorias de sistemas de información. Objetivo. Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
12.7.1 Se realizan auditorias periódicas a los sistemas de información?	40	80	
13. SEGURIDAD DE LAS COMUNICACIONES			
13.1 Gestión de seguridad de redes. Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
13.1.1 Se monitorea y se controla las redes para proteger la información de los sistemas y las aplicaciones?	60	60	A través de un equipo UTM-Fortigate 80C
13.1.2 Se identifica e incluye en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red?	40	60	
13.1.3 Se segregan las redes en función de los grupos de servicios, usuarios y sistemas de información?	40	60	Las redes están segmentadas de acuerdo al área de trabajo
13.2 Transferencia de Información. Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
13.2.1 Existen políticas, procedimientos y controles formales de transferencia para proteger la información?	20	60	
13.2.2 Se auditan el intercambio de información comercial entre la empresas y personas externas?	20	60	
13.2.3 Se protege adecuadamente la información recibida a través de correos electrónicos?	60	60	Se analizan a través del UTM y del antivirus
13.2.4 Se realizan acuerdos de confidencialidad y "no divulgación" con las partes externas que reflejen las necesidades de la empresa para la protección de información?	20	60	
14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
14.1 Requisitos de seguridad de los sistemas de información. Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes publicas	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
14.1.1 Los requisitos relacionados con seguridad de la información se incluyen en los requisitos para nuevos	40	60	

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
sistemas de información o para mejoras a los sistemas de información existentes?			
14.1.2 La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se protegen de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	20	60	
14.1.3 La información involucrada en las transacciones de servicios de aplicaciones se protege para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizado	20	60	
14.2 Seguridad en los procesos de desarrollo y soporte. Objetivo. Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
14.2.1 Se tienen establecidas y se aplican las reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización	20	60	En la empresa no se realiza desarrollos de sistemas de información, son contratados a terceros.
14.2.2 Existen procedimientos de control para para realizar cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas y a los desarrollos dentro de la organización?	40	60	
14.2.3 Cuando se cambian las plataformas de operación, se revisan las aplicaciones críticas del negocio, y se pone a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacional?	40	60	
14.2.4 Existen restricciones a los cambios en los paquetes de software?	20	60	
14.2.5 Se tiene documentado y se mantienen principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información?	20	60	
14.2.6 La empresa establecer y protege adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistema	20	60	En la empresa no se realiza desarrollos de sistemas de información, son contratados a terceros.
14.2.7 La organización supervisa y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados?	20	60	
14.2.8 Durante el desarrollo se lleva a cabo ensayos de funcionalidad de la seguridad?	40	60	
14.2.9 Existen programas o alguna lista de chequeo que contenga los criterios mínimos para la aceptación de nuevos sistemas de información?	40	60	
14.3 Datos de prueba. Objetivo. Asegurar la protección de los datos usados para ensayos	CUMPLIMIENTO	ESPERADO	OBSERVACIONES

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
Se protegen los datos que son utilizados en las pruebas?	20	60	
15. RELACIONES CON LOS PROVEEDORES			
15.1 Seguridad de la información en las relaciones con suministradores. Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
15.1.1 Existe una política donde este acordado y documentado adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas?	0	60	
15.1.2 Se establece y acuerda todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización?	20	60	
15.1.3 Los acuerdos con los proveedores incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones?	0	60	
15.2 Gestión de la prestación del servicio por suministradores. Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
15.2.1 Se monitorea, revisa y audita la presentación de servicios del proveedor regularmente?	20	60	
15.2.2 Se administra los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos?	0	60	
16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION			
16.1 Gestión de incidentes y mejoras en la seguridad de la información. Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
16.1.1 ¿Existen procedimientos y responsables que permitan gestionar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?	20	60	Existe delegación en el grupo de ingenieros pero esta no se encuentra documentada.
16.1.2 ¿Existen Canales que garantizan informar oportunamente los eventos de seguridad de la información?	20	60	Se elabora informe de algunos incidentes de seguridad, de definen controles y medidas necesarias para disminuir los incidentes y prevenir su

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
			ocurrencia en el futuro pero no se incluyen en el plan de mejoramiento continuo.
16.1.3 ¿Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información toman nota y comunican cualquier debilidad observada o sospechada en la seguridad de los sistemas e Información?	0	60	Solo algunos miembros de la entidad informan eventos que son reportados de forma inconsistente.
16.1.4 ¿Se evalúan los eventos de Seguridad de la Información para ser clasificación como Incidentes de Seguridad de la Información?	0	60	Algunos de los eventos reportados son analizados para determinar si constituyen un incidente de seguridad y entender el objetivo del ataque y su método. No son categorizados y no se cuenta con planes de respuesta para cada categoría.
16.1.5 ¿Existen procedimientos documentados para dar respuesta oportuna a los incidentes de Seguridad de la Información?	0	60	No se cuenta con un plan de recuperación de incidentes durante o después del mismo.
16.1.6 ¿Existe una bitácora con los análisis y soluciones de los incidentes, que permita reducir los incidentes futuros?	0	60	
16.1.7 ¿Existen procedimientos documentados donde la identificación, recopilación, adquisición y preservación de la información que implique una acción legal (civil o criminal), permita ser utilizadas como evidencias?	0	60	Para la recolección de evidencia no se cuenta con: a) definir la cadena de custodia; b) establecer la seguridad de la evidencia; c) definir la seguridad del personal; d) definir los roles y responsabilidades del personal involucrado; e) establecer la competencia del personal; f) realizar la documentación; g) definir las

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
			sesiones informativas.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO			
17.1 Continuidad de seguridad de la información. Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
17.1.1 ¿La entidad en situaciones adversas o durante una crisis o desastres tiene un proceso de gestión (controles preventivos y de recuperación) que permita asegurar la continuidad de los servicios?	0	60	La Entidad no cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan).
17.1.2 ¿La Entidad aplica procesos, procedimientos y controles documentados que permitan asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversas?	0	60	
17.1.3 ¿Los controles establecidos e implementados por la entidad, son verificados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas?	0	60	
17.2 Redundancia. Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
17.2.1 ¿La entidad tiene implementado para el procesamiento de la información redundancia para cumplir los requisitos de disponibilidad?	0	60	La Entidad no cuenta con arquitecturas redundantes.
18. CUMPLIMIENTO			
18.1 Cumplimiento de los requisitos legales y contractuales. Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
18.1.1 ¿La entidad tiene identificado y documentado el Normograma (requisitos estatutarios, normativos y contractuales legislativos), para cada sistema de información, de acuerdo a la operación del Negocio?	60	60	La entidad cuenta con el grupo de apoyo de SIG que recolecta la información, de acuerdo a lo reportado por las diferentes áreas y la actualiza en el Normograma que se encuentra publicado en la web. Falta apropiación por los miembros de la organización para reportar estos datos.
18.1.2 ¿La Entidad garantiza la propiedad intelectual del uso de software mediante procedimientos apropiados para el cumplimiento de los requisitos legislativos, de reglamentación y contractuales?	20	60	La entidad garantiza DPI, pero no tiene procedimientos

Continuación Tabla 2 Lista de chequeo cumplimiento estándar ISO 27001:2013

CONTROLES	SELECCIÓN DE RESPUESTA		
			eficaces para el cumplimiento de los requisitos legales.
18.1.3 ¿La entidad cuenta con procesos y procedimientos documentados que permitan proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, los registros?	40	60	La entidad cuenta con tablas de retención documental que especifican los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción.
18.1.4 ¿La entidad cuenta con procesos y procedimientos documentados que permitan asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación vigente?	20	60	
18.1.5 ¿La entidad aplica controles de cifrado de la información?	0	60	
18.2 Revisiones de la seguridad de la información. Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales	CUMPLIMIENTO	ESPERADO	OBSERVACIONES
18.2.1 ¿La entidad revisa, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información de forma independiente?	60	60	El área de Control Interno anualmente realiza auditoría sobre los procesos de Gestión de la información y comunicaciones y establece recomendaciones.
18.2.2 ¿La entidad aplica las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad?	20	60	La entidad cuenta con un manual de políticas de sistemas desactualizada y no se establece revisión periódica de ellas.
18.2.3 ¿La Entidad revisa con regularidad el cumplimiento con las políticas y normas de seguridad dispuestas la entidad?	0	60	No hace la revisión o evaluación de seguridad técnicas, de acuerdo a políticas o normas, utiliza solo las buenas practicas

Fuente: Los autores

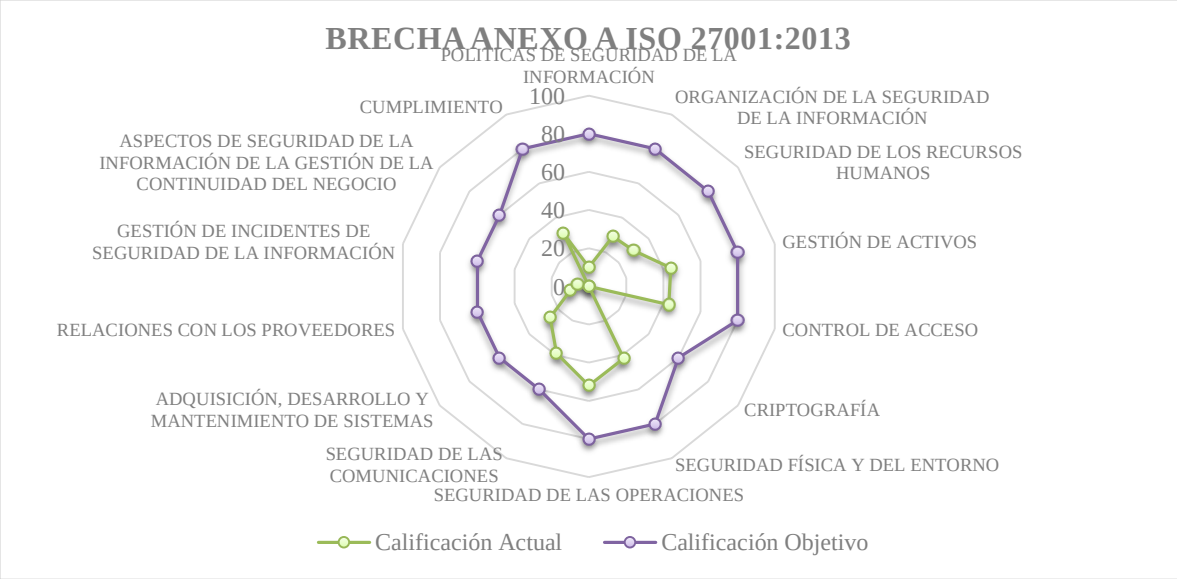
Basado en esta valoración, se promedia los valores por grupo de dominio, obteniendo una evaluación de efectividad del control y un valor promedio general del estado actual frente a lo esperado:

Tabla 3. Evaluación de Efectividad de controles Actual

No	DOMINIO	Calificación Actual	Calificación Objetivo	Evaluación de efectividad del control actual
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	10	80	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	29	80	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	30	80	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	44	80	EFECTIVO
A.9	CONTROL DE ACCESO	43	80	EFECTIVO
A.10	CRIPTOGRAFÍA	0	60	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	42	80	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	52	80	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	39	60	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	26	60	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	10	60	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	6	60	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	60	INEXISTENTE
A.18	CUMPLIMIENTO	31	80	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**26**	**71**	**REPETIBLE**

Fuente: Los autores

Gráfico 1. Brecha Anexo A ISO 27001:2013



Fuente: Los autores

Se realiza análisis de la brecha y se establece que la ESE se encuentra en un estado Inicial REPETIBLE y en el nivel de madurez se encuentra en estado INTERMEDIO; en donde se cuenta con procesos y los controles básicos de gestión de seguridad que siguen un patrón regular, éstos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas, sin embargo, estos no se encuentran documentados o están desactualizados. Existe un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente de planificación del SGSI.

No se cuenta con una metodología de Gestión de Riesgos aplicada a la Seguridad de la Información, que permita detectar el grado de criticidad de la información, por lo tanto, solo algunos controles están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información.

8. IDENTIFICACION DE ACTIVOS

En esta etapa se realiza la enumeración de una serie de activos de la entidad, los cuales se agruparon según el tipo al que corresponden según MAGERIT.

8.1 ACTIVOS DATOS / INFORMACION

Agrupa los activos referentes a los soportes físicos y digitales usados dentro de la empresa para el desarrollo de las actividades diarias de los usuarios.

- ***Información física*:** es toda la información física de gestión documental que se almacena en la oficina, estos documentos son impresos y en papel, entre ellos tenemos comunicaciones internas, evidencias de soporte de capacitación, formatos de solicitud de creación – inactivación de usuarios, oficio remisión de información de bases de datos de afiliados.
- ***Información Digital:*** Aquí se contiene toda la documentación de manera digital de las copias de seguridad tanto de servidores, bases de datos y de usuarios; archivos de ofimática, escaneos.
- ***Base de Datos:*** Almacenamiento de los datos de la organización que ha sido registrada en los diferentes aplicativos institucionales, contamos con SQL Server, MySQL, PostgreSQL.
- ***Código fuente de aplicaciones:*** Algunas aplicaciones han sido desarrolladas a la medida por la institución entre ellas Audihuem, Visitantes, Antimicrobianos, Inventario documental, Contratación, solicitud de citas web.

8.2 SERVICIOS

Función que satisface una necesidad de los usuarios (del servicio). Contempla servicios prestados por el sistema

- Acceso a internet
- Correo electrónico
- Almacenamiento de copias de seguridad se realiza de manera local y en la nube

8.3 ACTIVOS DE SOFTWARE – APLICACIONES INFORMATICAS

Agrupa los activos referentes a los programas o aplicativos usados dentro de la empresa para el desarrollo de las actividades diarias de los usuarios.

- ***Sistemas Operativos*:** es un software base que permite administrar los recursos del equipo, archivos y tareas. Además, ofrece al usuario una interfaz gráfica sencilla para la comunicación con el computador y así realizar sus tareas.
- ***SQL Server 2008 R2:*** Es un manejador de base de Datos bajo un modelo relacional creado por Microsoft. La información está contenida dentro de tablas las cuales guardan relaciones entre sí, respetando el principio de integridad y garantiza que no existe duplicidad de información.
- ***PostgreSQL***: Es un manejador de bases de datos libre.
- ***MySQL***: Manejador de bases de datos libre.
- ***Vmware***: Software de virtualización de máquinas.
- ***Dinámica Gerencial Hospitalaria – DGH .NET:*** Es un software integrado al sector salud, compuesto por módulos que integran las áreas administrativas y las asistenciales. Fue donado por el Ministerio de Salud en el año 2000. Entre los módulos administrativos y financieros contamos con Contabilidad, Información financiera NIIF, Tesorería, Cartera, Pagos, Presupuestos oficiales, Nómina – Talento Humano, Activos fijos, Gestión gerencial y generales. De los módulos operativos - asistenciales tenemos: Inventarios, contratos, citas médicas, admisiones, hospitalización, facturación, historias clínicas, laboratorio, programación de cirugías, entre otros. Actualmente cuenta con301 reportes generados personalizados de acuerdo a solicitudes de los usuarios para llevar controles en cada una de las áreas del HUEM, adicionales a los que vienen pre-diseñados en la aplicación. Cuenta en algunos módulos con tableros de control, permitiendo hacer seguimientos a la actividad registrada en el software.
- ***SIEP Documental***: es un software web de Gestión Documental y de Procesos, que permite gestionar electrónicamente la producción, el trámite, el almacenamiento digital y la recuperación de documentos, evitando el manejo de papel, garantizando la seguridad de la información y la trazabilidad de cualquier proceso que se implemente mediante su funcionalidad.
- ***Contratación***: Es un software web de Gestión de la Contratación de Bienes y servicios, que previa verificación de acceso, permite realizar registro de la actividad contractual de la ESE HUEM, así como adjuntar documentos que sirven de soporte en estas actuaciones. Cuenta con reportes de control para realizar seguimiento a las carpetas contractuales.
- ***Aplicativo de Inventario Único Documental – Ley General De Archivos:*** Es un software web en el que se realiza el registro en línea del Inventario Único Documental, que es un Instrumento de recuperación de información que describe de manera exacta y precisa las series o asuntos de un fondo documental.

- ***Contratación electrónica***: en aras de garantizar la transparencia en la contratación, usa la herramienta de Contratación electrónica BIONEXO, a través de las modalidades de contratación electrónica o subasta electrónica.
- ***Plataforma E-Learning:*** Esta herramienta de aprendizaje aprovecha el uso de la tecnología para proporcionar un ambiente de aprendizaje virtual, en el que los usuarios, funcionarios y público en general pueden adquirir o profundizar conocimientos realizando capacitaciones asincrónicas, teniendo la gran ventaja de aprovechar el tiempo libre, sin importar horarios.
- ***Antivirus:*** Mecanismos de protección que ayudan a detectar y eliminar amenazas informáticas que desestabilizan el funcionamiento de los equipos.
- ***Ofimática:*** herramientas informáticas utilizadas para optimizar y mejorar tareas y procedimientos. Las más conocidas son el paquete de Microsoft Office y Open Office.
- ***Skype:*** Software gratuito utilizado para comunicarse en línea por medio de chat con otras personas, compartir archivos y realizar conferencias integrando video si se desea.
- ***Navegadores:*** Software que permite visualizar la información contenida en las páginas web, puede estar alojada en un servidor web o en un servidor local.

8.4 ACTIVOS DE HARDWARE

El hardware de cómputo provee el fundamento físico básico para el desarrollo TI de la empresa, son los medios físicos destinados a dar soporte de los servicios que presta la oficina de TICS

- ***Servidores***: Corresponde a equipos con gran capacidad de procesamiento y almacenamiento de datos, en ellos se encuentra centraliza la información almacenada por los diferentes aplicativos usados en la empresa y la ejecución de los mismos.
- ***PC de escritorio***: es una computadora personal cuya característica principal frente a los demás ordenadores es que está diseñada para ser instalada en una ubicación fija como un escritorio.
- ***Equipos móviles*** (PORTATILES): corresponde a equipos de cómputo con procesamiento de información que puede ser transportada a diferentes ubicaciones dentro de la entidad o fuera de ella.
- ***SAN:*** Arreglo de discos duros en donde se almacena la información de la institución
- Impresoras
- Scanner

- Discos duros externos
- ***Router***: Es un dispositivo enrutador que proporciona conectividad a nivel de red y a su vez proporciona las IP.
- ***Switch***: También conocido como conmutador es un dispositivo de interconexión de redes informáticas.
- ***Access point:*** punto de acceso inalámbrico (en inglés: Wireless Access Point, conocido por las siglas WAP o AP), en una red de computadoras, es un dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas.

8.5 ACTIVOS DE REDES Y COMUNICACIONES

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

- ***Red local:*** Hace referencia a la interconexión que se realiza usando cable UTP, fibra óptica para transportar datos a través de la red de la entidad y hacia el exterior.
- ***Red inalámbrica:*** Designa la conexión a la red que se realiza a través de ondas electromagnéticas.
- ***Canal dedicado para internet:*** desde la antena de comunicación a través de fibra óptica llega el servicio de internet al Fortinet.

8.6 EQUIPAMIENTO AUXILIAR

Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con los datos:

- Sistema de alimentación ininterrumpida
- Equipos de climatización
- Sistema de energía eléctrica

8.7 INSTALACIONES

Lugares donde se hospedan los sistemas de información y comunicaciones:

- Central de datos
- Centrales de cableado

8.8 ACTIVOS DE PERSONAL

Personas relacionadas con los sistemas de información:

- Usuarios internos
- Usuarios externos
- Administrador de sistemas
- Programador
- Ingenieros y técnicos de soporte
- ***Proveedores de impresoras***: Hace referencia a las Empresas que proveen el hardware necesario para la funcionalidad de los equipos informáticos.
- ***Proveedores de software****:* Empresa que provee los programas lógicos necesarios para el funcionamiento de la empresa.

9. INVENTARIO DE ACTIVOS DE LA ENTIDAD

Tabla 4. Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
DA001	Información Física	Datos	Información de historias clínicas de pacientes, tramites de comunicados y peticiones del publico	Planta física de Sede entidad	Coordinador TI, Gerente, Usuarios	
DA002	Información Digital	Datos	Es toda la información contenida en dispositivos de almacenamiento, Backup y PC de usuarios.	Oficina de Sistemas	Coordinador TI, Gerente, Usuarios	
DA003	Bases de datos afiliados	Datos	Información de afiliación de pacientes.	Oficina de Sistemas	Coordinador TI, Usuarios	
DA004	Bases de datos DNS	Datos	Información relevante categorizada en el área de datos, maneja los listados de los DNS	Rack Principal oficina de sistemas	Coordinador TI	
DA005	Bases de datos DGH	Datos	Base de datos de información registrada en el software DGH.	Oficina de Sistemas	Coordinador TI, Usuarios	
DA006	Base de datos Registro de correspondencia	Datos	Base de datos de inf. registrada de la correspondencia (entradas, salidas) Siepdocumental	Oficina de Sistemas	Técnico gestión documental, Usuarios	
DA007	Base de datos contratación	Datos	Base de datos de información y registros de contratación de Bienes y servicios.	Oficina de Sistemas	Coordinador TI, Usuarios	
DA008	Cuentas de correo electrónico	Datos	Información de cuentas de correo electrónico y almacenamiento de mensajes.	Oficina de Sistemas	Coordinador TI, Usuarios	
SER001	Acceso a internet	Servicios	Servicio que proporciona el acceso a consulta e intercambio de información internet.	N/A	Coordinador TI	N/A
SER002	Correo electrónico	Servicios	Servicio que proporciona la	N/A	Coordinador TI	N/A

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
			recepción y envío de mensajes entre usuarios.			
SER003	Hosting del sitio web	Servicios	Almacenamiento del sitio web institucional y la intranet que permite la consulta de información a través de la WWW.	N/A	Coordinador TI	N/A
SER004	Almacenamiento de copias de seguridad se realiza de manera local y en la nube	Servicios	Respaldo de copias de seguridad e históricos.	N/A	Coordinador TI	N/A
SW001	Sistemas Operativos	Software	Gestionar recursos de hardware	Oficina de Sistemas	Coordinador de TI	3
SW002	SQL Server 2008R2	Software	Gestionar Base de Datos de Ventas, compras, clientes, inventario, precios.	Rack Principal oficina de sistemas	Coordinador de TI	1
SW003	PostgreSQL	Software	Gestionar Base de Datos de SiepDocumental (gestión documental)	Rack Principal oficina de sistemas	Coordinador de TI	1
SW004	MySQL	Software	Gestionar Bases de datos de contratación e inventario único documental	Rack Principal oficina de sistemas	Coordinador de TI	1
SW005	Vmware	Software	Software para virtualización de servidores	Rack Principal oficina de sistemas	Coordinador de TI	1
SW006	Dinámica Gerencial Hospitalaria – DGH.NET	Software	Sistema de información para la gestión de la organización	Rack Principal oficina de sistemas	Coordinador de TI	1
SW007	SIEP Documental	Software	Software para manejo y control del archivo documental	Rack Principal oficina de sistemas	Coordinador de TI	1

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
SW008	Contratación	Software	Software para manejo de los contratos de la clínica	Rack Principal oficina de sistemas	Coordinador de TI	1
SW009	Aplicativo Inventario Único Documental	Software	Software para clasificación de tipos documentales	Rack Principal oficina de sistemas	Coordinador de TI	1
SW010	Contratación Electrónica	Software	Software para subasta de oferentes	Se ingresa a través del link de bionexo		1
SW011	Plataforma E-learning	Software	Software para realización de cursos de interés hospitalario	Rack Principal oficina de sistemas	Coordinador de TI	1
SW012	Antivirus	Software	Detección y Prevención de Amenazas	Rack Principal oficina de sistemas	Coordinador de TI	1
SW013	Ofimática	Software	Realizar y organizar tareas administrativas	Rack Principal oficina de sistemas	Coordinador de TI	2
SW014	Spark	Software	Chat interno en Línea entre usuarios	Rack Principal oficina de sistemas	Coordinador de TI	1
SW015	Navegadores	Software	Subir información a plataformas web. Consulta de derechos de afiliados. Descarga de información de interés	Rack Principal oficina de sistemas	Coordinador de TI	3
HW001	Servidor principal (EVANS)	Hardware	Servidor de base de datos y de la aplicación	Informática	Coordinador TI	1
HW002	Servidor de archivos (CEGDOC)	Hardware	almacenamiento de carpetas compartidas por usuarios	Informática	Coordinador TI	1
HW003	Servidor de Dominio (MSCD1)	Hardware	Servidor de Terminal services y DNS.	Informática	Coordinador TI	1

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
HW004	SAN HP	Hardware	Arreglo de discos duros en donde se almacena la información de la institución	Rack Principal oficina de sistemas	Coordinador TI	1
HW005	FORTIGATE 300C	Hardware	Proteger las redes empresariales de ataques, spam, y otros peligros informáticos.	Rack Principal oficina de sistemas	Coordinador TI	1
HW006	PC Control Interno de gestión	Hardware	Acceso para consulta de información. Generación de documentos.	Control Interno	Asesor de control interno	5
HW007	PC Revisoría Fiscal	Hardware	Acceso para consulta de información. Generación de documentos.	Revisoría	Revisor fiscal	3
HW008	PC Gerencia	Hardware	Acceso para consulta de información. Generación de documentos.	Gerencia	Gerente	3
HW009	Portátil Gerencia	Hardware	Acceso para consulta de información. Generación de documentos.	Gerencia	Gerente	2
HW010	PC Jurídica administrativa	Hardware	Acceso para consulta de información. Generación de documentos.	Jurídica administrativa	Abogado administrativo	4
HW011	PC Jurídica laboral	Hardware	Acceso para consulta de información. Generación de documentos.	Jurídica laboral	Abogado laboral	2
HW012	PC gabys	Hardware	Acceso para consulta de información. Generación de documentos. Montaje de información a plataformas de control.	GABYS	Abogado GABYS	10
HW013	PC PLANEACION	Hardware	Acceso para consulta de información. Generación de documentos.	Planeación	Asesor de planeación y calidad	13

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
HW014	PORTATIL PLANEACION	Hardware	Acceso para consulta de información. Generación de documentos.	Planeación	Asesor de planeación y calidad	3
HW015	PC SISTEMAS	Hardware	Acceso a la aplicación para consulta de información. Generación de informes	Informática	Coordinador TI	18
HW016	PORTATIL SISTEMAS	Hardware	Acceso a la aplicación para consulta de información. Generación de informes	Informática	Coordinador TI	2
HW017	PC ESTADISTICA	Hardware	Acceso para consulta de información. Generación de documentos.	Estadística	Asesor de planeación y calidad / Agremiación	18
HW018	PC PRENSA	Hardware	Acceso para consulta de información. Generación de documentos.	Prensa	Asesor de planeación y calidad / Agremiación	5
HW019	PC CEGDOC	Hardware	Acceso para consulta de información. Generación de documentos.	CEGDOC	Asesor de planeación y calidad / Agremiación	5
HW020	PC Subsalud	Hardware	Acceso para consulta de información. Generación de documentos.	Subgerencia de salud	Subgerente de salud	4
HW021	Portátil Subsalud	Hardware	Acceso para consulta de información. Generación de documentos.	Subgerencia de salud	Subgerente de salud	1
HW022	PC Epidemiología	Hardware	Acceso para consulta de información. Generación de documentos.	Epidemiología	Epidemiólogo	9
HW023	Portátil Epidemiología	Hardware	Acceso para consulta de información. Generación de documentos.	Epidemiología	Epidemiólogo	1
HW024	PC Docencia	Hardware	Acceso para consulta de información.	Docencia	Subgerente de salud	2

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
			Generación de documentos.			
HW025	PC SIAU	Hardware	Acceso para consulta de información. Generación de documentos.	SIAU	Coordinador SIAU	6
HW026	PC Medicina interna y especialidades – Piso 7	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 7	Coordinadora medicina interna	5
HW027	PC Medicina interna y especialidades – Piso 10	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 10	Coordinadora medicina interna	1
HW028	PC Medicina interna y especialidades administrativo	Hardware	Acceso para consulta de información. Registro en software institucional. Administrativo. Generación de documentos	Piso 7	Coordinadora medicina interna	3
HW029	Portátil Medicina interna y especialidades	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 7	Coordinadora medicina interna	1
HW030	PC Pediatría	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 3	Coordinador Pediatría	9
HW031	PC Pediatría administrativo	Hardware	Acceso para consulta de información. Registro en software institucional. Administrativo. Generación de documentos	Piso 3	Coordinador Pediatría	3
HW032	Portátil Pediatría	Hardware	Acceso para consulta de información. Registro en software	Piso 3	Coordinador Pediatría	1

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
			institucional. Historias clínicas			
HW033	PC Pediatría quirúrgica	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 4	Coordinador Pediatría	3
HW034	PC Banco de leche	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 3	Coordinador Pediatría	3
HW035	Portátil Madre canguro	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 3	Coordinador Pediatría	3
HW036	PC Sala cuna - Neonatos	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 2	Coordinador Pediatría	5
HW037	PC Cirugía general	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 8	Coordinador Cx general	3
HW038	Portátil Cirugía general	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 8	Coordinador Cx general	2
HW039	PC Endoscopia	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 12	Coordinador Cx general	1
HW040	PC Cirugía general piso 9	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 9	Coordinador Cx general	1
HW041	Portátil Cirugía	Hardware	Acceso para consulta de información.	Piso 9	Coordinador Cx general	2

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
	general piso 9		Registro en software institucional. Historias clínicas			
HW042	PC Neuro	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 6	Coordinador Cx general	1
HW043	Portátil Neuro	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 6	Coordinador Cx general	1
HW044	PC Ginecología -obstetricia	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 5	Coordinador Ginecología	6
HW045	PC Sala de partos	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso2 - Sala de partos	Coordinador Ginecología	10
HW046	PC Consulta externa	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 1 - Consulta externa	Líder servicios ambulatorios	17
HW047	PC Consulta externa administrativo	Hardware	Acceso para consulta de información. Registro en software institucional. Citas médicas	Piso 1 - Consulta externa	Coordinadora Consulta externa	2
HW048	PC Consulta externa - urología	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 11 - Urología	Líder servicios ambulatorios	1
HW049	PC Urgencias adultos y cuidados intermedios	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 1 - Urgencias adultos	Líder servicios ambulatorios	15

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
HW050	PC Urgencias adultos administrativo	Hardware	Acceso para consulta de información. Registro en software institucional. Administrativo. Generación de documentos	Piso 1 - Urgencias adultos	Líder servicios ambulatorios	3
HW051	PC Urgencias pediatría	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 1 - Urgencias pediatría	Líder servicios ambulatorios	9
HW052	PC Referencia	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 1 - Entrada urgencias	Coordinador referencia	4
HW053	PC Quirófanos	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 2 - Quirófanos	Líder servicios quirúrgicos	4
HW054	PC Quirófanos - Administrativo	Hardware	Acceso para consulta de información. Registro en software institucional. Generación de documentos	Piso 2	Líder servicios quirúrgicos	2
HW055	PC Esterilización	Hardware	Acceso para consulta de información. Registro en software institucional. Generación de documentos	Piso 2	Coordinador esterilización	2
HW056	PC Apoyo a la atención	Hardware	Acceso para consulta de información. Registro en software institucional. Generación de documentos	Piso 2	Líder de apoyo a la atención	2
HW057	PC Radiología	Hardware	Acceso para consulta de información. Registro en software	Piso 1	Coordinador imagenología	7

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
			institucional. Historias clínicas			
HW058	PC Ecografía	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas	Piso 1	Coordinador imagenología	2
HW059	PC Laboratorio clínico	Hardware	Acceso para consulta de información. Registro en software institucional. Registro datos laboratorio	Piso 1	Coordinador laboratorio	2
HW060	PC Banco de sangre	Hardware	Acceso para consulta de información. Registro en software institucional. Registro datos banco de sangre	Piso 1	Coordinador banco de sangre	3
HW061	PC Patología	Hardware	Acceso para consulta de información. Registro en software institucional. Patología	Piso 1	Coordinador imagenología	5
HW062	PC Radioterapia	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas. Generación de documentos	Piso 1	Coordinador Radioterapia	10
HW063	PC Rehabilitación	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas. Generación de documentos	Piso 1	Coordinador Rehabilitación	5
HW064	PC Farmacia administrativo	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas - Inventarios. Generación de documentos	Piso 1	Coordinador de Farmacia	2
HW065	PC Farmacia principal	Hardware	Acceso para consulta de información. Registro en software institucional. Historias	Piso 1	Coordinador de Farmacia	2

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
			clínicas - Inventarios. Generación de documentos			
HW066	PC Farmacia 2piso	Hardware	Acceso para consulta de información. Registro en software institucional. Historias clínicas - Inventarios. Generación de documentos	Piso 2	Coordinador de Farmacia	5
HW067	PC Coordinación de enfermería	Hardware	Acceso para consulta de información. Generación de documentos	Piso 8	Coordinador de Farmacia	4
HW068	PC Nutrición	Hardware	Acceso para consulta de información. Generación de documentos	Piso 1	Coordinador de Nutrición	4
HW069	PC Subgerencia administrativa	Hardware	Acceso para consulta de información. Registro en software institucional. Generación de documentos	Piso 1	Subgerente administrativo	7
HW070	Portátil Subgerencia administrativa	Hardware	Acceso para consulta de información. Registro en software institucional. Generación de documentos	Piso 1	Subgerente administrativo	1
HW071	PC Financiera	Hardware	Acceso para consulta de información. Registro en software institucional. Módulos administrativos. Generación de documentos	Piso 1	Líder Financiero	17
HW072	PC Facturación	Hardware	Acceso para consulta de información. Registro en software institucional. Módulos administrativos y consulta de módulos asistenciales.	Piso 1	Coordinador facturación	43

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
			Generación de documentos			
HW073	PC Cartera - Auditoría de cuentas	Hardware	Acceso para consulta de información. Registro en software institucional. Módulos administrativos y consulta de módulos asistenciales. Generación de documentos	Piso 1	Coordinador facturación	22
HW074	PC Contratación y mercadeo	Hardware	Acceso para consulta de información. Registro en software institucional. Módulos administrativos. Generación de documentos	Piso 1	Coordinador Contratación	3
HW075	PC Talento humano	Hardware	Acceso para consulta de información. Módulos administrativos. Generación de documentos	Piso 1	Líder de talento humano	17
HW076	PC Nómina	Hardware	Acceso para consulta de información. Registro en software institucional. Módulos administrativos. Generación de documentos	Piso 1	Líder de talento humano	6
HW077	PC Recursos físicos	Hardware	Acceso para consulta de información. Registro en software institucional. Módulos administrativos. Generación de documentos	Piso 1	Líder de Recursos físicos	5
HW078	PC Almacén	Hardware	Acceso para consulta de información. Registro en software institucional. Módulos administrativos.	Piso 1	Almacenista	4

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
			Generación de documentos			
HW079	PC Biomedicina	Hardware	Acceso para consulta de información. Registro en software institucional. Módulos administrativos. Generación de documentos	Piso 1	Ing. Biomédico	4
HW080	PC Mantenimiento	Hardware	Acceso para consulta de información. Registro en software institucional. Módulos administrativos. Generación de documentos	Piso 1	Coordinador mantenimiento	2
RED001	CORE	Red	Dispositivo central de red, al que se interconectan los demás dispositivos para contar con una topología tipo estrella.	DATACENTER	Coordinador TI	1
RED002	SW SERVIDORES	Red	Dispositivo de red que permite la interconexión entre servidores y data storage.	DATACENTER	Coordinador TI	1
RED003	SW URG_ADULTOS	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED004	SW URG_PEDIATRIA	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED005	SW RAYOSX	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED006	SW BANCO_DE_SANGRE	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED007	SW LABORATORIO	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
RED008	SW ESTADISTICA	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED009	SW CONTABILIDAD1	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED010	SW CONTABILIDAD2	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED011	SW VIGILANCIA	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED012	SW CARTERA	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED013	SW ALMACEN1	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED014	SW ALMACEN2	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED015	SW MANTENIMIENTO	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED016	SW RADIOTERAPIA	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED017	SW CENTRAL	Red	Dispositivo de red que da conectividad al área.	PISO 1	Coordinador TI	1
RED018	SW PISO3	Red	Dispositivo de red que da conectividad al área.	PISO 3	Coordinador TI	1
RED019	SW PISO5	Red	Dispositivo de red que da conectividad al área.	PISO 5	Coordinador TI	1
RED020	SW PISO6	Red	Dispositivo de red que da conectividad al área.	PISO 6	Coordinador TI	1
RED021	SW PISO7	Red	Dispositivo de red que da conectividad al área.	PISO 7	Coordinador TI	1

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
RED022	SW PISO8	Red	Dispositivo de red que da conectividad al área.	PISO 8	Coordinador TI	1
RED023	SW PISO9	Red	Dispositivo de red que da conectividad al área.	PISO 9	Coordinador TI	1
RED024	SW PISO9-2	Red	Dispositivo de red que da conectividad al área.	PISO9	Coordinador TI	1
RED025	SW PISO10	Red	Dispositivo de red que da conectividad al área.	PISO 10	Coordinador TI	1
RED026	SW PISO11	Red	Dispositivo de red que da conectividad al área.	PISO 11	Coordinador TI	1
RED027	SW PISO12	Red	Dispositivo de red que da conectividad al área.	PISO 12	Coordinador TI	1
RED028	ACCES POINT INALAMBRICO	Red	Interconexión de Equipos a través de WIFI	Pisos	Coordinador TI	10
EQ001	Equipos de climatización - Aire acondicionado	Equipamiento auxiliar	Regulación de temperatura de equipos informáticos	Piso 2 - Sala de servidores	Coordinador TI	1
EQ002	UPS Servidores	Equipamiento auxiliar	Sistema de energía de soporte en caso de fallas.	Piso 2 - Sala de servidores	Coordinador TI	2
EQ003	UPS Switches	Equipamiento auxiliar	Sistema de energía de soporte en caso de fallas.	Centrales de cableado	Coordinador TI	20
EQ004	Sistema de energía eléctrica	Equipamiento auxiliar	Alimentación de energía eléctrica.	Piso 1	Coord.mantenimiento	
EQ005	Sistema de energía eléctrica de emergencia	Equipamiento auxiliar	Alimentación de electricidad en caso de falla o de pérdida de la continuidad de la prestación del servicio.	Piso 1	Coordinador mantenimiento	N/A
INS001	Central de datos	Instalaciones	Lugares donde se hospedan los sistemas	Piso 2 - Sistemas	Coordinador TI	1

Continuación Tabla 4 Inventario activos del Hospital Universitario Erasmo Meoz

Código activo	Nombre de activo	Tipo de Activo	Función (características del equipo)	Ubicación	Propietario / custodio	cantidad
			de información y comunicaciones			
INS002	Centrales de cableado	Instalaciones	Lugares donde se hospedan los dispositivos de comunicaciones	Pisos	Coordinador TI	8
PER001	Usuarios internos	Personal	Persona que interactúa con los sistemas de información	N/A	N/A	N/A
PER002	Usuarios externos	Personal	Persona que requiere información del sistema	N/A	N/A	N/A
PER003	Administrador de sistemas	Personal	Persona que administra y vela por el buen funcionamiento del sistema	N/A	N/A	N/A
PER004	Ingeniero de sistemas	Personal	Persona que apoya la administración y es generador de informes	N/A	N/A	6
PER005	Técnicos de soporte	Personal	Persona que apoya la administración en lo referente a actividades técnicas de hardware y redes	N/A	N/A	6
PER006	Proveedores de impresoras	Personal	Contratista que tiene bajo su administración las impresoras de la institución	N/A	N/A	1
PER007	Proveedores de software	Personal	Dueño de la aplicación que realiza ajustes y mejoras en la misma, a través de solicitudes que se realizan en el centro de soporte en línea.	N/A	N/A	1

Fuente: Los autores

10. DIMENSIONES DE VALORACIÓN

Las dimensiones a tener en cuenta para la valoración de los activos fijos, serán las definidas por las características de la información:

10.1 DISPONIBILIDAD [D]

¿Qué importancia tiene un activo sino estuviera disponible? Tendría un valor alto si la no disponibilidad del activo trajera consecuencias graves; por el contrario, sería bajo si puede estar no disponible por un período largo.

10.2 INTEGRIDAD [I]

¿Qué importancia tiene el activo si los datos fueran modificados fuera de control? Tendrá una valoración alta si su modificación, de forma involuntaria o intencionada, trajera graves daños a la empresa. De igual manera, supone una valoración baja si su alteración no supone preocupación alguna.

10.3 CONFIDENCIALIDAD [C]

¿Qué importancia tendría el activo si fuera conocido por personas no autorizadas? Tendrá una valoración alta si su revelación trae consecuencias graves para la organización, o una valoración baja si su divulgación no reviste preocupación alguna.

10.4 AUTENTICIDAD [A]

¿Qué importancia tiene el activo si quien accede a él no es realmente quien se cree que es? De esta manera un activo tendría una elevada valoración cuando su prestación se realice a falsos usuarios supondría un grave perjuicio para la organización, o una valoración inferior si su acceso no reviste importancia para la compañía.

10.5 TRAZABILIDAD [T]

¿Qué importancia tiene el activo si no queda constancia del uso del mismo? Si no existe registro podría realizarse un fraude, imposibilitando el seguimiento a un delito y suponer el incumplimiento de obligaciones legales.

Estas dimensiones de activos son evaluadas por medio de una escala de valores ya sea con un análisis cualitativo o cuantitativo:

- El análisis cualitativo es una medición de activos, por medio de niveles de importancia. Por ejemplo: nivel bajo, nivel medio y nivel alto
- El análisis cuantitativo: Medición de activos por medio de escala numérica. Por ejemplo: valorar de 1 a 10, donde 10 es la calificación más alta.

Para el caso de los activos de la ESE HOSPITAL UNIVERSITARIO ERASMO MEOZ, se utiliza el análisis cuantitativo y cualitativo reflejado así:

Tabla 5. Valoración activos

VALORACION		CRITERIO
10	EXTREMO	DAÑO EXTREMADAMENTE GRAVE
9	MUY ALTO	DAÑO MUY GRAVE
6 A 8	ALTO	DAÑO GRAVE
3 A 5	MEDIO	DAÑO IMPORTANTE
1 A 2	BAJO	DAÑO MENOR
0	DESPRECIABLE	IRRELEVANTE A EFECTOS PRÁCTICOS

Fuente: Los autores

11. VALORACION DE ACTIVOS

A continuación, se evalúa los activos de la entidad con respecto a las dimensiones correspondientes a la integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad, bajo los criterios establecidos anteriormente (ver Tabla 4 – Valoración de activos); para valorar las consecuencias de la materialización de una amenaza, que corresponde a la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

En la tabla 6 – Valoración de activos, se cuenta con un valor cuantitativo y un valor cualitativo que se genera del promedio de la valoración en cada una de sus dimensiones.

Tabla 6. Valoración de activos - Estimación del impacto

TIPO DE ACTIVO	ACTIVO	VALORACIÓN DIMENSIONES					VALORACION CUANTITATIVA	VALORACIÓN CUALITATIVA
		D	I	C	A	T		
Datos	Información Física	10	10	10	10	10	**10**	**Extremo**
Datos	Información Digital	10	10	10	10	10	**10**	**Extremo**
Datos	Bases de datos afiliados	5	9	8	10	10	**8**	**Alto**
Datos	Bases de datos DNS	10	9	9	10	10	**10**	**Extremo**
Datos	Bases de datos DGH	10	10	10	10	10	**10**	**Extremo**
Datos	Base de datos Registro de correspondencia	8	9	9	9	8	**9**	**Muy alto**
Datos	Base de datos contratación	8	9	10	8	8	**9**	**Muy alto**
Datos	Cuentas de correo electrónico	8	9	8	10	10	**9**	**Muy alto**
Servicios	Acceso a internet	10	6	5	8	8	**7**	**Alto**
Servicios	Correo electrónico	9	9	9	10	10	**9**	**Muy alto**
Servicios	Hosting del sitio web	8	10	8	9	9	**9**	**Muy alto**
Servicios	Almacenamiento de copias de seguridad se realiza de manera local y en la nube	8	10	10	10	10	**10**	**Extremo**
Software	Sistemas Operativos	9	5	2	2	2	**4**	**Medio**
Software	SQL Server 2008R2	10	10	10	10	10	**10**	**Extremo**
Software	PostgreSQL	8	10	10	10	10	**10**	**Extremo**
Software	MySQL	8	10	10	10	10	**10**	**Extremo**
Software	Vmware	10	10	9	10	10	**10**	**Extremo**
Software	Dinámica Gerencial Hospitalaria – DGH.NET	10	10	10	10	10	**10**	**Extremo**
Software	SIEP Documental	9	10	9	10	9	**9**	**Muy alto**
Software	Contratación	8	10	9	9	9	**9**	**Muy alto**
Software	Aplicativo Inventario Único Documental	2	7	8	7	6	**6**	**Alto**
Software	Contratación Electrónica	8	10	10	10	10	**10**	**Extremo**
Software	Plataforma E-learning	3	5	5	9	5	**5**	**Medio**
Software	Antivirus	8	9	9	8	8	**8**	**Alto**
Software	Ofimática	8	5	5	5	2	**5**	**Medio**
Software	Spark	4	6	6	8	8	**6**	**Alto**

Continuación Tabla 6 Valoración de activos - Estimación del impacto

TIPO DE ACTIVO	ACTIVO	VALORACIÓN DIMENSIONES					VALORACION CUANTITATIVA	VALORACIÓN CUALITATIVA
		D	I	C	A	T		
Software	Navegadores	9	8	9	8	8	**8**	**Alto**
Hardware	Servidor principal (EVANS)	10	10	10	10	10	**10**	**Extremo**
Hardware	Servidor de archivos (CEGDOC)	10	10	8	9	9	**9**	**Muy alto**
Hardware	Servidor de Dominio (MSCD1)	10	10	10	10	10	**10**	**Extremo**
Hardware	SAN HP	10	10	10	10	10	**10**	**Extremo**
Hardware	FORTIGATE 300C	9	9	9	9	9	**9**	**Muy alto**
Hardware	PC Control Interno de gestión	8	9	8	8	6	**8**	**Alto**
Hardware	PC Revisoría Fiscal	8	9	8	8	6	**8**	**Alto**
Hardware	PC Gerencia	9	9	10	8	6	**8**	**Alto**
Hardware	Portátil Gerencia	6	8	9	8	6	**7**	**Alto**
Hardware	PC Jurídica administrativa	9	10	10	8	8	**9**	**Muy alto**
Hardware	PC Jurídica laboral	8	10	10	8	8	**9**	**Muy alto**
Hardware	PC GABYS	9	10	10	8	8	**9**	**Muy alto**
Hardware	PC PLANEACION	8	9	10	9	8	**9**	**Muy alto**
Hardware	PORTATIL PLANEACION	1	1	6	2	2	**2**	**Bajo**
Hardware	PC SISTEMAS	8	10	10	9	8	**9**	**Muy alto**
Hardware	PORTATIL SISTEMAS	1	1	6	2	2	**2**	**Bajo**
Hardware	PC ESTADISTICA	8	9	8	8	8	**8**	**Alto**
Hardware	PC PRENSA	5	9	9	8	8	**8**	**Alto**
Hardware	PC CEGDOC	9	9	9	8	6	**8**	**Alto**
Hardware	PC Subsalud	6	9	10	9	8	**8**	**Alto**
Hardware	Portátil Subsalud	5	2	2	2	2	**3**	**Medio**
Hardware	PC Epidemiología	9	10	9	7	5	**8**	**Alto**
Hardware	Portátil Epidemiología	5	2	2	2	2	**3**	**Medio**
Hardware	Pc Docencia	8	8	8	8	8	**8**	**Alto**
Hardware	PC SIAU	8	9	8	8	6	**8**	**Alto**
Hardware	PC Medicina interna y especialidades - Piso 7	5	6	8	9	8	**7**	**Alto**
Hardware	PC Medicina interna y especialidades - Piso 10	5	6	8	9	8	**7**	**Alto**
Hardware	PC Medicina interna y especialidades administrativo	7	9	8	8	6	**8**	**Alto**
Hardware	Portátil Medicina interna y especialidades	5	6	8	9	8	**7**	**Alto**
Hardware	PC Pediatría	5	6	8	9	8	**7**	**Alto**
Hardware	PC Pediatría administrativo	7	9	8	8	6	**8**	**Alto**
Hardware	Portátil Pediatría	5	6	8	9	8	**7**	**Alto**
Hardware	PC Pediatría quirúrgica	5	6	8	9	8	**7**	**Alto**
Hardware	PC Banco de leche	5	6	8	9	8	**7**	**Alto**
Hardware	Portátil Madre canguro	5	6	8	9	8	**7**	**Alto**
Hardware	PC Sala cuna - Neonatos	5	6	8	9	8	**7**	**Alto**
Hardware	PC Cirugía general	5	6	8	9	8	**7**	**Alto**
Hardware	Portátil Cirugía general	5	6	8	9	8	**7**	**Alto**
Hardware	PC Endoscopia	5	6	8	9	8	**7**	**Alto**
Hardware	PC Cirugía general piso 9	5	6	8	9	8	**7**	**Alto**
Hardware	Portátil Cirugía general piso 9	5	6	8	9	8	**7**	**Alto**
Hardware	PC Neuro	5	6	8	9	8	**7**	**Alto**

Continuación Tabla 6 Valoración de activos - Estimación del impacto

TIPO DE ACTIVO	ACTIVO	VALORACIÓN DIMENSIONES					VALORACION CUANTITATIVA	VALORACIÓN CUALITATIVA
		D	I	C	A	T		
Hardware	Portátil Neuro	5	6	8	9	8	**7**	**Alto**
Hardware	PC Ginecología-obstetricia	5	6	8	9	8	**7**	**Alto**
Hardware	PC Sala de partos	5	6	8	9	8	**7**	**Alto**
Hardware	PC Consulta externa	6	6	8	9	8	**7**	**Alto**
Hardware	PC Consulta externa administrativo	8	9	10	9	8	**9**	**Muy alto**
Hardware	PC Consulta externa - urología	6	6	8	9	8	**7**	**Alto**
Hardware	PC Urgencias adultos y cuidados intermedios	8	6	8	9	8	**8**	**Alto**
Hardware	PC Urgencias adultos administrativo	8	9	10	9	8	**9**	**Muy alto**
Hardware	PC Urgencias pediatría	8	6	8	9	8	**8**	**Alto**
Hardware	PC Referencia	6	6	8	9	8	**7**	**Alto**
Hardware	PC Quirófanos	5	5	7	9	7	**7**	**Alto**
Hardware	PC Quirófanos - Administrativo	5	9	10	9	8	**8**	**Alto**
Hardware	PC Esterilización	5	6	8	9	8	**7**	**Alto**
Hardware	PC Apoyo a la atención	8	9	10	9	8	**9**	**Muy alto**
Hardware	PC Radiología	3	5	9	9	8	**7**	**Alto**
Hardware	PC Ecografía	3	5	9	9	8	**7**	**Alto**
Hardware	PC Laboratorio clínico	3	5	9	9	8	**7**	**Alto**
Hardware	PC Banco de sangre	3	5	9	9	8	**7**	**Alto**
Hardware	PC Patología	3	3	7	9	8	**6**	**Alto**
Hardware	PC Radioterapia	5	5	7	9	7	**7**	**Alto**
Hardware	PC Rehabilitación	3	5	7	9	7	**6**	**Alto**
Hardware	PC Farmacia administrativo	3	5	8	8	8	**6**	**Alto**
Hardware	PC Farmacia principal	3	5	8	8	8	**6**	**Alto**
Hardware	PC Farmacia 2piso	3	5	6	8	8	**6**	**Alto**
Hardware	PC Coordinación de enfermería	3	5	9	8	5	**6**	**Alto**
Hardware	PC Nutrición	3	5	6	8	8	**6**	**Alto**
Hardware	PC Subgerencia administrativa	2	8	9	8	8	**7**	**Alto**
Hardware	Portátil Subgerencia administrativa	1	1	6	2	2	**2**	**Bajo**
Hardware	PC Financiera	3	9	9	8	8	**7**	**Alto**
Hardware	PC Facturación	1	2	2	9	8	**4**	**Medio**
Hardware	PC Cartera - Auditoría de cuentas	1	3	9	9	8	**6**	**Alto**
Hardware	PC Contratación y mercadeo	1	3	9	9	5	**5**	**Medio**
Hardware	PC Talento humano	2	3	9	8	5	**5**	**Medio**
Hardware	PC Nómina	2	3	9	8	6	**6**	**Alto**
Hardware	PC Recursos físicos	2	8	8	8	6	**6**	**Alto**
Hardware	PC Almacén	2	8	8	8	6	**6**	**Alto**
Hardware	PC Biomedicina	2	1	8	5	5	**4**	**Medio**
Hardware	PC Mantenimiento	1	1	4	5	5	**3**	**Medio**
Red	CORE	10	8	6	5	4	**7**	**Alto**
Red	SW SERVIDORES	10	8	6	5	4	**7**	**Alto**
Red	SW URG_ADULTOS	9	8	6	5	3	**6**	**Alto**
Red	SW URG_PEDIATRIA	9	8	6	5	3	**6**	**Alto**
Red	SW RAYOSX	9	8	6	5	3	**6**	**Alto**
Red	SW BANCO_DE_SANGRE	7	8	6	5	3	**6**	**Alto**
Red	SW LABORATORIO	7	8	6	5	3	**6**	**Alto**
Red	SW ESTADISTICA	8	8	6	5	3	**6**	**Alto**

Continuación Tabla 6 Valoración de activos - Estimación del impacto

TIPO DE ACTIVO	ACTIVO	VALORACIÓN DIMENSIONES					VALORACION CUANTITATIVA	VALORACIÓN CUALITATIVA
		D	I	C	A	T		
Red	SW CONTABILIDAD1	7	8	5	5	3	**6**	**Alto**
Red	SW CONTABILIDAD2	7	8	5	5	3	**6**	**Alto**
Red	SW VIGILANCIA	7	8	5	5	3	**6**	**Alto**
Red	SW CARTERA	7	8	5	5	3	**6**	**Alto**
Red	SW ALMACEN1	7	8	5	5	3	**6**	**Alto**
Red	SW ALMACEN2	7	8	5	5	3	**6**	**Alto**
Red	SW MANTENIMIENTO	7	8	5	5	3	**6**	**Alto**
Red	SW RADIOTERAPIA	7	8	5	5	3	**6**	**Alto**
Red	SW CENTRAL	7	8	5	5	3	**6**	**Alto**
Red	SW PISO3	5	5	4	3	3	**4**	**Medio**
Red	SW PISO5	5	5	4	3	3	**4**	**Medio**
Red	SW PISO6	5	5	4	3	3	**4**	**Medio**
Red	SW PISO7	5	5	4	3	3	**4**	**Medio**
Red	SW PISO8	5	5	4	3	3	**4**	**Medio**
Red	SW PISO9	5	5	4	3	3	**4**	**Medio**
Red	SW PISO9-2	5	5	4	3	3	**4**	**Medio**
Red	SW PISO10	5	5	4	3	3	**4**	**Medio**
Red	SW PISO11	5	5	4	3	3	**4**	**Medio**
Red	SW PISO12	5	5	4	3	3	**4**	**Medio**
Red	ACCES POINT INALAMBRICO	5	5	4	3	3	**4**	**Medio**
Equipamiento auxiliar	Equipos de climatización - Aire acondicionado	8	1	1	1	1	**2**	**Bajo**
Equipamiento auxiliar	UPS Servidores	6	1	1	1	4	**3**	**Medio**
Equipamiento auxiliar	UPS Switches	6	1	1	1	4	**3**	**Medio**
Equipamiento auxiliar	Sistema de energía eléctrica	10	8	1	1	5	**5**	**Medio**
Equipamiento auxiliar	Sistema de energía eléctrica de emergencia	8	8	1	1	5	**5**	**Medio**
Instalaciones	Central de datos	9	5	7	9	5	**7**	**Alto**
Instalaciones	Centrales de cableado	9	5	7	9	5	**7**	**Alto**
Personal	Usuarios internos	3	3	7	8	8	**6**	**Alto**
Personal	Usuarios externos	3	3	5	8	8	**5**	**Medio**
Personal	Administrador de sistemas	10	8	6	5	3	**6**	**Alto**
Personal	Ingeniero de sistemas	10	8	10	8	4	**8**	**Alto**
Personal	Técnicos de soporte	8	8	8	8	4	**7**	**Alto**
Personal	Proveedores de impresoras	6	2	4	7	7	**5**	**Medio**
Personal	Proveedores de software	6	2	4	7	7	**5**	**Medio**

Fuente: Los autores

De acuerdo a esta valoración, se ratifica el concepto que el activo más importante en la organización es la información, obteniendo un puntaje promedio de 9.3,

seguido del grupo de servicios con una puntuación de 8.75, tal como lo sugiere la metodología Magerit.

12. AMENAZAS

Las amenazas son eventos, circunstancias o personas que pueden causar daño a los activos de la información. Para analizar las amenazas a las que pueden estar expuestos, se tomará como referencia el catálogo de elementos que propone MAGERIT, los pueden ser:

12.1 DESASTRES NATURALES [N]

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta:

- DAÑOS POR FUEGO [N.1]: incendios: posibilidad de que el fuego acabe con recursos del sistema.
- DESASTRES NATURALES [N.*]: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.

12.2 DE ORIGEN INDUSTRIAL [I]

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

- DAÑOS POR FUEGO [I.1]: incendio: posibilidad de que el fuego acabe con los recursos del sistema.
- DAÑOS POR AGUA [I.2]: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
- DESASTRES INDUSTRIALES [I.*]: otros desastres debidos a la actividad humana: explosiones que pueden generarse en el área de calderas o lavandería, sobrecarga eléctrica, fluctuaciones eléctricas.
- CONTAMINACION MECANICA [I.3]: vibraciones, polvo, suciedad.
- CONTAMINACION ELECTROMAGNETICA [I.4]: interferencias de radio, campos magnéticos, luz ultravioleta,
- AVERÍA DE ORIGEN FÍSICO O LOGICO [I.5]: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
- CORTE DE SUMINISTRO ELECTRICO [I.6]: cese de la alimentación de potencia.
- FALLO DE SERVICIOS DE COMUNICACIONES [I.8]: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de

conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

- DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN [I.10] Daño ocasionado por el paso del tiempo

12.3 ERRORES Y FALLO NO INTENCIONADOS [E]

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

- ERRORES DE LOS USUARIOS [E.1]: equivocaciones de las personas cuando usan los servicios, datos, etc.
- ERRORES DEL ADMINISTRADOR [E.2]: equivocaciones de personas con responsabilidades de instalación y operación, introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, etc. Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos.
- DEFICIENCIAS EN LA ORGANIZACIÓN [E.7]: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.
- DIFUSIÓN DE SOFTWARE DAÑINO [E.8]: corresponde a la propagación no intencionada de virus.
- ALTERACIÓN ACCIDENTAL DE LA INFORMACIÓN [E.15]: Cuando sin intención se hace modificación sobre los datos
- DESTRUCCIÓN DE INFORMACIÓN [E.18]: Corresponde a la pérdida accidental de información.
- FUGAS DE INFORMACIÓN [E.19]: Revelación por indiscreción que puede ser de manera verbal, medios electrónicos, papel, u otros medios.
- VULNERABILIDADES DE LOS PROGRAMAS (Software) [E.20]: Defectos o fallas que inciden en la operación no adecuada del software con consecuencias sobre la integridad de los datos o su funcionamiento.
- ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (Software) [E.21]: Fallas sobre los controles de actualización que permitan corregir fallas detectadas en el software.

- ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS (Hardware) [E.23]: Falla en la actualización de hardware que permiten que sigan utilizándose más allá de su obsolescencia.
- CAIDA POR AGOTAMIENTO DE RECURSOS [E.24]: Recursos insuficientes del activo que ocasiona la caída del sistema.
- PÉRDIDA DE EQUIPO [E.25]: Afecta directamente la disponibilidad ya que no se cuenta con el activo para prestar los servicios.
- INDISPONIBILIDAD DEL PERSONAL [E.28]: Falta de personal para el ejercicio de sus funciones.

12.4 ATAQUES INTENCIONADOS

Fallos deliberados causados por las personas, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

- SUPLANTACION DE LA IDENTIDAD DEL USUARIO [A.5]: Refiere a un ataque en el que se consigue pasar por un usuario autorizado.
- ABUSO DE PRIVILEGIOS DE ACCESO [A.6]: Cuando un usuario cuenta con un nivel de privilegios y hace mal uso de éste para realizar tareas que no son de su competencia.
- USO NO PREVISTO [A.7]: Uso de los activos para fines diferentes a los cuales se le fueron asignados, generalmente de interés personal.
- DIFUSION DE SOFTWARE DAÑINO [A.8]: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
- RE-ENCAMINAMIENTO DE MENSAJES [A.9]: Envío de información a un destino que no corresponde a través de un sistema o una red, o forzar la información a llevarse por un camino diferente al establecido.
- ACCESO NO AUTORIZADO [A.11]: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
- MODIFICACIÓN DELIBERADA DE LA INFORMACIÓN [A.11]: Alteración intencional de la información, con la intensión de obtener beneficio o causar daño.
- DESTRUCCION DE LA INFORMACIÓN [A.18]: Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
- DIVULGACIÓN DE INFORMACIÓN [A.19]: Revelación de información clasificada.
- MANIPULACIÓN DE LOS EQUIPOS [A.23]: Alteración intencionada del hardware de los equipos.

- DENEGACIÓN DE SERVICIO [A.24]: Falta de recursos que pueden probar la caída del sistema.
- ROBO [A.25]: Extraer sin consentimiento del propietario algún activo de la información.
- ATAQUE DESTRUCTIVO [A.26]: Ocurrido por vandalismo, terrorismo.
- INDISPONIBILIDAD DEL PERSONAL [A.28]: Ausencia a propósito del puesto de trabajo
- INGENIERÍA SOCIAL (PICARESCA) [A.30]: Abuso de la buena fe para que las personas realicen actividades con beneficio para un tercero.

13. IDENTIFICACION DE AMENAZAS Y VALORACION DE RIESGOS

Las amenazas deben ser valoradas según:

Frecuencia: se mide la probabilidad, el número de veces que ocurre una amenaza sobre un activo en un determinado periodo.
Queda esta

Tabla 7. Valoración de la frecuencia de las amenazas

Frecuencia	Descripción	Valor
Muy Frecuente	Puede ocurrir en una semana	5
Frecuente	Puede ocurrir en un mes	4
Poco Frecuente	Puede ocurrir en el semestre	3
Ocasional	Puede ocurrir en un año	2
Despreciable	Puede ocurrir en más de un año	1

Fuente: Los autores

Impacto: nivel de degradación o afectación que pueda ocasionar sobre un activo en cada una de sus dimensiones de seguridad.

Tabla 8 Valoración del impacto

Impacto	Valor
Muy Grave	5
Grave	4
Alto	3
Medio	2
Bajo	1

Fuente: Los autores

Riesgo es la probabilidad de ocurrencia de una amenaza por el impacto causado, se calcula de la siguiente forma:

Riesgo = Impacto * Frecuencia

Se define tres niveles de riesgo:

- Inaceptable: ocurre con mucha frecuencia y afecta mucho a los activos, por tal motivo debe evaluarse y tomar controles necesarios para corregirse.
- Importante: puede ocurrir con mucha frecuencia con una afectación baja o puede ocurrir con muy poca frecuencia, pero con una afectación alta.

- Tolerable: Sucede esporádicamente y afecta en un nivel medio, pero se debe estudiar para tratarlo
- Aceptable: No tiene mucha afectación y se presenta muy rara vez, aunque es importante tener el registro en una bitácora.

El riesgo residual se calcula listando los controles aplicables según la metodología ISO 27001 y 27002, la eficacia del control esperada que va de 1 a 4, en donde 4 es la mayor efectividad y la valoración del impacto residual por cada dimensión se calcula dividiendo el valor de riesgo potencial sobre el valor de la eficacia del control.

Riesgo residual = Eficacia del control / Valor del riesgo potencial en cada dimensión

Tabla 9. Valoración del riesgo potencial y residual

VALORACIÓN DEL RIESGO POTENCIAL Y RESIDUAL	
INACEPTABLE	> 16
IMPORTANTE	11 a 16
TOLERABLE	2 a 10
ACEPTABLE	< 2

Fuente: Los autores

13.1 ANALISIS

Como se evidenció en la valoración de activos de la entidad, los activos más valiosos corresponden a los datos y los servicios, por lo tanto, son los que mayor control y cuidado deben tener; sin embargo, son precisamente este grupo de activos los que mayor riesgo presentan y afectan principalmente la disponibilidad.

Las amenazas que con mayor riesgo afectan los activos son:

Tabla 10. Análisis de Riesgo

	Activos afectados							
Amenazas	Datos e información	Servicios	Software	Hardware	Red	Instalación	Equipamiento auxiliar	Personal
Denegación de servicio	X			X	X			
Errores de los usuarios	X	X	X					
Acceso no autorizado	X			X		X	X	
Errores del administrador	X				X			
Uso no previsto		X				X		
Caída del sistema por agotamiento de recursos		X		X				
Abuso de privilegios de acceso			X					
Avería de origen físico o lógico			X	X				
Vulnerabilidades de programas			X					
Errores de mantenimiento			X					
Divulgación de información			X					
Contaminación mecánica				X			X	
Pérdida de equipos							X	
Robo				X			X	
Suplantación de la identidad del usuario					X			
Extorsión								X
Ingeniería social (picaresca)								X

Fuente: Los autores

De acuerdo a lo evidenciado en la tabla 10 Análisis del riesgo, la entidad debe prestar mucha atención para buscar una solución inmediata a los errores de usuario que están incidiendo directamente en los activos más importantes como datos e información, servicios y software.

En el mismo orden se debe vigilar y propender por establecer controles para evitar ataques intencionados a los datos e información, redes de comunicaciones y al personal; toda vez que a través de la observación en la organización se evidencia

que existe gran cantidad de personal que no cuenta con habilidades para los sistemas de información debido a que no se preocupan por su capacitación, tal vez en algunos casos porque ya están pronto a pensionarse, algunos por otra parte opinan que si se capacitan tendrán mayor carga laboral. En torno a los errores del administrador, la gerencia ya evidenció este riesgo, por lo que realizó contratación de un ingeniero con experiencia que se dedica al tema de infraestructura, mitigando un poco este ítem realizando recomendaciones para el uso de mejores prácticas y cambio de dispositivos de red y servidores para obtener un mejor rendimiento de las aplicaciones y así poder mitigar también las caídas por agotamiento de recursos que se ven evidenciadas también en este análisis.

En la parte de errores de mantenimiento y averías de origen físico o lógico se podría pensar en reducir el tiempo de mantenimiento de equipos e instruir a los técnicos de mantenimiento en el uso de check-list que permitan minimizar los errores en las actividades de mantenimiento de equipos.

Por otra parte, la organización cuenta con procedimientos, pero que, al hacer revisión de ellos, estos se encuentran desactualizados, ya que la actividad a pesar de seguirse ejecutando no se realiza como está descrito; por ello es sumamente importante realizar una revisión y actualización de los procedimientos que se están realizando en el área de TICS.

Según la información recolectada y la observación realizada en el medio, el acceso no autorizado a la información es latente, ya que entre los usuarios aún no tienen la conciencia de la salvaguarda de contraseña, por lo que algunos la comparten entre sus compañeros u otras personas; esto lo hacen muy a pesar que en el formato para la creación de usuario se les indica y asumen la responsabilidad administrativa y penal por el mal uso de ella.

De acuerdo a la recolección de información realizada en la entidad, a pesar que el área de TICS ha empezado a controlar un poco más el uso de los recursos; el control del personal no es el adecuado, posiblemente al volumen que se maneja y las diversas maneras de contratación que se realizan para el recurso humano, siendo esta una debilidad latente que se evidencia en los resultados del análisis de riesgo realizado.

En la tabla 12, se realiza la evaluación del riesgo residual, que corresponde a aquel riesgo que después de aplicar los controles recomendados no es posible controlar por la entidad, porque como se dijo anteriormente, no existe un sistema de información 100% seguro.

14. SISTEMA DE CONTROL INTERNO SEGÚN ISO 27001

El control interno se define como aquellas actividades que se realizan para prevenir, corregir errores o irregularidades que puedan afectar el funcionamiento de un sistema para conseguir sus objetivos; aplicado a ISO 27001, el cual es basado en el ciclo PHVA y a procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI, tenemos el ciclo completo de control en el que se planea la ejecución, se ejecuta, se verifica su cumplimiento y de ser necesario se realizan ajustes para el mejoramiento continuo.

Para asegurar la integridad, confidencialidad y disponibilidad de los sistemas, se requiere establecer mecanismos de control, para verificar el cumplimiento de las reglas del negocio. Estos controles pueden ser manuales o automáticos o una combinación de ellos.

Para ayudar en el establecimiento de ellos para mitigar el impacto de las vulnerabilidades y que según el análisis de riesgos promedio deben ser atendidos ya que causarían un daño importante en la organización, y para este caso, se hará un análisis de acuerdo a lo sugerido en la ISO 270001.

En atención a que los grupos de activos Datos e información (DeI), Redes y comunicaciones (RyC) y Personal (Per) son los que mayor factor de riesgo tienen, se analizarán los siguientes dominios:

- A.5 Política de la seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad de los Recursos humanos
- A.8 Gestión de Activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y ambiental
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.15 Relaciones con los proveedores
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de seguridad de la información de la gestión de la continuidad de negocio
- A.18 Cumplimiento

Existen varias opciones de tratamiento, aunque de manera general se pueden agrupar en las siguientes categorías:

- ELIMINAR EL RIESGO: eliminando los activos
- TRANSFERIR EL RIESGO: Se valora la sub contratación o póliza en el caso de ocurrir una incidencia. (tener en cuenta que no todo se puede transferir)
- ASUMIR EL RIESGO: Implica que no se van a tomar medidas frente al riego (Es la dirección quien toma la decisión, teniendo en cuenta que este no aumente)
- MITIGAR EL RIESGO: Implantación de medidas que actúen de salvaguardas (Se deben documentar y gestionar)

14.1 DECLARACION DE APLICABILIDAD - SoA

En el siguiente documento de Declaración de Aplicabilidad (SoA), se resume en términos generales los objetivos de control, las amenazas y vulnerabilidades, los controles seleccionados, las razones por las cuales fueron seleccionados entre las que tenemos de tipo legal, es decir, que son de obligatorio cumplimiento por una norma superior a la entidad y que de no llevarse a cabo la entidad incurriría en sanciones, de tipo contractual, son aquellas que en la celebración de contratos con las entidades o personas la institución debe cumplir, de requerimiento del negocio, son aquellos que en el desempeño de su actividad el hospital ha determinado que se deben realizar y por último aquellas que fueron evidenciadas en el análisis de riesgos realizado en el trabajo anterior. También se aclaran los controles que ya se encuentran implementados y que deben seguir trabajándose, así como aquellos que desde nuestra experiencia y análisis consideramos se deben tener en cuenta para el cumplimiento de los objetivos de control de la institución. Además, al finalizar se aclara y se justifica aquellos controles que serán excluidos del análisis.

El hospital entendiendo la importancia de la seguridad de la información, está en búsqueda de la certificación en ISO27001, razón por la cual el establecimiento de este documento se hace indispensable. Además, que organiza y resume las amenazas identificadas y analizadas durante la evaluación de riesgos, obteniendo un panorama de lo que está haciendo y lo que debe hacer para asegurar las correspondientes medidas de seguridad.

Tabla 11 Declaración de aplicabilidad SoA

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.5 Política de seguridad												
A.5.1.1	Políticas para la Seguridad de la Información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas	Deficiencias en la organización	Falta de claridad en las acciones a seguir	ASUMIR	La entidad cuenta con una política de seguridad de la información, aprobada por la gerencia		X		X		
A.5.1.2	Revisión de la política de seguridad de la información	Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas	Deficiencias en la organización	Desactualización de las políticas establecidas de acuerdo al avance de la tecnología y a los requisitos de la organización.	MITIGAR		Se debe revisar y de ser necesario actualizar; posteriormente se debe publicar y dar a conocer a los funcionarios y personal externo de ella. Dentro de la resolución que aprueba la política de seguridad de la información se debe establecer la periodicidad y el responsable de realizar la validación de la política.	X		X	X	
A.6 Organización de la seguridad de la información						CONTROLES		RAZONES PARA LA SELECCIÓN DE CONTROLES				
A.6.1 Organización interna												

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.6.1.1	Seguridad de la Información Roles y Responsabilidades.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	Deficiencias en la organización Errores del administrador Errores de los usuarios	Trabajo descoordinado y desarticulado sin el establecimiento de objetivos claros. Posible generación de trabajo repetido desde diferentes áreas. Asignación baja en el presupuesto de inversión para la compra y mantenimiento de herramientas y recurso humano indispensables para el establecimiento de controles Falta de toma de decisiones	MITIGAR	Las responsabilidades son conocidas informalmente en la entidad.	Generar un documento de buenas prácticas en el uso de los activos de información, estableciendo responsabilidades en su uso			X	X	
A.6.1.2	Separación de los deberes	Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización	Deficiencias en la organización Errores del administrador	Desconocimiento de directrices y falta de toma de decisiones. Toma de decisiones contradictorias	TRANSFERIR	Dentro de los compromisos contractuales de tercerización del área de TICS se encuentra esta función.	En la validación de la Política de Seguridad de la Información, establecer la conformación de un grupo de seguridad de la información, conformado por miembros de la organización con descripción clara de actividades y rol.		X	X		

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.6.1.3	Contacto con las autoridades	Se debe mantener contactos apropiados con las autoridades pertinentes	Errores del administrador Deficiencias en la organización Difusión de software dañino Fallo de servicios de comunicaciones	Detección de accesos abusivos al sistema sin determinar responsables.	ASUMIR	Existe un proceso de gestión legal y cumplimiento normativo en donde se establecen los procedimientos para gestionar las relaciones con las autoridades reguladoras. El área de control interno, anualmente emite un informe de cumplimiento de requisitos legales en el tema de licenciamiento de software.		X		X		
A.6.1.4	Contacto con grupos de interés especiales	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	Errores de los usuarios Fallo de servicios de comunicaciones	Desconocimiento del entorno. Aplicación de actividades o reglas que han sido fallidas en otros entornos. Capacitación de personal.	MITIGAR	Desde la oficina de TICS se mantiene contacto con las empresas que tienen contrato con la institución proveedoras de software y hardware.	El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en la organización a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Vincular a los funcionarios responsables de la seguridad de la información con grupos de interés haciendo uso de herramientas libres en internet.			X		

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.6.1.5	Seguridad de la información en Gestión de Proyectos.	La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto	Fallo de servicios de comunicaciones Errores de los usuarios Errores del administrador Deficiencias en la organización Alteración o destrucción de la información caídas por agotamiento de recursos Acceso no autorizado	Al trabajarlo como proyecto se asegura que se realice la debida planeación de actividades, asegurando los recursos para ellos y el seguimiento en el cumplimiento de las actividades.	ASUMIR	Existe en el área de planeación una sección dedicada a la gestión de proyectos		X				
A.6.2 Dispositivos Móviles y Teletrabajo.												
A.6.2.1	Política para dispositivos móviles.	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles	Acceso no autorizado Alteración o destrucción de la información Fallo de servicios de comunicaciones	Falta de aplicación de pruebas de vulnerabilidad.	MITIGAR	El acceso a personal externo para la aplicación es autorizado por la Subgerencia de servicios de salud, y se da cumplimiento al proceso institucional para la creación, actualización y/o desactivación para el acceso a sistemas de información institucional.	Realizar pruebas de hacking ético para evaluar los riesgos actuales.			X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.6.2.2	Teletrabajo	Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo	Acceso no autorizado Alteración o destrucción de la información Fallo de servicios de comunicaciones	Asignación inadecuada de los permisos asignados	ELIMINAR				X	X	X	Para la organización aún no es atractiva la idea de realizar contratación a través del Teletrabajo. Sin embargo ya existe un convenio de trabajo en telemedicina, ellos son los que administran sus recursos y no tienen acceso a los recursos del hospital.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS.												
A.7.1 Antes de la contratación laboral												
A.7.1.1	selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos	Deficiencias en la organización	Falta de claridad en las acciones a seguir	MITIGAR	La empresa siempre debe verificar los antecedentes del personal	seguir realizando la actividad de verificación de antecedentes en la contratación de personal			X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información	Deficiencias en la organización	Falta de claridad en las acciones a seguir	ASUMIR	Los empleados asumen los términos y condiciones a la hora de firmar su contrato de acuerdo a su responsabilidad		X				
A.7.1.2 durante la ejecución del empleo												
A.7.2.1	Responsabilidades de la Dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización	errores de administrador	falta de capacitación con el uso de herramientas	MITIGAR	no existen políticas de seguridad	crear e implementar políticas de seguridad				X	
A.7.2.2	Toma de conciencia, educación y formación de la Seguridad de la Información	Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo	errores de administrador	falta de capacitación con el uso de herramientas	EXCLUIR	No se han realizado actividades de formación para la mitigación de riesgo					X	excluida hasta que se realicen políticas de seguridad de la información
A.7.2.3	proceso disciplinario	Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información	Alteración o destrucción de la información	Fallas en las condiciones de almacenamiento de la información	MITIGAR	Se abren procesos disciplinarios a quienes intenten acceder sin permisos a la información sensible				X		

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.7.3 términos y cambio de empleo												
A.7.3.1	termino o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir	Deficiencias en la organización	Toma de decisiones que no son socializadas al personal	MITIGAR	se define las responsabilidades para los cambios de contratación				X		
A.8 Gestión de activos												
A.8.1 Responsabilidad por los activos												
A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Avería de origen físico o lógico Deficiencias en la organización	Inventario desactualizado. Movimientos y cambios ejecutados que no son informados. Pérdida de activos. Descontrol en garantías de equipos. Instalación de software no autorizado.	MITIGAR	Existe un inventario de activos y de aplicaciones	Organizar y actualizar el listado de activos y de software con su respectivo responsable.	X	X	X	X	
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben ser propios.	Avería de origen físico o lógico Deficiencias en la organización Acceso no autorizado	Establecer responsabilidades en el personal que usa los recursos.	ASUMIR	El inventario de activos se encuentra distribuido por responsable en cada dependencia.	Incluir en los procedimientos de talento humano la entrega de activos al cambio de puesto o retiro de la institución.			X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información	Errores de los usuarios Deficiencias en la organización Difusión de software dañino Alteración o destrucción de la información caídas por agotamiento de recursos Acceso no autorizado	Poca claridad en el uso de los recursos y de la responsabilidad en el cuidado de ellos.	MITIGAR		Las regulaciones para el uso adecuado de la información y los activos para su administración, se deben incluir y documentar en el manual de buen uso de sistemas		X	X	X	
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo	Errores de los usuarios Deficiencias en la organización Alteración o destrucción de la información Acceso no autorizado	Existe un protocolo para la entrega de activos que no es realizado por todo el personal.	MITIGAR	Protocolo de entrega de activos	Establecer controles para garantizar que toda la población laboral ejecute el protocolo de entrega de activos.		X	X		
A.8.2 Clasificación de la información												
A.8.2.1	Clasificación de la Información.	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada	Deficiencias en la organización Acceso no autorizado Alteración o destrucción de la información	Posibilidad de almacenamiento y consumo de recursos en información no importante o repetida.	MITIGAR		Establecer un sistema de clasificación de la información descrito en la Política de Seguridad de la información.	X		X		
A.8.2.2	Etiquetado y manejo de información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de	Deficiencias en la organización Acceso no autorizado Alteración o destrucción de la información	Desconocimiento de la información almacenada. Almacenamiento y etiquetado inadecuado de los datos. Posibilidad de fallo y	TRANSFERIR		Identificar dentro de la Política de Seguridad de la información, directrices para realizar el etiquetado y manejo de la información de acuerdo al esquema de			X		

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
		información adoptado por la organización		reproceso al restaurar información antigua.			clasificación establecido.					
A.8.2.3	Manejo de Activos.	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Deficiencias en la organización Acceso no autorizado Alteración o destrucción de la información	La entidad no cuenta con un esquema claro de clasificación de la información	MITIGAR		Establecer un protocolo claro para el manejo de activos que haga parte del procedimiento de contratación.		X	X	X	
A.8.3 Manejo de medios de soporte.												
A.8.3.1	Gestión de medios de Soporte Removibles	Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización	Deficiencias en la organización Acceso no autorizado Alteración o destrucción de la información	La entidad no cuenta con un esquema claro de clasificación de la información	TRANSFERIR	El hospital tiene contratado el almacenamiento y salvaguarda de la información						
A.8.3.2	Disposición de los medios de soporte.	Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales	Deficiencias en la organización Acceso no autorizado Alteración o destrucción de la información Avería de origen físico o lógico	Procedimiento que no está documentado. Por gestión documental existen tablas documentales para el apoyo de esta tarea	ASUMIR	La organización está trabajando en la revisión de tablas documentales.	Incorporar en los procedimientos el manejo de activos.					
A.8.3.3	Transferencia de medios de soporte físicos.	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Deficiencias en la organización Acceso no autorizado Alteración o destrucción de la información Avería de origen físico o lógico	Salvaguarda de medios de almacenamiento con poca seguridad	MITIGAR		Revisar procedimiento de copias de seguridad e implementar un servicio para salvaguarda fuera de la institución con las condiciones mínimas de seguridad.					

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.9 CONTROL DE ACCESO												
A.9.1 Requisito del negocio para el control de acceso												
A.9.1.1	Política de control de acceso	Deficiencias en la organización	Falta de difusión. Cultura organizacional	Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso	MITIGAR		Establecer políticas de control de acceso al hospital.	x		X		
A.9.1.2	Acceso a redes y a servicios en red	Acceso no autorizado	No existen comprobaciones de los equipos de la red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	MITIGAR		Realizar comprobaciones de autenticación a través de la MAC de los pcs del hospital			X	X	
A.9.2 Gestión del acceso de usuarios												
A.9.2.1	Registro y cancelación del registro de usuarios	Acceso no autorizado	Los contratistas no informan cuando sale personal pasa su inactivación	Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	MITIGAR	Existe un formato de creación y desactivación de usuarios	Exigir a las diferentes empleadoras contratadas por el hospital actualizar periódicamente las bases de datos de sus empleados para que el proceso de desactivación dé usuarios ya retirados sea más fluido y real	x		X	X	
A.9.2.2	Suministro de acceso de usuarios	Acceso no autorizado	No hay control sobre los accesos que los usuarios tienen a los diferentes sistemas	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios	MITIGAR	Se cuenta con políticas de grupo que delimitan los accesos de los usuarios a los servicios de red	Revisar el proceso de alta y bajas de usuarios en la red			X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.9.2.3	Gestión de derechos de acceso privilegiado	Acceso no autorizado	No existe criterios para la asignación de privilegios	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	MITIGAR	Existen perfiles de usuarios con diferentes privilegios en los diferentes sistemas de información	Establecer control para la asignación de privilegios			X		
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Acceso no autorizado	Contraseñas débiles	La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal	MITIGAR		Establecer un proceso formal de gestión de contraseñas	X		X	X	
A.9.2.5	Revisión de los derechos de acceso de usuarios	Deficiencias en la organización	Desconocimiento del personal encargado para realizar esta verificación	Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares	MITIGAR		Revisar periódicamente los derechos de acceso de los usuarios por parte del área de control interno del hospital.	X				
A.9.2.6	Cancelación o ajuste de los derechos de acceso	Deficiencias en la organización	Desconocimiento del personal encargado para realizar esta verificación	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	MITIGAR		Revisar periódicamente los derechos de acceso de los usuarios por parte del área de control interno del hospital.	X				

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.9.3 Responsabilidades de los usuarios												
A.9.3.1	Uso de información secreta	Acceso no autorizado	Contraseñas débiles	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.	MITIGAR	Cuando se asignan las contraseñas se da la información sobre el manejo de estas	Establecer métodos para asignación de contraseñas seguras e indicar a los usuarios la importancia de esto			X	X	
A.9.4 Control de acceso a sistemas y aplicaciones												
A.9.4.1	Restricción de accesos a la información	Acceso no autorizado	No existen políticas claras y ampliamente conocidas por el personal	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso	MITIGAR		Documentar la política de registro y acceso de los usuarios para el hospital.			X	X	
A.9.4.2	Procedimiento de conexión segura	NO APLICA	NO APLICA	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura	ASUMIR	NO APLICA				X	X	En la compañía no se usa el acceso remoto por parte de los usuarios
A.9.4.3	Sistemas de gestión de contraseñas	Acceso no autorizado	No existen métodos de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	MITIGAR		establecer un sistema de gestión de contraseñas interactivo que promueve el cumplimiento de las políticas de contraseñas establecidas				X	
A.9.4.4	Uso de programas utilitarios privilegiados	Acceso no autorizado	No se audita con una periodicidad determinada el software instalado	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los	ASUMIR	Existen GPOs encaminadas a denegar el uso de ciertos utilitarios o programas no autorizados	Revisar el estado de los distintos software para garantizar que los usuarios no tengan acceso a códigos fuentes ni a utilitarios			X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
				controles del sistema y de la aplicación.			de desarrollo o línea de comandos					
A.9.4.5	Control de acceso a códigos fuentes de programas	Acceso no autorizado	No se audita con una periodicidad determinada el software instalado	Se debe restringir el acceso a códigos fuentes de programas	ASUMIR	Existen GPOs encaminadas a denegar el uso de ciertos utilitarios o programas no autorizados	Revisar el estado de los distintos software del hospital para garantizar que los usuarios no tengan acceso a códigos fuentes ni a utilitarios de desarrollo o línea de comandos			X	X	
A.10 Criptografía												
A.10.1 Controles criptográficos												
A.10.1.1	Política sobre el uso de controles Criptográficos.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información	Errores de Administrador	Falta de políticas para implementar herramientas criptográficas que ayuden a mitigar los fallos en la información	ASUMIR		Incluir en los procesos contractuales de la entidad con terceros por contratación de la implementación de controles criptográficos con especialistas en el área.	X		X		
A.10.1.2	Gestión de Claves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida	Error de Administrador y Deficiencia de la Organización	Falta de complementar un control por llaves secretas, para evitar el acceso a la información	ASUMIR		Se debe implementar unas llaves secretas para apoyar el uso criptográfico en la Empresa	X		X		
A.11 SEGURIDAD FISICA Y DEL ENTORNO.												
A.11.1 áreas seguras												
A 11.1.1	perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información	Acceso no autorizado	Fallo en la autenticidad para el ingreso.	MITIGAR		delimitar las áreas donde pueden acceder el personal			X		

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A11.1.2	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado	Alteración o destrucción de la información	Acceso no restringido a áreas donde guarda la información	MITIGAR		delimitar las áreas donde pueden acceder el personal			X		
A11.1.3	Seguridad de oficinas, salones e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones	Acceso no autorizado	Fallo en la autenticidad para el ingreso.	MITIGAR		delimitar las áreas donde pueden acceder el personal			X		
A11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes	desastres naturales	Edificación antigua que al momento de la construcción no fue preparada para sismo resistencia	MITIGAR	se tienen rutas de evacuación , herramientas contra incendio				X		
A11.1.5	trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras	Deficiencias en la organización	Toma de decisiones que no son socializadas al personal	MITIGAR	la áreas de trabajo están asignadas y distribuidas de acuerdo a la actividad				X		
A11.1.6	área de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado	Deficiencias en la organización	Toma de decisiones que no son socializadas al personal	MITIGAR	la áreas de trabajo están asignadas y distribuidas de acuerdo a la actividad, controlando el acceso a áreas restringidas por el personal de seguridad a través de las cámaras				X		

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.11.2 equipos												
A.11.2.1	ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado	Acceso no autorizado	Políticas del uso de sistema obsoletas. Fallo en la autenticidad para el ingreso		la ubicación de los dispositivos se asigna de acuerdo al rol del empleado, los que contienen información importante deben ser protegidos mediante contraseñas y puertas de acceso seguras				X		
A.11.2.2	servicios públicos de soportes	Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.	Corte de suministro eléctrico	Accesibilidad a la información sin suministro eléctrico		Uso de UPS	adquirir Ups para evitar incidentes con fallas eléctricas			X		
A.11.2.3	seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.	Avería de origen físico o lógico	Cableado obsoleto en algunas sesiones de la entidad		el cableado debe tener un monitoreo y mantenimiento preventivo	verificar el estado del cableado estructurado			X	X	
A.11.2.4	mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas	Condiciones inadecuadas de temperatura o humedad	Daño en los aires acondicionados sin soporte para reparación. Falla en la ejecución de mantenimientos preventivos del sistema de refrigeración de las áreas.	MITIGAR		realizar el mantenimiento periódicamente			X	X	
A.11.2.5	retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa	Perdida de equipos	Falencias en la vigilancia. Responsabilidad en la custodia	MITIGAR	informar a telemática antes de retirar un equipo				X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.11.2.6	seguridad de equipos y activos fuera del predio	se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización , teniendo en cuenta el riesgo de trabajar por fuera	Otros desastres naturales	Hay debilidades en la conexión a tierra de algunos sectores de la red eléctrica y de comunicaciones	ASUMIR					X		No existen equipos fuera de las instalaciones
A.11.2.7	disposición segura o reutilización de equipo	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia	Alteración o destrucción de la información	Fallas en las condiciones de almacenamiento de la información	MITIGAR		Verificar que no existan datos sensibles para la empresa en los dispositivos a eliminar o reutilizar			X	X	
A.11.2.8	equipos sin supervisión de usuario	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada	Alteración o destrucción de la información	Fallas en las condiciones de almacenamiento de la información	MITIGAR		Verificar que los equipos tengan contraseñas adecuadas para la protección de datos sensibles			X	X	
A.11.2.9	política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información	Deficiencias en la organización	Toma de decisiones que no son socializadas al personal	MITIGAR		implantar políticas de seguridad				x	
A12. SEGURIDAD DE LAS OPERACIONES												
A12.1 Procedimientos operacionales y responsabilidades.												

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.12.1.1	Procedimientos de operación documentadas	Deficiencias en la organización	Rotación de personal constante y falta de capacitación	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	MITIGAR	En la intranet del hospital se encuentran publicados los procedimientos y que se encuentran aprobados a la fecha	Realizar validación de los procedimientos para solicitar ajuste al comité de control interno			X	X	
A.12.1.2	Gestión de Cambios.	Deficiencias en la organización	Rotación de personal constante y falta de capacitación	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	ASUMIR	Los cambios son realizados por el personal debidamente autorizado	Evaluar y socializar el procedimiento de gestión de cambios que actualmente maneja la oficina de gestión documental del hospital.			X	X	
A.12.1.3	Gestión de Capacidad	Errores del administrador	Falta de políticas claras	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	MITIGAR	Los recursos de información se monitorean informalmente	Establecer responsabilidades en la monitorización del uso de los recursos.	X		X		
A.12.1.4	Separación de los ambientes de desarrollo, ensayo y operación.	Deficiencias en la organización Errores del administrado	Falta de control de los usuarios administradores con contraseñas compartidas por varios usuarios	Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional	MITIGAR	Se utilizan perfiles de acceso a los diferentes sistemas con el fin de limitar el accionar de los usuarios dentro de los diferentes sistemas de información e información disponible en la red	Utilización de sistemas de autenticación y autorización independientes para los diferentes ambientes.			X		
A12.2 Protección contra códigos maliciosos.												

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.12.2.1.	Controles contra códigos maliciosos	Errores de los usuarios. Difusión de software dañino Acceso no autorizado	Exceso de confianza y facilidad de ingreso a los pc del hospital	Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos	ASUMIR	Los equipos del hospital se encuentran protegidos por software de detección y reparación de virus	Establecer GPOs para impedir la ejecución de archivos .ese sin autorización del administrador. Establecer medidas de protección frente a código malicioso.			X		
A12.3 Copias de Respaldo												
A.12.3.1.	Copias de respaldo de la información.	Errores del administrador Acceso no autorizado	Asignación de permisos inadecuada. Fuga de información sin determinación de responsables	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	MITIGAR	Existe documentación sobre el proceso y la periodicidad de los diferentes Backups del hospital así como de los lugares de almacenamiento	Realizar revisión y verificación de los procedimientos de Backup del hospital y actualizarlos de ser necesario.	X	X	X	X	
A12.4 Registro y Seguimiento												
A.12.4.1.	Registro de eventos	Errores del administrador	No existe registro de fallas	Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.	MITIGAR		Llevar un record de las averías registradas y documentar las medidas tomadas para su resolución.	X		X		

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.12.4.2.	Protección de la información de registro.	Acceso no autorizado Errores del administrador	Vulnerabilidades en los sistemas de información	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	MITIGAR		Realizar pruebas de penetración sobre los sistemas del hospital.	X			X	
A.12.4.3	Registros del administrador y del operador	Acceso no autorizado Errores del administrador	Falta de seguridad en la administración de las claves de administrador	Las actividades del administrador y del operador del sistema se deben registrar, proteger y revisar con regularidad	MITIGAR		Llevar un log de las acciones sobre el sistema y los diferentes servidores del hospital y almacenar estos en un sitio seguro			X		
A.12.4.4	Sincronización de relojes	Errores del administrador	Fallas en la administración de servidores	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	ASUMIR	Los servidores y los pc's están sincronizados según la hora del servidor de control de dominio		X		X		
A.12.5. Control de Software Operacional												
A.12.5.1.	Instalación de software en sistemas operativos	Acceso no autorizado	El monitoreo se realiza de forma informal	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	MITIGAR		Establecer GPO's para impedir la ejecución de archivos .ese sin autorización del administrador. Establecer parámetros de monitoreo de los sistemas del hospital				X	
A.12.6. Gestión de vulnerabilidad técnica												

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.12.6.1.	Gestión de las vulnerabilidades técnicas.	Información sensible no encriptado	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información queso usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	MITIGAR		Establecer políticas de evaluación de vulnerabilidades de los sistemas de información			X	X	
A.12.6.2	Restricciones sobre la instalación de Software	Errores de los usuarios. Difusión de software dañino Acceso no autorizado	Exceso de confianza y facilidad de ingreso a los PCs del hospital	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.	MITIGAR	Los equipos del hospital se encuentran protegidos por software de detección y reparación de virus	Establecer GPOs para impedir la ejecución de archivos, sin autorización del administrador. Establecer medidas de protección frente a código malicioso.			X		
A.12.7. Consideraciones sobre auditorías de sistemas de información.												
A.12.7.1.	Controles sobre auditorías de Sistemas de Información.	Deficiencias en la organización	Falta de capacitación del personal. Falta de retroalimentación de las auditorias	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	MITIGAR	La aplicación DGH tiene un log de auditoria del cual también se realiza Backup	Establecer acciones de mejora basados en los logs de auditoria del programa			X	X	
A13. SEGURIDAD DE LAS COMUNICACIONES												

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.13.2 Transferencia de información												
A.13.2.1.	Políticas y procedimientos de transferencia de información.	Acceso no autorizado. Alteración o destrucción de la información.	Información sensible no encriptado	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.	ASUMIR		Establecer políticas de intercambio de información			X		
A.13.2.2.	Acuerdos sobre transferencia de información.	Acceso no autorizado. Alteración o destrucción de la información.	Información sensible no encriptado	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	MITIGAR		Incluir cláusulas de confidencialidad en los contratos con terceros			X		
A.13.2.3	Mensajes electrónicos.	Fallo de servicios de comunicaciones	No se garantiza alta disponibilidad	Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	MITIGAR		Encriptar el servidor de correo electrónico que contiene la información de las cuentas de correo y limitar su acceso a los usuarios administradores			X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.13.2.4	Acuerdos de confidencialidad o de no divulgación.	Acceso no autorizado. Alteración o destrucción de la información.	Información sensible no encriptado	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información	MITIGAR		Incluir cláusulas de confidencialidad en los contratos con terceros			X		
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.												
A.14.1												
A.14.1.1	Requisitos de seguridad de los sistemas de información	. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existente	Errores de Usuario	Por qué no existe una comunicación entre el Administrador del Sistema, referente a los procesos que a diario se actualizan en la Empresa.	ASUMIR	La entidad cuenta con las políticas de seguridad a la cual se exigen una serie de requisitos para su implementación	Se debe actualizar los métodos aplicados para este sistema.	X		X	X	
A.14.1.2		Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Error de Administrador	Falta un plan de contingencia para la seguridad y las aplicaciones en las redes de información	MITIGAR	Todos los datos se validan al ingreso de la información, para conocer su estado y requerimiento exigido.	Los datos ingresados a las bases de datos, deben ser confiables y coordinados por el usuario que los ingrese.			X		

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.14.1.3		Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizado	Deficiencia de la Organización, Errores de Administrador	Falta de Control en los accesos de Datos y aplicaciones	MITIGAR	Existen unas reglas que se deben cumplir en cuanto al procesamiento de datos	El procesamiento de datos debe ser validado, para evitar la duplicidad y complejidad de archivos		X	X		
A.14.2.1	Seguridad en los procesos desarrollo y soporte	Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización	Caída por agotamiento de recursos	Falta de un sistema que permita la estabilidad y constancia de los procesos de información	ASUMIR		Generar un procedimiento que permita identificar los activos y el mensaje dependiendo de su aplicación, para definir un control adecuado			X	X	
A.14.2.2		Procedimiento de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización	Error de Administrador	Falta de planeación en el momento de implantar un sistema para controlar los cambios que se ejecuten en la Empresa, con referencia a la información.	MITIGAR	La entidad cuenta con un procedimiento interno que permite hacer el control de los cambios en el sistema	Realizar validación del procedimiento.		X	X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.14.2.3		Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacional	Errores de Administrador	Falta de políticas para implementar herramientas para la revisión en el proceso técnico.	ASUMIR		Incluir en los procesos contractuales. La implementación de herramientas para el manejo y revisión de los paquetes de software y control de la Empresa	X		X		
A.14.2.4		Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones de seguridad organizacional	Error de Administrador y Deficiencia de la Organización	Falta control en los paquetes que se implementen en el sistema de información	ASUMIR		Se debe implementar controles para una aplicación de revisión técnica que favorezca los datos de la información suministrada.	X		X		
A.14.2.5		Principios de construcción de sistemas de seguros. Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.	difusiones Software Dañino	falta de Control y supervisión en los paquetes de software que se instalan y operan dentro de la Organización	MITIGAR	existe el área de Control de los sistemas que se manejan en la Empresa, la cual permite controlar de inmediato las posibles fallas que se presentan				X		

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.14.2.6		Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistema	Error de Administrador	Falta de personal auxiliar que mantenga actualizado los procesos que se ejecutan en el sistema de información	ASUMIR		Los datos que a diario se incluyen en las bases de datos de la Empresa, deben ser salvaguardados bajo un control y medida adoptada por la Empresa	X	X			
A.14.2.7		Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados	Errores de Administrador	Falta de control en el funcionamiento de cada una de las aplicaciones contempladas en el software instalado	ASUMIR	Existe en la Empresa un Equipo de trabajo encargado de realizar las aplicaciones que se necesite implementar, a diferencia de los paquetes como por ejemplo TNS, son protocolizados por la misma Empresa que comercializa.	Se necesita implementar software con firmas reconocidas y con experiencia en cada área específica.	X	X	X	X	
A.14.2.8		Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad	Errores de Administrador	Falta de coordinación en el momento de hacer la puesta en marcha del software instalado.	ASUMIR		Cada vez que se haga un cambio en los sistemas operativos que conlleve a una aplicación nueva, se debe primero hacer una revisión técnica para verificar lo implantado en el sistema.		X	X	X	
A.15.2 Gestión de la prestación de servicios de proveedores												

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores.	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores	Acceso no autorizado Alteración o destrucción de la información Fallo de servicios de comunicaciones	Software institucional con restricciones, sin embargo no se puede limitar el acceso en tipo de registro, es decir, un auditor puede consultar historias de cualquier usuario	MITIGAR		Solicitud de personalización al software institucional			X	X	
A.15.2.2	Gestión de cambios a los servicios de los proveedores.	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos	Acceso no autorizado Alteración o destrucción de la información Fallo de servicios de comunicaciones	Falta de políticas de uso para proveedores	MITIGAR		Involucrar en los acuerdos contractuales con proveedores la categoría para el acceso a la información		X	X		
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.											
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información.	Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información	Deficiencias de la Organización	Falta de implementar un manual de responsabilidades a cada uno de los usuarios que manejan la información dentro de la Empresa	TRANSFERIR	En la Empresa existe un manual de funciones donde cada uno de los usuarios, contempla sus actividad y su rol dentro del área donde está su puesto de trabajo,	Se debe implementar un manual de funciones acorde a las necesidades, capacidades y preparación académica de cada uno de los usuarios del sistema.	X	X	X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.16.2		Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible	Deficiencias de la Organización	Falta de personal calificado para la recolección de las evidencias que se produzcan en el momento de una amenaza, clasificar el tipo y la causa que lo genero.	ASUMIR	En la Empresa existe un departamento Jurídico, que asesora al departamento se sistemas, para los eventos que inciden en la parte jurídica dependiendo del incidente causado, se redacta un informe técnico avalado por conceptos jaricos autorizados.		X	X	X	X	
A.16.3		Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios		Falta de personal calificado para la recolección de las evidencias que se produzcan en el momento de una amenaza, clasificar el tipo y la causa que lo genero.	ASUMIR	En la Empresa existe un departamento Jurídico, que asesora al departamento se sistemas, para los eventos que inciden en la parte jurídica dependiendo del incidente causado, se redacta un informe técnico avalado por conceptos jaricos autorizados.		X	X	X	X	
A.16.4		Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información	Error de Administrador	Falta generar reportes de eventos generados para garantizar la seguridad de la información	MITIGAR		Se debe implementar un proceso dentro de la Empresa, que genere información precisa de los eventos ocurridos en los procesos informáticos.		X		X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.16.5		Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados	Error de Administrador	Falta de personal calificado para la recolección de las evidencias que se produzcan en el momento de una amenaza, clasificar el tipo y la causa que lo genero.	ASUMIR	En la Empresa existe un departamento encargado de atender las solicitudes de los usuarios, para solucionar los incidentes ocasionados.			X	X	X	
A.16.6		Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados	Error de Administrador	Falta de personal calificado para la recolección de las evidencias que se produzcan en el momento de una amenaza, clasificar el tipo y la causa que lo genero.	ASUMIR	En la Empresa existe un departamento encargado de atender las solicitudes de los usuarios, para solucionar los incidentes ocasionados.			X	X	X	
A.16.7		Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros	Deficiencia de la Organización	Falta de mecanismos que cuantifiquen cuales el costo-beneficio al momento de recuperar un incidente	ASUMIR	En la Empresa se debe implementar un mecanismo de control interno de los recursos informáticos, para evaluar los incidentes ocasionados durante los diferentes procesos que se ejecutan en el sistema de información de la misma			X	X	X	
A.16.8		Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia	Deficiencia de la Organización	Falta de personal calificado para la recolección de las evidencias que se produzcan en el momento de una amenaza, clasificar el tipo y la causa que lo genero.	ASUMIR	Existe una oficina Jurídico, que asesora a TIC, para los eventos que inciden en la parte jurídica dependiendo del incidente causado, se redacta un informe técnico avalado por conceptos jurídicos autorizados.		X	X	X	X	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.												
A.17.1. Continuidad de seguridad de la información Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.												
A.17.1.1.	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	Deficiencias en la organización Daños por fuego Daños por agua Desastres industriales Contaminación mecánica contaminación electromagnética Avería de origen físico o lógico Corte de suministro eléctrico Condiciones inadecuadas de temperatura o humedad Fallo de servicios de comunicaciones	Existe inicios de plan de contingencia que no está documentado	ASUMIR	Se definen las Políticas de Seguridad de la Información de la organización basada en la Norma ISO27001, con el fin de buscar las causas que originaron la ocurrencia de los eventos que atentan contra la información, los activos y la continuidad del negocio.	La entidad debe elaborar el plan de contingencias con el personal de las áreas responsables por los planes relacionados. Ejemplos de planes relacionados son: los planes de continuidad de negocio, plan de recuperación de desastres, plan de continuidad de las operaciones, plan de recuperación del negocio, plan de respuesta a incidentes y plan de acción de emergencias			x	x	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.17.1.2.	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Deficiencias en la organización Daños por fuego Daños por agua Desastres industriales Contaminación mecánica contaminación electromagnética Avería de origen físico o lógico Corte de suministro eléctrico Condiciones inadecuadas de temperatura o humedad Fallo de servicios de comunicaciones	No existen procedimientos direccionados para conocer el actuar en caso de activar un plan de contingencia	ASUMIR	Se cuentan con Planes de continuidad del negocio enfocados únicamente a la infraestructura tecnológica, dejando de lado los procesos críticos de la organización.	La entidad coordina las pruebas al plan de contingencias con el personal de las áreas responsables por los planes relacionados. Ejemplos de planes relacionados son: los planes de continuidad de negocio, plan de recuperación de desastres, plan de continuidad de las operaciones, plan de recuperación del negocio, plan de respuesta a incidentes y plan de acción de emergencias			x	x	
A.17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.	Deficiencias en la organización Daños por fuego Daños por agua Desas. industriales Contaminación mecánica contaminación electromagnética Avería de origen físico o lógico Corte de suministro eléctrico Condiciones inadecuadas de temperatura o humedad Fallo de servicios de comunicaciones caídas por	No hay seguimiento posterior a la entrada en funcionamiento después de un evento catastrófico	ASUMIR		La entidad deberá poner en prueba el plan de contingencias en ambientes controlados para familiarizar al personal de contingencias con las instalaciones y los recursos disponibles y evaluar las capacidades del sitio para soportar las operaciones de contingencia.			x	x	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
			agotamiento de recursos									
A.17.2. Redundancia Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.												
A.17.2.1.	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Deficiencias en la organización Caídas por agotamiento de recursos Fallo de servicios de comunicaciones	Existe un sistema de virtualización que soporta caídas, sin embargo los servidores se encuentran desactualizados para prestar eficazmente este servicio.	ASUMIR		Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.			x	x	
A.18. CUMPLIMIENTO.												
A.18.1. Cumplimiento de requisitos legales y contractuales. Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.												

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.18.1.1.	Identificación de los requisitos de legislación y contractuales aplicables.	Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.	Deficiencias en la organización Alteración o destrucción de la información	No se ha tenido la visión de involucrar el tema legal de seguridad de la información	ASUMIR	Se cuenta con la asesoría legal para el tema.	Se deben definir los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos normativos, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.		x	x	x	
A.18.1.2.	Derechos de Propiedad Intelectual.	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.	Deficiencias en la organización Alteración o destrucción de la información	La entidad está en una etapa incipiente en el reconocimiento del registro de propiedad intelectual	ASUMIR		Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores. El procedimiento debe cubrir, como mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual y responsabilidades de conclusión, así como obligaciones (que incluyan cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben	x		x	x	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
							revisar asesores legales.					
A.18.1.3	Protección de registros.	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Deficiencias en la organización Alteración o destrucción de la información	No se cuenta con herramientas eficientes para realizar este tipo de bloqueo.	ASUMIR		Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.	x		x	x	
A.18.1.4.	Privacidad y protección de la información identificable personalmente	Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	Deficiencias en la organización Alteración o destrucción de la información	Se cuenta con la política de protección de datos	ASUMIR	Se cuenta con la política de protección de datos	Se deben establecer procedimientos para manejar la privacidad de la información el cual cubre: a) uso aceptable de la información de identificación personal b) los derechos de las personas sobre los cuales se tiene la información de identificación personal c) la evaluación de la privacidad, los programas de conciencia y cumplimiento d) los requerimientos legales y regulatorios para la privacidad	x		x	x	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
A.18.1.5.	Reglamentación de Controles Criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos	Deficiencias en la organización Alteración o destrucción de la información		EXCLUIR		11.4.6 Regulación de Controles para el Uso de Criptografía			x	x	Se excluye control toda vez que se priorizaran otros controles de seguridad de la información.
A.18.2. Revisiones de seguridad de la información Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.												
A.18.2.1	Revisión independiente de la seguridad de la información.	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, la políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Caídas por agotamiento de recursos Deficiencias en la organización Alteración o destrucción de la información	Falta de auditorías sobre la aplicación	ASUMIR	El área de control interno realiza verificación de procedimientos.	La entidad debe revisar periódicamente la evaluación de riesgos o siempre que se efectúen cambios significativos en los sistemas de información, las instalaciones donde reside el sistema o que existan otras condiciones que pueden impactar la seguridad o el estado de acreditación del sistema.	x		x	x	
A.18.2.2.	Cumplimiento con las políticas y normas de seguridad.	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.	Caídas por agotamiento de recursos Deficiencias en la organización Alteración o destrucción de la información	Políticas de seguridad desactualizadas	ASUMIR		Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas y	x		x	x	

Tabla 11 (continuación) Declaración de aplicabilidad SOA

Política	Descripción	Control ISO 27001:2013	Amenaza	Vulnerabilidad	Tratamiento del riesgo	Control Existente	Control Planeado	Legal	Obligación contractual	Requerimiento del negocio	Análisis de riesgos	Justificación para la exclusión
							procedimientos de seguridad junto con las políticas TI.					
A.18.2.3.	Revisión del Cumplimiento Técnico.	Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Caídas por agotamiento de recursos Deficiencias en la organización Alteración o destrucción de la información	Falta de auditorías sobre la aplicación	ASUMIR		Revisar y ajustar las políticas, estándares, procedimientos y metodologías de TI para garantizar que los requisitos legales, reglamentarios y contractuales son direccionados y socializados.	x		x	x	

Fuente Los autores

15. MANUAL DE POLÍTICAS

INTRODUCCION

El Sistema de Gestión de Seguridad de la Información – SGSI, es parte del Sistema de Gestión Integral - SGI, está basado en un enfoque hacia la gestión de riesgos globales de seguridad dentro del contexto de una organización. Su fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener, y mejorar la seguridad de la información, o sea gestionar la seguridad de la información.

La seguridad de la información se gestiona con elementos como la infraestructura, procesos que apliquen, aspectos legales y contractuales de cumplimiento y el componente humano. Para tener en cuenta que El SGSI no es un área, no es un solo proceso, no es infraestructura, es un sistema y en la compañía aprovechamos esos elementos ya definidos e implementados para gestionar la seguridad de la información, inicialmente en el alcance de certificación y extendiéndose de forma general en la organización.

Este documento contiene el manual de políticas de seguridad de la información para la empresa ESE Hospital Universitario Erasmo Meoz. Se tiene la intención de servir como repositorio centralizado de la información, tareas y procedimientos que serían necesarios para facilitar a la empresa. el proceso de toma de decisiones de la administración y su respuesta oportuna a cualquier interrupción perjudicial o prolongada de operaciones comerciales normales del departamento y servicios. Esto es especialmente importante para que las operaciones y actividades de los empleados sean normales y evitar afectaciones.

A cada individuo que reciba el manual de políticas, o cualquier parte del mismo, o que tiene un papel y / o responsabilidad por cualquier información o materiales contenidos en el documento, asegurar la adecuada y suficiente atención y recursos estén comprometidos con el mantenimiento y la seguridad del documento y su contenido.

El manual debe ser considerado como un documento sensible. Todos los contenidos de la información y materiales de este documento deben ser etiquetados como, "Uso Oficial Únicamente".

OBJETIVO

Dar a conocer a funcionarios, empleados y terceros relacionados con la empresa, las políticas y estándares a cumplir con el fin de mantener la protección y preservación de los activos y la información relacionada y almacenados en estos

ALCANCE

Las políticas estipuladas en este manual aplican para funcionarios, empleados, terceros relacionados con la empresa que utilicen recursos informáticos

NIVEL DE CUMPLIMIENTO

Aquellas personas cubiertas por el alcance y aplicabilidad deberán aplicar en un 100% las políticas estipuladas, quienes incumplan dichas políticas serán objeto de sanción.

SANCIONES POR INCLUMPLIMIENTO

El incumplir con el presente manual será considerado como causa de Responsabilidad administrativa hasta penal, pendiendo de gravedad y afectación, estas sanciones serán aplicadas por las autoridades competentes

REVISIÓN

Esta política será revisada por lo menos una vez al año o cuando se identifiquen cambios en la entidad, su estructura, sus objetivos o alguna condición que afecte la política, para asegurar que sigue siendo adecuada y valida a los requerimientos identificados.

1. Política general

La política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la ESE Hospital Universitario Erasmo Meoz con respecto a la protección de los activos de información (funcionarios, contratistas, terceros, información, procesos, tecnologías de información incluido el hardware y software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados con la misión, visión y funciones de la Institución, ,así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La ESE Hospital Universitario Erasmo Meoz se compromete a salvaguardar la información que genera en la ejecución de sus funciones o la que le es entregada en custodia por clientes dentro de la ejecución de los servicios prestados por la empresa, identificando y mitigando los riesgos asociados mediante la definición de lineamientos y directrices a las dependencias, funcionarios, contratistas, practicantes y todo aquel que tenga interacción con esta información y la utilización físicamente o a través de equipos, plataformas o sistemas de información dispuestos para su gestión y resguardo.

Toda la información que es generada por los empleados, contratistas y practicantes de ESE Hospital Universitario Erasmo Meoz en beneficio y desarrollo de las actividades propias de la empresa es propiedad de la ESE Hospital Universitario Erasmo Meoz., a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la información que pueda ser adquirida o cedida a la Institución de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la Institución.

La ESE Hospital Universitario Erasmo Meoz. protege la información creada, procesada, transmitida o resguardada por los procesos de su competencia, su infraestructura tecnológica y activos, del riesgo que se genera con los accesos otorgados a terceros (ej.: contratistas, proveedores o ciudadanos), o como resultado de servicios internos en outsourcing.

La ESE Hospital Universitario Erasmo Meoz protege la información creada, procesada, transmitida o resguardada por sus procesos de operación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

La ESE Hospital Universitario Erasmo Meoz realiza aseguramiento de las instalaciones físicas de la entidad y las áreas de procesamiento de información, con el fin de enviar el acceso físico no autorizado, la interferencia o daño de la información propia o de terceros resguardada por la entidad.

La ESE Hospital Universitario Erasmo Meoz realiza aseguramiento a través de una adecuada gestión, de los eventos de seguridad y las debilidades asociadas con los sistemas de información o para una mejora efectiva de su modelo de seguridad.

La ESE Hospital Universitario Erasmo Meoz da cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en materia de seguridad de la información.

2. Política de Gestión de Activos

Los activos de información son clasificados de acuerdo a la criticidad, sensibilidad y reserva de la misma. Se realiza etiquetado de la información identificando el responsable del mismo.
Una vez finalizada el empleo, el funcionario debe realizar entrega a su jefe inmediato de los activos físicos y de la información realizando un acta de entrega y con este el llenado del “Paz y salvo” para continuar con los trámites de finalización del empleo.

Se prohíbe el uso del almacenamiento de archivos on line, es decir, en aquellas unidades virtuales de almacenamiento personal por medio de internet. Por lo que se prohíbe: Almacenar o transportar información clasificada o reservada, ejecutar

cualquier tipo de programa no autorizado por la empresa desde cualquier de las unidades de almacenamiento externo, descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en los equipos informáticos.

Los recursos informáticos que tiene dispuesta la empresa, no deben ser utilizados para el almacenamiento de información que no es para propósitos laborales, por ejemplo: música, videos, películas, fotos.

Avisar con antelación a la coordinación de TI para cualquier tipo de traslado de recursos informáticos, a fin de garantizarse el correcto funcionamiento posterior de los mismos.

En el evento de un traslado de equipo o de información, se deben tomar las precauciones necesarias para no realizar borrado de información sensible para la empresa; por tal motivo se recomienda que siempre sea bajo la supervisión de la oficina de sistemas.

El Backup de la información está bajo la responsabilidad de la oficina de sistemas, sin embargo, el usuario debe velar porque éste se realice periódicamente.

Los equipos móviles que tendrán acceso a la red de datos de la empresa deberán estar debidamente autorizados por la Gerencia de la empresa.

3. Política de seguridad de los recursos humanos

Se realizará verificación del personal al momento de la postulación para la contratación.

Al momento de la terminación de contrato o finalización de labores de un tercero o funcionario, debe ser informado por la oficina de Talento humano a la oficina de sistemas para que sean inactivos los usuarios y sean eliminados los accesos a la red y sistemas de información que tenga asociados.

La oficina de sistemas con el coordinador de área debe revisar periódicamente los accesos y permisos asignados a los usuarios.

Al ingreso de funcionarios, terceros, estudiantes, deberán conocer y apropiar la presente política de seguridad de la información.

Los funcionarios, terceros y/o estudiantes deben reportar a la oficina de sistemas los eventos detectados o potenciales u otros riesgos de seguridad para la entidad.

Se debe resguardar la reserva de los documentos y bases de datos que contengan información personal de funcionarios y terceros que laboran o laboraron en la entidad.

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo. De igual manera, se firmarán un Compromiso de confidencialidad o no divulgación, en lo que respecta al tratamiento de la información. La copia de este compromiso deberá ser archivada de forma segura por el área de talento humano.

La Gerencia de la ESE Hospital Universitario Erasmo Meoz promoverá la capacitación y formación de su talento humano en los temas relacionados con la seguridad de la información; de igual manera estos funcionarios deberán replicar en el resto de personal los conocimientos adquiridos.

4. Política de Acuerdos de Confidencialidad

Todo aspirante a un determinado cargo dentro de la empresa ESE Hospital Universitario Erasmo Meoz, deberá firmar un acuerdo de confidencialidad, en el cual acepta las cláusulas que se le exponen sobre la seguridad de la información.

El líder de Talento humano y los supervisores en su defecto, deberá revisar los contratos y asegurar de que se estén cumpliendo las cláusulas de confidencialidad.

Se deben ejecutar revisiones y auditorías en la prestación de servicios por terceros en cuanto al cumplimiento de las cláusulas de confidencialidad incluidas en los contratos.

5. Política de Acceso físico

La empresa destinará un área de acceso restringido, donde se ubicarán los servidores o almacenamiento de información, la infraestructura que soporta los sistemas de información y comunicaciones, por lo cual se deben emplear mecanismos de control de acceso físico que garanticen que sólo se permite el acceso al personal autorizado.

Las áreas de acceso restringido, deben contar con buenas condiciones ambientales tanto de temperatura, humedad, polvo, especificados por los fabricantes de los equipos en funcionamiento, y contar además con las hojas de vida de cada equipo, con su historial de mantenimientos preventivos y correctivos.

El acceso a las áreas restringidas por parte del personal de soporte técnico de proveedores se debe solicitar por medio de una autorización, con supervisión del encargado del área tecnológica.

No se permitirá tomar fotografías o grabaciones de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la empresa, a menos que esté autorizado.

Todos los proveedores y contratistas deben portar en un lugar visible el carnet que los identifica para el acceso a la Empresa y mientras se encuentren dentro de ella.

Para mover, cambiar o extraer equipo de cómputo, el encargado del área tecnológica deberá diligenciar su salida, a través de formatos de autorización de Entrada/Salida, los cuales deberá ser notificado y firmado por alguna de las personas delegadas por el Gerente para dar esta autorización.

6. Política de respaldo

Se debe asegurar que la información perteneciente a la Empresa, guardada en archivos de red, bases de datos, correos electrónicos, sean periódicamente resguardada mediante lineamientos y controles adecuados que establezcan su identificación, fecha de respaldo, ubicación y garanticen la protección, confidencialidad, integridad y disponibilidad de la información.

Se debe seleccionar los medios de almacenamiento adecuados de buena calidad para guardar la información de las copias de respaldo, almacenándolas en otra ubicación diferente a las instalaciones donde se encuentra en funcionamiento. El sitio debe ser un sitio externo donde se resguardan dichas copias, cumpliendo con los mismos controles de seguridad adecuados, teniendo en cuenta todas las medidas de protección y seguridad física. Si es posible adquirir un espacio en cloud para el almacenamiento más seguro de estas copias de seguridad.

7 Política de uso de internet

El acceso a internet tiene uso exclusivo para razones y causas laborales

La red y el servicio de internet del hospital solo deberán ser usados con fines laborales, administrativos, técnicos y de promoción del hospital. Abstenerse de ingresar a páginas con contenido pornográfico, juegos, ocio y diversión, ya que constantemente se hace un control de navegación para verificar el buen uso del mismo.

Actividades prohibidas:

- No descargar archivos no legales, música, video ni demás contenido multimedia.
- No abrir mensajes no solicitados ni aquellos que no tengan que ver con la entidad

- No abrir archivos que no tengan nada en común con lo solicitado por la entidad.

8 Política de uso de correo electrónico institucional

La asignación del correo electrónico institucional es para uso estrictamente laboral, abstenerse de enviar información que no corresponda con el cumplimiento de sus funciones.

El correo institucional deberá ser asignado por el área de sistemas para cada empleado

No se permite el envío de correos o mensajes que atenten contra la dignidad de funcionarios ni usuarios asociados a la empresa

Los correos enviados por la empresa deben contener su respectiva firma digital con los datos de acuerdo a cada área en específico.

Se prohíbe:

- el envío de spam a usuarios o clientes con fines comerciales,
- cometer acciones ilícitas desde el correo institucional,
- no se permite el envío de archivos ejecutables

El servicio de correo electrónico, es un servicio gratuito, se debe hacer buen uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red del hospital.

El correo electrónico es de uso exclusivo, para los empleados.

El usuario será responsable de la información que sea enviada con su cuenta.

9 Política de control de acceso lógico

Los empleados o usuarios son responsables de las cuentas de usuario y claves asignadas con las cuales se va a acceder a la información y a la infraestructura tecnológica de la Empresa.

Los accesos remotos solo se permiten con previa autorización del departamento de sistemas los cuales determinan los permisos y niveles de acceso a los documentos físicos y digitales

Actividades prohibidas

- No está permitido el acceso a departamentos distintos a sus funciones donde los sistemas soliciten autenticación
- No está permitido el uso de dispositivos o equipos que no estén a cargo del empleado y que no sean usados dentro de sus funciones
- No intentar, ni acceder a las bases de datos con información importantes, este acceso solo es permitido al personal con autorización.

10. Política de uso de software

Los usuarios autorizados deberán solicitar la aprobación del encargado del sistema antes de instalar cualquier software que no haya sido aprobado previamente para su uso.

No está permitida la distribución por cualquier medio, de software propiedad o con licencia de la entidad ESE Hospital Universitario Erasmo Meoz a personal no autorizado.

Cada usuario es responsable de los recursos tecnológicos que le hayan sido asignados dentro de la institución y a estos se les realizará periódicamente una auditoría interna para verificar la legalidad del software instalado; en caso de encontrar software que afecte el rendimiento del equipo, este será considerado como ilegal y es responsabilidad exclusiva del usuario designado.

11. Política de contraseñas

Es responsabilidad de cada uno de los funcionarios que posean cuenta de usuario para el acceso a la red o los sistemas de información de la empresa hacer buen uso de la misma, no divulgando ni escribiendo la contraseña en lugares visibles.

La contraseña de la cuenta de usuario asignada por primera vez debe ser inmediatamente cambiada en el primer inicio de sesión, cumpliendo con los siguientes requisitos:

- Tener mínimo ocho caracteres.
- Contener caracteres de dos de las tres siguientes clases de caracteres:
- Caracteres en mayúsculas y minúsculas (es decir, Aa-Zz)
- Base de 10 dígitos (es decir, 0-9)
- Puntuación y otros caracteres (es decir: !@#$%^&*()_+|~-=\ `{}[]:";'<>?,./).

Se debe exigir el cambio de contraseña de red y del correo institucional cada 90 días, advirtiendo sobre éste cambio al usuario a partir de 5 días antes de su vencimiento.

El encargado del sistema no restablecerá la contraseña a un usuario, a menos que este mismo lo solicite y se identifique a sí mismo.

El usuario debe evitar mantener un registro (por ejemplo, en papel, archivos electrónicos) de las contraseñas, a menos que se pueda almacenar de forma segura y el método de almacenamiento haya sido aprobado por el encargado de sistemas de la empresa.

Todo usuario autorizado debe cambiar las contraseñas cada vez que exista o haya algún indicio de una posible vulnerabilidad del sistema.

Las contraseñas de las cuentas para operar los sistemas son intransferibles, y las consecuencias por la mala utilización de las mismas son de exclusiva responsabilidad del propietario de la cuenta.

12. Política de protección contra software malicioso

Se debe tener instalado como mínimo un software antivirus que brinde protección contra código malicioso en todos los recursos informáticos de la empresa, asegurándose que estas herramientas no puedan ser deshabilitadas, así como de su actualización permanente.

Cada uno de los funcionarios y terceros deben revisar previamente al acceso el dispositivo de almacenamiento removible con el antivirus. Cada uno es responsable por la seguridad física y lógica del dispositivo con el fin de no poner en riesgo la información de la empresa ESE Hospital Universitario Erasmo Meoz.

No está permitida la utilización de medios de almacenamiento virtual que no estén previamente autorizados por el encargado de sistemas.

No está permitida la generación, propagación, ejecución o introducción de cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica de la empresa.

No se permite la instalación de software de espionaje, monitoreo de tráfico o programas maliciosos que atenten contra los sistemas de información relacionados a los servicios entregados por el HUEM.

13. Política de equipo desatendido.

El área de Sistemas, garantizará que todos los equipos de cómputo tengan instalados controles de accesos como contraseñas y protectores de pantalla, el cual se activará si el equipo se deja desatendido después de cierto tiempo (15 minutos).

14. Política de intercambio de información

La entidad firmara acuerdos de confidencialidad y responsabilidades, con los usuarios que intercambien información de la empresa ESE Hospital Universitario Erasmo Meoz

Todos los funcionarios y terceros de la empresa ESE Hospital Universitario Erasmo Meoz, son responsables de la confidencialidad, intercambio e integridad de la información y de los medios utilizados con el fin de no permitir una divulgación o modificación no autorizada.

Los empleados y terceros de la empresa ESE Hospital Universitario Erasmo Meoz, son responsables de la información que requieren intercambiar y son responsables de implementar controles que garanticen los criterios de confidencialidad, integridad y disponibilidad requeridos.

15. Política de gestión de incidentes

La empresa ESE Hospital Universitario Erasmo Meoz, debe definir y seguir los procedimientos para la gestión de los incidentes de seguridad de la información que garantice la ejecución de las actividades de planificación, atención de incidentes y mejora continua para enfrentar nuevos incidentes.

Los empleados y terceros de la empresa ESE Hospital Universitario Erasmo Meoz, están en la obligación de informar de cualquier evento que afecte la confidencialidad, integridad o disponibilidad de los recursos de las Tecnologías de la Información y las Comunicación (TIC) al área de Sistemas

El equipo de soporte técnico de TI es el único autorizado para realizar funciones de mantenimiento y configuración de los diferentes elementos de comunicación que utilizan los usuarios.

16. PLAN DE CONTINUIDAD DEL NEGOCIO

Es importante contar con un plan de continuidad del negocio que garantice de forma ordenada las actividades a seguir en casos en que se materialice alguna amenaza y por lo tanto se hace de suma importancia que este plan sea ampliamente conocido por todos los empleados de la organización que tienen contacto directo con procesos en los cuales tiene injerencia directa el área de tecnología de información y comunicación.

16.1 FASE I. ANALISIS DEL NEGOCIO Y EVALUACION DE RIESGOS

Marco contextual
El marco contextual se encuentra en el punto 5.2 del presente documento, en donde se conoce la funcionalidad de la empresa, capacidad instalada para la prestación de servicios, la plataforma estratégica, organigrama institucional.

Identificación de procesos misionales
Se encuentra en el punto 5.3 del presente documento con el mapa de procesos vigente.

Relación de departamentos y usuarios
Encontramos el organigrama institucional en el punto 5.2.3

Tabla 12. Procesos de la entidad

Nombre del proceso	Descripción del proceso	Responsable
PROCESOS ESTRATÉGICOS		
Gestión Jurídica	Buscar que las actuaciones de la ESE HUEM y sus servidores públicos estén siempre enmarcadas en la normatividad legal vigente, asegurando la defensa de los intereses de la entidad.	Asesor jurídico
Planeación Estratégica y gerencial	Formular, diseñar y establecer las políticas, orientaciones, estrategias, planes, programas y proyectos de la entidad orientados a una gestión por resultados	Asesor de Planeación y calidad
PROCESOS MISIONALES		
Apoyo diagnóstico y terapéutico	Realizar actividades de apoyo diagnóstico y terapéutico que contribuyan a brindar a los médicos las herramientas de diagnóstico e intervención temprana en los procesos de enfermedad para el restablecimiento de la salud del paciente.	Líder de apoyo diagnóstico

Continuación Tabla 12 – Procesos de la entidad

Nombre del proceso	Descripción del proceso	Responsable
Consulta externa	Desarrollar actividades, intervenciones y procedimientos programados ambulatoriamente que se prestan al usuario que requiere de una atención en salud	Líder de servicios ambulatorios
Docencia e investigación	Ser un instrumento fundamental como escenario de prácticas en el desarrollo de acciones educativas, con las que se apoye el fortalecimiento de programas de formación académica de profesionales, tecnólogos, técnicos y auxiliares, así como el desarrollo de programas de extensión a la comunidad en general e investigación, para lo cual pone a disposición sus recursos humanos, infraestructura física, dotación y tecnológica con el objeto de favorecer los más rigurosos procesos de aprendizaje y, por ende, el logro de las competencias requeridas en los respectivos desempeños laborales de cada una de las disciplinas en formación, perfeccionando habilidades y destrezas como mecanismos de generación de conocimiento a los futuros profesionales, garantizando siempre una prestación del servicio con calidez y calidad	Coordinador de Docencia e investigación
Hospitalización	Prestar los servicios en hospitalización a usuarios con patologías de II, III y IV nivel de complejidad incluidas en el portafolios de servicio institucional, de conformidad con los requisitos legales, los del servicio, y las expectativas razonables del usuario	Subgerente de servicios de salud
Servicios quirúrgicos	Prestar servicios en salud que requieran una terapéutica segura, oportuna, humana y de calidad, acorde al nivel de complejidad de la institución, para contribuir a mejorar el estado de salud-enfermedad del usuario	Líder de Servicios quirúrgicos
Urgencias	Prestar servicios en salud que requieran atención Urgente y/o prioritaria en donde, prevalezca la vida cumpliendo los parámetros científicos, éticos y legales con el fin de estabilizar y definir conducta al usuario.	Líder de Servicios ambulatorios

Continuación Tabla 12 – Procesos de la entidad

Nombre del proceso	Descripción del proceso	Responsable
PROCESOS DE APOYO		
Adquisición de bienes y servicios	Asegurar la adquisición oportuna de bienes y servicios requeridos por las dependencias de la ESE HUEM, para el desarrollo de sus actividad y cumplimiento de los objetivos misionales de la institución, de acuerdo a los criterios de eficiencia, eficacia, economía, transparencia, publicidad, celeridad, imparcialidad, selección objetiva y demás principios que rigen la contratación.	Líder de Recursos físicos
Gestión de información y comunicaciones	Administrar los sistemas de información y comunicación institucional que permitan el suministro de información adecuada y oportuna a los clientes internos y externos.	Asesor de planeación y calidad
Gestión de Talento Humano	Planear, programar y ejecutar actividades de administración, formación y bienestar del talento humano para promover el desarrollo humano de la Entidad y propiciar un ambiente laboral y clima organizacional acorde a los objetivos y metas institucionales.	Líder de Talento humano
Gestión financiera	Desarrollar y ejecutar actividades de administración eficiente de los recursos financieros de la ESE HUEM buscando que sea una entidad auto sostenible y/o rentable, brindando información clara y concisa para la toma de decisiones y presentando informes sobre la gestión y movimientos financieros ante los órganos de control externos.	Líder de Recursos financieros
PROCESOS DE EVALUACIÓN		
Evaluación del sistema de Control Interno	Siguiendo lo planteado por el Modelo Estándar de Control Interno este proceso es el “Conjunto de Elementos de Control que garantiza el examen autónomo y objetivo del Sistema de Control Interno, la gestión y resultados corporativos de la Entidad Pública por parte de la Oficina de Control Interno, Unidad de Auditoría Interna o quien haga sus veces. Presenta como características la independencia, la neutralidad y la objetividad de quien la realiza y debe corresponder a un plan y a un conjunto de programas que	Asesor de Control Interno

Continuación Tabla 12 – Procesos de la entidad

Nombre del proceso	Descripción del proceso	Responsable
	establecen objetivos específicos de evaluación al control, la gestión, los resultados y el seguimiento a los Planes de Mejoramiento de la Entidad	
Garantía de calidad	Promover el mejoramiento continuo en la calidad de la atención en salud de la ESE HUEM, mediante la implementación de elementos de evaluación y monitorización periódicos que permitan comparar la calidad esperada, para establecer acciones de mejora que garanticen la satisfacción de los usuarios.	Asesor de planeación y calidad
Vigilancia epidemiológica	Identificar eventos de interés en salud pública de acuerdo a los lineamientos establecidos por el Ministerio de la Protección Social esto con el fin de obtener datos para establecimiento de estrategias de medidas de prevención y control.	Coordinador de Epidemiología.

Fuente: Caracterización de procesos

Relación de aplicaciones
Se encuentra en el presente documento en el punto en el punto 9 Inventario de activos de la institución – Software.

Análisis de riesgos
Se aplica la metodología MAGERIT, de la cual se encuentra su explicación en el punto 5.1.6 del presente documento. Para el desarrollo de la metodología, se encuentra evidencia en el punto 12 – Amenazas, 13 – Identificación de amenazas y valoración de riesgos.

16.2 FASE II– SELECCIÓN DE ESTRATEGIAS

Objetivo

- Analizar y tomar medidas concretas frente a interrupciones en el servicio puesto que, teniendo en cuenta la misión de la entidad, no se puede detener nunca la prestación de los servicios.
- Implementar controles para mitigar o prevenir hechos similares en el futuro
- Garantizar la efectividad de las operaciones de contingencia con el establecimiento de planes que incluyan la detección y determinación del daño, restauración de las operaciones y recuperación del daño al sistema

original y la restauración del sistema a las condiciones normales de operación.

Para el desarrollo del presente plan se tienen en cuenta los riesgos y vulnerabilidades frente a las cuales está expuesta la organización y que han venido siendo consideradas en el presente trabajo a través del análisis de riesgos.

16.3 FASE III- DESARROLLO DEL PLAN

Fallos en Servidor (software):

- Comunicar a la comunidad hospitalaria el inconveniente presentado a través del sistema de mensajería institucional. En caso que este también se encuentre afectado realizar recorrido por la institución empezando por las áreas de urgencias y servicios asistenciales.
- Utilizar los formatos y/o manuales previamente establecidos en el listado maestro de documentos para continuar la operación manualmente mientras se recupera el sistema.
- Cuando se reestablezcan las operaciones se deben realizar pruebas y comunicar igualmente el fin de la contingencia.
- El personal encargado deberá alimentar el sistema de información reestablecido con la información que se llevó manualmente durante la contingencia.
- Realizar auditoria para verificar que la información del sistema concuerde con lo que fue llevado a mano durante la duración de la contingencia.

Fallos en Servidor (Hardware):

Puede producir Pérdida de Hardware y Software, perdida del proceso automático de backup e Interrupción de las operaciones. Las actividades a seguir en este caso serán:

- Comunicar a la comunidad hospitalaria el inconveniente presentado a través del sistema de mensajería institucional. En caso que este también se encuentre afectado realizar recorrido por la institución empezando por las áreas de urgencias y servicios asistenciales.

- Utilizar los formatos y/o manuales previamente establecidos en el listado maestro de documentos para continuar la operación manualmente mientras se recupera el sistema.

- Bajar el sistema y apagar el equipo.

- Determinar el origen de la falla para estimar el tiempo estimado de desconexión

- Si no se puede recuperar rápidamente el servidor afectado reemplazando la pieza dañada entonces se procederá a montar la última copia de seguridad que se tenga en otro de los servidores de la organización para restablecer el servicio, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.

- Realizar pruebas locales para verificar el correcto funcionamiento de la aplicación

- Habilitar las entradas para los usuarios

- Comunicar el fin de la contingencia

- El personal encargado deberá alimentar el sistema de información restablecido con la información que se llevó manualmente durante la contingencia.

- Realizar auditoria para verificar que la información del sistema concuerde con lo que fue llevado a mano durante la duración de la contingencia.

Recursos de Contingencia
- Servidor de contingencia
- Componente de Remplazo (Memoria, Disco Duro, etc.).
- Backup diario de información del servidor

Perdida de servicio internet:
- Comunicar a la comunidad hospitalaria el inconveniente presentado a través del sistema de mensajería institucional. En caso que este también se encuentre afectado realizar recorrido por la institución empezando por las áreas administrativas donde el uso de este servicio sea más sensible.

- Realizar pruebas para identificar posible problema dentro de la entidad

- Si se evidencia problema en el hardware, se procederá a cambiar el componente

- Si se evidencia problema con el equipo de borde (FORTIGATE) se procederá a revisar revisión en la configuración de este.

- Si no se evidencia falla en los equipos de la entidad, se procederá a comunicarse con la empresa prestadora del servicio, para asistencia.

- Si el servicio no se puede restablecer rápidamente o el proveedor informa que la caída se extenderá por mucho tiempo entonces se procederá a configurar el servicio de internet alternativo de la entidad.

- Es necesario registrar la avería para llevar un historial que servirá de guía para futuros daños.

- Realizar pruebas de operatividad del servicio y comunicar su restablecimiento.

Recursos de Contingencia
- Router
- Software
- Herramientas de Internet.

Perdida del servicio de correo electrónico
Para restablecer los servicios de correo electrónico se deben seguir los siguientes pasos:
- Comunicar a la comunidad hospitalaria el inconveniente presentado a través del sistema de mensajería institucional.

- Se desconecta totalmente de la red el servidor de correo electrónico ESX1 que es donde se encuentra actualmente alojado el servidor.

- Realizar pruebas y verificar si se puede corregir el inconveniente

- En caso que no se pudiera corregir el inconveniente se procederá a restablecer las copias de configuración del servicio.

- Reiniciar los servicios de correo y verificar que el servicio quede funcionando.

- Comunicar el restablecimiento del servicio a toda la comunidad hospitalaria

Recursos de Contingencia

- Manual de funciones actualizado del Administrador del sistema
- Relación de los sistemas de información de la organización
- Copia de la configuración del servidor de correo correctamente almacenada

Daño total o parcial en equipo de cómputo:

En caso de daño total o parcial de algún pc de cómputo se realizará lo siguiente:

- Verificar el daño en sitio y verificar si se puede arreglar allí mismo o si es necesario trasladarlo al taller ubicado en la oficina de sistemas

- Informar al líder o encargado de la oficina que el pc va a ser retirado del sitio (en caso de ser necesario)

- En caso que la falla sea muy grave y de la relevancia de las labores efectuadas en el pc averiado se procederá a pasar la información del disco duro del pc dañado a un pc temporal que será ubicado en el mismo lugar donde fue retirado el pc mientras se realiza el arreglo del pc averiado.

- Cuando el pc sea reparado se volverá a realizar el intercambio de equipos pasando los archivos actualizados al pc reparado y luego borrándolos del pc temporal para tenerlo listo en caso que se dañe algún pc en otra área.

- Informar al líder y a los usuarios del pc que ya fue retornado el pc al sitio de trabajo.

16.4 FASE IV- PRUEBAS Y MANTENIMIENTO

El plan de continuidad debe ser revisado y actualizado periódicamente y ser una parte integrada en los diversos procesos de las diferentes áreas de la empresa.

Cuando el administrador de la red se encuentre ausente se recomienda capacitar a una persona que pueda hacer lo mínimo indispensable para levantar todos los servicios, a fin de que la operación básica de la organización no se vea interrumpida.

Tener actualizados los contratos de garantía y licencias tanto de hardware como de software, así como pólizas de aseguramiento.

Hacer de conocimiento general el contenido del presente plan de continuidad del negocio, con la finalidad de instruir adecuadamente al personal de la Ese Hospital Universitario Erasmo Meoz.

17. DIVULGACIÓN

La comunicación y sensibilización son elementos básicos para el éxito en la implementación del SGSI planteado en este documento; por ello, éste será publicado en la biblioteca virtual de la UNAD para que sirva de guía a otros compañeros que estén trabajando en el tema, adicionalmente la Gerencia del hospital con el apoyo de la Oficina Asesora de Planeación y Calidad y la oficina de TI, debe asignar responsabilidades definidas en el modelo y procurar porque esté suficientemente capacitado y culturizado. Además, deberá:

- Establecerlos requerimientos necesarios para el personal que realiza las actividades en la implementación del modelo SGSI
- Incluir actividades de capacitación y formación al equipo
- Evaluar la eficacia de las acciones realizadas

La entidad también debe procurar la publicación de la política de seguridad de la información de tal manera que todo el personal la conozca y la apropie, para ello se sugiere que sea publicada en los diferentes medios que usa la entidad como página web, intranet, INFOHUEM; y que ésta se comunique y se encuentre dentro del proceso de inducción y reinducción en la entidad, para garantizar que todo personal que ingrese nuevo la conozca y así mismo los que ya se encuentran vinculados la apropien.

La oficina de TI, a través de correo electrónico, mensajería instantánea, carteleras debe realizar un proceso permanente de socialización de las políticas. De igual manera debe hacer seguimiento a los controles establecidos y re-alimentación si se deben ajustar e informar a la dirección y a las autoridades pertinentes.

RECOMENDACIONES

La dirección del hospital está comprometida y apoya el proceso de implementación de un SGSI, por ello se han hecho diferentes cambios al interior de la oficina de TI, sin embargo, se debe procurar por ampliar el conocimiento de seguridad al interior de la entidad, promoviendo un cambio de cultura y de cuidado frente al manejo de la información en general.

El tema de seguridad de la información al interior de la oficina TI debe ser mejorado, se deben establecer responsabilidades y compromiso en los diferentes actores, ya que el eslabón más débil en esta cadena es el usuario. Por el exceso de trabajo en ocasiones los responsables y administradores de los sistemas y aplicaciones solo centran su atención en la funcionalidad y disponibilidad de los mismos perdiendo de vista la imperiosa necesidad de construir e implementar escenarios óptimos que permitan contrarrestar las amenazas que se ciernen sobre la información.

Las actuales prácticas por parte de algunos de los miembros del departamento TI, evidencian que desconocen las recomendaciones de buenas prácticas conocidas actualmente. Lo que genera situaciones riesgosas que podrían vulnerar la seguridad de la información y los recursos tecnológicos sobre la que esta se administra.

Es necesario diseñar estrategias para garantizar la difusión del presente manual y ajustar los procedimientos de inducción al personal para que al momento de ingresar a prestar funciones o servicios tenga conocimiento de las presentes políticas de seguridad informática y demás disposiciones de la empresa ESE Hospital Universitario Erasmo Meoz, para que de esta forma tenga claro las obligaciones para con los usuarios y las sanciones que pueden acarrear su incumplimiento, y los documentos en las que están consignadas.

CONCLUSIONES

Basados en el levantamiento de información realizado, el conocimiento de la organización, los conceptos de los diferentes actores involucrados en el proceso de Gestión de la Información, los resultados del análisis de riesgos practicados sobre los activos de la información del área TIC de la ESE Hospital Universitario Erasmo Meoz, se requiere pronto y oportunamente la aplicación de un Sistema de Gestión de Seguridad de la Información para garantizar la integridad, confidencialidad y disponibilidad de la información.

MAGERIT como metodología para el Análisis de Riesgos se basa en conocer a la empresa y saber qué le puede pasar. Aquí se detallan entonces cuales son los activos, se valoran, se detectan sus amenazas, se determina el impacto que tendrían, el riesgo y la selección de salvaguardas; después de este análisis se evidencia que los activos más importantes en la organización son los de Datos e Información y los de Servicios.

Un Sistema de Gestión de Seguridad de la Información (SGSI), se constituye en una excelente alternativa para contribuir efectivamente a la seguridad de la información. A través del SGSI el departamento de TI podrá tener herramientas para aplicar la política, establecer controles, realizar verificación y realizar ajustes cumpliendo con el proceso de PHVA. Se traducirá en un manejo responsable y seguro de la información y los recursos tecnológicos alrededor de la misma, mediante la aplicación de la metodología.

El Plan de continuidad es un conjunto de procedimientos alternativos al orden normal de una empresa, cuyo fin es permitir su funcionamiento continuo, aun cuando alguna de sus funciones se vea afectada por un accidente interno o externo. Que una Entidad prepare su Plan de Contingencia, supone un avance a la hora de contrarrestar cualquier eventualidad, que puedan acarrear importantes pérdidas y llegado el caso no solo materiales sino personales y de información.

BIBLIOGRAFIA

BERNAL LOPEZ, W. (16 de 05 de 2015). Diagnosticar y asesorar la implantación de un sistema SGSI que permita controlar y gestionar todos los procesos relacionados con la información. Obtenido de http://hdl.handle.net/10596/3509

BORAU, P. (31 de 07 de 2012). Sistemas de Información en la Empresa. Obtenido de http://siempresa.blogspot.com.co/2012/07/sgsi-sistemas-de-gestion-de-la.html

CEPEDA, L. E. (2016). *Análisis para la implementación de un Sistema de Gestión de la Seguridad de la Información según la norma ISO 27001 en la empresa SERVIDOC S.A.* Cali: UNAD.

COMUNICACIONES, M. d. (s.f.). *MINTIC - Todos por un nuevo país.* Obtenido de http://www.mintic.gov.co/

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. (2012). *Compendio, tesis y otros trabajos de grado.* Bogotá: ICONTEC.

ISOTOOLS EXCELLENCE. (07 de 05 de 2015). SGSI Blog especializado en Sistemas de Gestión. Obtenido de http://www.pmg-ssi.com/2015/05/por-que-implantar-un-sgsi-basado-en-la-norma-iso-27001/

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAs - Secretaría de Estado de Administraciones Públicas. (s.f.). *PAe Portal administración electrónica*. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WDdhvbLhCM8

MORENO, Y. P. (11 de 2014). *Gerencie.com*. Obtenido de http://www.gerencie.com/ciclo-phva.html

PORTILLA, D. O. (2015). *Diseño de un sistema de gestión de Seguridad de la Información (SGSI) para el área de informática de la Cooperativa del Magisterio de Túqueres bajo la norma ISO 27001:2013.* San Juan de Pasto.

PULIDO BARRETO, A. (16 de 04 de 2016). Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. Obtenido de Recuperado de http://hdl.handle.net/10596/6327

QUINTERO MADROÑERO, J. (2015). Creación e implantación del sistema de gestión de seguridad de la información (SGSI) bajo el estándar ISO/IEC 27001:2013 para la institución educativa Luis Carlos Galán de Villagarzón Putumayo. Obtenido de Recuperado de http://hdl.handle.net/10596/3625

RIESGOSCONTROLINFORMATICO. (s.f.). *Riesgos informáticos*. Obtenido de http://riesgoscontrolinformatico.blogspot.es/tags/metodologia-coras/

ANEXOS

Anexo A Carta de aval de la entidad

E.S.E. Hospital Universitario ERASMO MEOZ

13-

S.A.

Cúcuta, 18 OCT 2016

Señores

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

Atn. Ing. Manuel Antonio Sierra – Tutor de Proyecto de Seguridad Informática

Ciudad

Reciba un cordial saludo:

La ESE Hospital Universitario Erasmo Meoz, dentro de sus principios institucionales cuenta con el valor de "Orientar el trabajo en equipo para el logro de los resultados" y en aras de evaluar y mejorar sus procesos, brinda su aval a dos de sus agremiados partícipes CHERLY LILIANA LEAL SANDOVAL quien labora en la Oficina Asesora de Planeación y Calidad y a JAVIER RICARDO TARAZONA ANTELIZ quien presta sus servicios en la Oficina de Sistemas, para realizar un proyecto de grado para la Especialización de Seguridad Informática.

Esperando el logro de los objetivos planeados sean beneficiosos para la institución.

Atentamente,

SORAYA TATIANA CACERES SANTOS
Asesora de Planeación y Calidad

UN NORTE PRODUCTIVO PARA TODOS

Av. 11E No. 5AN-71 Guaimaral - PBX: (57) 574-6888
www.herasmomeoz.gov.co
Cúcuta - Norte de Santander

Gobernación de Norte de Santander

Anexo B Análisis de riesgos

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
ACTIVOS DE INFORMACIÓN	**Información física**																				
	[I.1] Fuego	1	5	3	1	1	1	5	3	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	1.0	0.3	0.3	0.3
	[I.2] Daños por agua	2	5	3	1	1	1	10	6	2	2	2	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	3.3	2.0	0.7	0.7	0.7
	[I.7] Condiciones inadecuadas de temperatura o humedad	3	5	3	1	1	1	15	9	3	3	3	Controlar	Detectivo	11.2.1. Ubicación y protección de los equipos	4	3.8	2.3	0.8	0.8	0.8
	[I.10] Degradación de los soportes de almacenamiento de la información	3	4	4	1	1	1	12	12	3	3	3	Aceptar	Preventivo	8.2.3. Manejo de Activos 11.1.4. Protección contra amenazas externas y ambientales 1.2.1. Ubicación y protección de los equipos	4	3.0	3.0	0.8	0.8	0.8
	[E.7] Deficiencias en la organización	3	3	2	2	2	2	9	6	6	6	6	Controlar	Detectivo	6.1.1. Seguridad de la Información Roles y Responsabilidades	4	2.3	1.5	1.5	1.5	1.5
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Detectivo	7.2.3. Proceso disciplinario A.18.1.3. Protección de registros	3	0.7	1.3	1.3	0.7	0.7
	[A.15] Modificación deliberada de la información	1	2	5	3	2	1	2	5	3	2	1	Aceptar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 12.3.1. Copias de respaldo de la información	3	0.7	1.7	1.0	0.7	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														A.18.1.3. Protección de registros						
[A.18] Destrucción de información	1	2	5	3	3	2	2	5	3	3	2	Controlar	Correctivo	9.2.3. Gestión de derechos de acceso privilegiado 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	3	0.7	1.7	1.0	1.0	0.7
[A.24] Denegación de servicio	4	5	2	1	1	1	20	8	4	4	4	Controlar	Preventivo	11.2.4. Mantenimiento de equipos	2	10.0	4.0	2.0	2.0	2.0
Información Digital																				
[I.3] Contaminación mecánica	3	4	2	1	1	1	12	6	3	3	3	Aceptar	Preventivo	11.2.1. Ubicación y protección de los equipos	4	3.0	1.5	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Controlar	Preventivo	8.2.3. Manejo de Activos 8.3.3. Transferencia de medios de soporte físicos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	3	4	1	1	1	1	12	3	3	3	3	Transferir	Preventivo	11.1.4. Protección contra amenazas externas y ambientales	4	3.0	0.8	0.8	0.8	0.8
[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	1	1	1	1	8	2	2	2	2	Controlar	Detectivo	11.1.4. Protección contra amenazas externas y ambientales 11.2.1. Ubicación y protección de los equipos	3	2.7	0.7	0.7	0.7	0.7
[I.10] Degradación de los soportes de almacenamiento de la información	2	5	3	1	1	1	10	6	2	2	2	Controlar	Preventivo	8.2.3. Manejo de Activos 11.1.4. Protección contra amenazas externas y ambientales	2	5.0	3.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															1.2.1. Ubicación y protección de los equipos							
	[E.1] Errores de los usuarios	3	4	5	4	1	1	12	15	12	3	3	Controlar	Detectivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	3.0	3.8	3.0	0.8	0.8
	[E.2] Errores del administrador	3	5	5	3	1	1	15	15	9	3	3	Controlar	Detectivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seg de la info 18.1.3. Protección de registros	4	3.8	3.8	2.3	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															18.2.2. Cumplimiento con las políticas y normas de segurid						
	[E.15] Alteración accidental de la información	2	4	5	1	1	1	8	10	2	2	2	Aceptar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	2.0	2.5	0.5	0.5	0.5
	[E.18] Destrucción de información	1	5	4	1	1	1	5	4	1	1	1	Controlar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la	4	1.3	1.0	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros							
	[A.6] Abuso de privilegios de acceso	1	1	3	5	4	2	1	3	5	4	2	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	4	0.3	0.8	1.3	1.0	0.5
	[A.7] Uso no previsto	2	3	3	4	2	1	6	6	8	4	2	Aceptar	Correctivo	5.1.1. Políticas para la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	4	1.5	1.5	2.0	1.0	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.11] Acceso no autorizado	3	3	3	4	2	1	9	9	12	6	3	Controlar	Preventivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	3	3.0	3.0	4.0	2.0	1.0
	[A.19] Divulgación de información	2	1	1	5	4	2	2	2	10	8	4	Aceptar	Preventivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 7.2.3. Proceso disciplinario 7.3.1. Terminación o cambio de responsabilidades de empleo 8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 9.2.3. Gestión de derechos de acceso privilegiado 9.2.5. Revisión de los derechos de acceso de usuarios. 9.3.1.Uso de información secreta 9.4.1. Restricción de acceso a información 14.3.1. Protección de datos de ensayo 15.1.2. Tratamiento	2	1.0	1.0	5.0	4.0	2.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															de la seguridad dentro de los acuerdos con proveedores 18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. 18.1.3. Protección de registros							
	Bases de datos afiliados																				
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Preventivo	8.2.3. Manejo de Activos 8.3.3. Transferencia de medios de soporte físicos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	3	4	1	1	1	1	12	3	3	3	3	Aceptar	Preventivo	11.1.4. Protección contra amenazas externas y ambientales	4	3.0	0.8	0.8	0.8	0.8
	[I.10] Degradación de los soportes de almacenamiento de la información	2	5	3	1	1	1	10	6	2	2	2	Controlar	Preventivo	8.2.3. Manejo de Activos 11.1.4. Protección contra amenazas externas y ambientales 1.2.1. Ubicación y	2	5.0	3.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															protección de los equipos						
	[E.2] Errores del administrador	3	5	5	3	1	1	15	15	9	3	3	Controlar	Preventivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la información 18.1.3. Protección de registros 18.2.2. Cumplimiento con las políticas y normas de seguridad	4	3.8	3.8	2.3	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.15] Alteración accidental de la información	2	4	5	1	1	1	8	10	2	2	2	Controlar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	2.0	2.5	0.5	0.5	0.5
	[A.7] Uso no previsto	2	3	3	4	2	1	6	6	8	4	2	Transferir	Correctivo	5.1.1. Políticas para la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	4	1.5	1.5	2.0	1.0	0.5
	Bases de datos DNS																				
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Transferir	Correctivo	8.2.3. Manejo de Activos 8.3.3. Transferencia de medios de soporte físicos	4	2.5	1.0	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.6] Corte del suministro eléctrico	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.1.4. Protección contra amenazas externas y ambientales	4	3.0	0.8	0.8	0.8	0.8
	[E.1] Errores de los usuarios	3	4	5	4	1	1	12	15	12	3	3	Aceptar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	3.0	3.8	3.0	0.8	0.8
	[E.2] Errores del administrador	3	5	5	3	1	1	15	15	9	3	3	Controlar	Preventivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la información 18.1.3. Protección de registros	4	3.8	3.8	2.3	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															18.2.2. Cumplimiento con las políticas y normas de seguridad						
	[A.6] Abuso de privilegios de acceso	1	1	3	5	4	2	1	3	5	4	2	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	4	0.3	0.8	1.3	1.0	0.5
	[A.11] Acceso no autorizado	3	3	3	4	2	1	9	9	12	6	3	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	3	3.0	3.0	4.0	2.0	1.0
	Bases de datos DGH																				

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Controlar	Preventivo	8.2.3. Manejo de Activos 8.3.3. Transferencia de medios de soporte físicos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	4	1	1	1	1	8	2	2	2	2	Transferir	Preventivo	11.1.4. Protección contra amenazas externas y ambientales	4	2.0	0.5	0.5	0.5	0.5
	[I.10] Degradación de los soportes de almacenamiento de la información	2	5	3	1	1	1	10	6	2	2	2	Transferir	Preventivo	8.2.3. Manejo de Activos 11.1.4. Protección contra amenazas externas y ambientales 1.2.1. Ubicación y protección de los equipos	2	5.0	3.0	1.0	1.0	1.0
	[E.1] Errores de los usuarios	3	4	5	4	1	1	12	15	12	3	3	Controlar	Detectivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	3.0	3.8	3.0	0.8	0.8
	[E.2] Errores del administrador	3	5	5	3	1	1	15	15	9	3	3	Controlar	Preventivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de	4	3.8	3.8	2.3	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la información 18.1.3. Protección de registros 18.2.2. Cumplimiento con las políticas y normas de seguridad								
	[E.15] Alteración accidental de la información	2	4	5	1	1	1	8	10	2	2	2	Aceptar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	2.0	2.5	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.18] Destrucción de información	1	5	4	1	1	1	5	4	1	1	1	Controlar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	1.3	1.0	0.3	0.3	0.3
	[A.6] Abuso de privilegios de acceso	2	1	3	5	4	2	2	6	10	8	4	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	4	0.5	1.5	2.5	2.0	1.0
	[A.7] Uso no previsto	3	3	3	4	2	1	9	9	12	6	3	Aceptar	Correctivo	5.1.1. Políticas para la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de	4	2.3	2.3	3.0	1.5	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															acceso a información A.18.1.3. Protección de registros						
	[A.11] Acceso no autorizado	3	3	3	4	2	1	9	9	12	6	3	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	3	3.0	3.0	4.0	2.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.19] Divulgación de información	3	1	1	5	4	2	3	3	15	12	6	Controlar	Preventivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 7.2.3. Proceso disciplinario 7.3.1. Terminación o cambio de responsabilidades de empleo 8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 9.2.3. Gestión de derechos de acceso privilegiado 9.2.5. Revisión de los derechos de acceso de usuarios. 9.3.1.Uso de información secreta 9.4.1. Restricción de acceso a información 14.3.1. Protección de datos de ensayo 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores 18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. 18.1.3. Protección de registros	2	1.5	1.5	7.5	6.0	3.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	Base de datos Registro de correspondencia																				
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Controlar	Preventivo	8.2.3. Manejo de Activos 8.3.3. Transferencia de medios de soporte físicos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	1	4	1	1	1	1	4	1	1	1	1	Transferir	Preventivo	11.1.4. Protección contra amenazas externas y ambientales	4	1.0	0.3	0.3	0.3	0.3
	[I.10] Degradación de los soportes de almacenamiento de la información	2	5	3	1	1	1	10	6	2	2	2	Transferir	Preventivo	8.2.3. Manejo de Activos 11.1.4. Protección contra amenazas externas y ambientales 1.2.1. Ubicación y protección de los equipos	2	5.0	3.0	1.0	1.0	1.0
	[E.1] Errores de los usuarios	2	4	5	4	1	1	8	10	8	2	2	Controlar	Detectivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	2.0	2.5	2.0	0.5	0.5
	[E.2] Errores del administrador	3	5	5	3	1	1	15	15	9	3	3	Controlar	Preventivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de	4	3.8	3.8	2.3	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la información 18.1.3. Protección de registros 18.2.2. Cumplimiento con las políticas y normas de seguridad									
	[E.15] Alteración accidental de la información	3	4	5	1	1	1	12	15	3	3	3	Aceptar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	3.0	3.8	0.8	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.18] Destrucción de información	1	5	4	1	1	1	5	4	1	1	1	Controlar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	1.3	1.0	0.3	0.3	0.3
	[A.6] Abuso de privilegios de acceso	3	1	3	5	4	2	3	9	15	12	6	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	4	0.8	2.3	3.8	3.0	1.5
	[A.7] Uso no previsto	3	3	3	4	2	1	9	9	12	6	3	Aceptar	Correctivo	5.1.1. Políticas para la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de	4	2.3	2.3	3.0	1.5	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															acceso a información A.18.1.3. Protección de registros							
	[A.11] Acceso no autorizado	2	3	3	4	2	1	6	6	8	4	2	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	3	2.0	2.0	2.7	1.3	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.19] Divulgación de información	3	1	1	5	4	2	3	3	15	12	6	Controlar	Preventivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 7.2.3. Proceso disciplinario 7.3.1. Terminación o cambio de responsabilidades de empleo 8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 9.2.3. Gestión de derechos de acceso privilegiado 9.2.5. Revisión de los derechos de acceso de usuarios. 9.3.1.Uso de información secreta 9.4.1. Restricción de acceso a información 14.3.1. Protección de datos de ensayo 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores 18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. 18.1.3. Protección de registros	2	1.5	1.5	7.5	6.0	3.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	Base de datos contratación																				
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Controlar	Preventivo	8.2.3. Manejo de Activos 8.3.3. Transferencia de medios de soporte físicos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	1	4	1	1	1	1	4	1	1	1	1	Transferir	Preventivo	11.1.4. Protección contra amenazas externas y ambientales	4	1.0	0.3	0.3	0.3	0.3
	[I.10] Degradación de los soportes de almacenamiento de la información	2	5	3	1	1	1	10	6	2	2	2	Transferir	Preventivo	8.2.3. Manejo de Activos 11.1.4. Protección contra amenazas externas y ambientales 1.2.1. Ubicación y protección de los equipos	2	5.0	3.0	1.0	1.0	1.0
	[E.1] Errores de los usuarios	4	4	5	4	1	1	16	20	16	4	4	Controlar	Detectivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	4.0	5.0	4.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.2] Errores del administrador	3	5	5	3	1	1	15	15	9	3	3	Controlar	Preventivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la información 18.1.3. Protección de registros 18.2.2. Cumplimiento con las políticas y normas de seguridad	4	3.8	3.8	2.3	0.8	0.8
	[E.15] Alteración accidental de la información	3	4	5	1	1	1	12	15	3	3	3	Aceptar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de	4	3.0	3.8	0.8	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros							
	[E.18] Destrucción de información	1	5	4	1	1	1	5	4	1	1	1	Controlar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	1.3	1.0	0.3	0.3	0.3
	[A.6] Abuso de privilegios de acceso	3	1	3	5	4	2	3	9	15	12	6	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	4	0.8	2.3	3.8	3.0	1.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.7] Uso no previsto	3	3	3	4	2	1	9	9	12	6	3	Aceptar	Correctivo	5.1.1. Políticas para la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	4	2.3	2.3	3.0	1.5	0.8
	[A.11] Acceso no autorizado	4	3	3	4	2	1	12	12	16	8	4	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	3	4.0	4.0	5.3	2.7	1.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.19] Divulgación de información	3	1	1	5	4	2	3	3	15	12	6	Controlar	Preventivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 7.2.3. Proceso disciplinario 7.3.1. Terminación o cambio de responsabilidades de empleo 8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 9.2.3. Gestión de derechos de acceso privilegiado 9.2.5. Revisión de los derechos de acceso de usuarios. 9.3.1.Uso de información secreta 9.4.1. Restricción de acceso a información 14.3.1. Protección de datos de ensayo 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores 18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. 18.1.3. Protección de registros	2	1.5	1.5	7.5	6.0	3.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	Cuentas de correo electrónico																				
	[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Controlar	Preventivo	8.2.3. Manejo de Activos 8.3.3. Transferencia de medios de soporte físicos	4	3.8	1.5	0.8	0.8	0.8
	[I.10] Degradación de los soportes de almacenamiento de la información	2	5	3	1	1	1	10	6	2	2	2	Transferir	Preventivo	8.2.3. Manejo de Activos 11.1.4. Protección contra amenazas externas y ambientales 1.2.1. Ubicación y protección de los equipos	2	5.0	3.0	1.0	1.0	1.0
	[E.2] Errores del administrador	4	5	5	3	1	1	20	20	12	4	4	Controlar	Preventivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la información 18.1.3. Protección de	4	5.0	5.0	3.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															registros 18.2.2. Cumplimiento con las políticas y normas de seguridad						
	[E.15] Alteración accidental de la información	2	4	5	1	1	1	8	10	2	2	2	Aceptar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	2.0	2.5	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.18] Destrucción de información	1	5	4	1	1	1	5	4	1	1	1	Controlar	Preventivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	1.3	1.0	0.3	0.3	0.3
	[A.7] Uso no previsto	3	3	3	4	2	1	9	9	12	6	3	Aceptar	Correctivo	5.1.1. Políticas para la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de acceso a información A.18.1.3. Protección de registros	4	2.3	2.3	3.0	1.5	0.8
	[A.11] Acceso no autorizado	2	3	3	4	2	1	6	6	8	4	2	Controlar	Detectivo	9.1.1. Política de Control de Acceso 9.2.2. Suministro de acceso de usuario 9.2.5. Revisión de los derechos de acceso de usuarios. 9.4.1. Restricción de	3	2.0	2.0	2.7	1.3	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															acceso a información A.18.1.3. Protección de registros						
	[A.19] Divulgación de información	3	1	1	5	4	2	3	3	15	12	6	Controlar	Preventivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 7.2.3. Proceso disciplinario 7.3.1. Terminación o cambio de responsabilidades de empleo 8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 9.2.3. Gestión de derechos de acceso privilegiado 9.2.5. Revisión de los derechos de acceso de usuarios. 9.3.1.Uso de información secreta 9.4.1. Restricción de acceso a información 14.3.1. Protección de datos de ensayo 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	2	1.5	1.5	7.5	6.0	3.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. 18.1.3. Protección de registros								
ACTIVOS DE SERVICIOS	**Acceso a internet**																				
	[E.1] Errores de los usuarios	2	4	3	2	1	1	8	6	4	2	2	Aceptar	Preventivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de	3	2.7	2.0	1.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															Sistemas de Información						
	[E.2] Errores del administrador	3	5	3	4	1	1	15	9	12	3	3	Controlar	Preventivo	5.1.1. Políticas para la Seguridad de la Información 6.1.1. Seguridad de la Información Roles y Responsabilidades 15.1.1. Política de seguridad de la información para las relaciones con proveedores	2	7.5	4.5	6.0	1.5	1.5
	[E.19] Fugas de información	2	1	4	4	4	1	2	8	8	8	2	Controlar	Correctivo	5.1.1. Políticas para la Seguridad de la Información 5.1.2. Revisión de las Políticas para seguridad de la información 6.1.1. Seguridad de la Información Roles y Responsabilidades 7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información	3	0.7	2.7	2.7	2.7	0.7
	[E.24] Caída del sistema por	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	8.2.3. Manejo de Activos	2	5.0	2.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	agotamiento de recursos														11.2.3. Seguridad del cableado						
	[A.6] Abuso de privilegios de acceso	3	4	4	4	1	1	12	12	12	3	3	Controlar	Detectivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 7.2.3. Proceso disciplinario 7.3.1. Terminación o cambio de responsabilidades de empleo 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.2.5. Revisión de los derechos de acceso de usuarios 9.3.1.Uso de información secreta 9.4.1. Restricción de acceso a información 13.2.4. Acuerdos de confidencialidad o de no divulgación 15.1.1. Política de seguridad de la información para las relaciones con proveedores	4	3.0	3.0	3.0	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.7] Uso no previsto	4	4	3	3	1	1	16	12	12	4	4	Aceptar	Correctivo	6.1.2. Separación de deberes 7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 9.4.1. Restricción de acceso a información 13.2.4. Acuerdos de confidencialidad o de no divulgación	4	4.0	3.0	3.0	1.0	1.0
	Correo electrónico																				
	[E.1] Errores de los usuarios	2	4	3	2	1	1	8	6	4	2	2	Controlar	Correctivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información	3	2.7	2.0	1.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.2] Errores del administrador	4	5	3	4	1	1	20	12	16	4	4	Controlar	Preventivo	5.1.1. Políticas para la Seguridad de la Información 6.1.1. Seguridad de la Información Roles y Responsabilidades 15.1.1. Política de seguridad de la información para las relaciones con proveedores	2	10.0	6.0	8.0	2.0	2.0
	[E.19] Fugas de información	3	1	4	4	4	1	3	12	12	12	3	Aceptar	Preventivo	5.1.1. Políticas para la Seguridad de la Información 5.1.2. Revisión de las Políticas para seguridad de la información 6.1.1. Seguridad de la Información Roles y Responsabilidades 7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información	3	1.0	4.0	4.0	4.0	1.0
	[E.24] Caída del sistema por agotamiento de recursos	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Detectivo	8.2.3. Manejo de Activos 11.2.3. Seguridad del cableado 12.1.3. Gestión de Capacidad	2	7.5	3.0	1.5	1.5	1.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.6] Abuso de privilegios de acceso	3	4	4	4	1	1	12	12	12	3	3	Controlar	Detectivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 7.2.3. Proceso disciplinario 7.3.1. Terminación o cambio de responsabilidades de empleo 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.2.5. Revisión de los derechos de acceso de usuarios 9.3.1.Uso de información secreta 9.4.1. Restricción de acceso a información 13.2.4. Acuerdos de confidencialidad o de no divulgación 15.1.1. Política de seguridad de la información para las relaciones con proveedores	4	3.0	3.0	3.0	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.7] Uso no previsto	2	4	3	3	1	1	8	6	6	2	2	Aceptar	Correctivo	6.1.2. Separación de deberes 7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 9.4.1. Restricción de acceso a información 13.2.4. Acuerdos de confidencialidad o de no divulgación	4	2.0	1.5	1.5	0.5	0.5
	[A.9] [Re-]encaminamiento de mensajes	3	1	1	4	1	1	3	3	12	3	3	Controlar	Correctivo	12.2.1. Controles contra códigos maliciosos 12.4.1. Registro de eventos 12.4.2. Protección de la información de registro 12.6.2. Restricciones sobre la instalación de Software 13.1.1. Controles de redes. 13.2.1. Políticas y procedimientos de transferencia de información 13.2.3. Mensajes electrónicos 14.1.2. Seguridad de servicios de las aplicaciones en redes públicas	4	0.8	0.8	3.0	0.8	0.8
	Hosting del sitio web																				

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.1] Errores de los usuarios	3	4	3	2	1	1	12	9	6	3	3	Aceptar	Correctivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información	3	4.0	3.0	2.0	1.0	1.0
	[E.2] Errores del administrador	2	5	3	4	1	1	10	6	8	2	2	Controlar	Preventivo	5.1.1. Políticas para la Seguridad de la Información 6.1.1. Seguridad de la Información Roles y Responsabilidades 15.1.1. Política de seguridad de la información para las relaciones con proveedores	2	5.0	3.0	4.0	1.0	1.0
	[E.19] Fugas de información	3	1	4	4	4	1	3	12	12	12	3	Controlar	Detectivo	5.1.1. Políticas para la Seguridad de la Información 5.1.2. Revisión de las Políticas para seguridad de la información 6.1.1. Seguridad de la Información Roles y Responsabilidades 7.1.2. Términos y condiciones del empleo	3	1.0	4.0	4.0	4.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información						
	[E.24] Caída del sistema por agotamiento de recursos	3	5	2	1	1	1	15	6	3	3	3	Controlar	Correctivo	8.2.3. Manejo de Activos 11.2.3. Seguridad del cableado 12.1.3. Gestión de Capacidad	2	7.5	3.0	1.5	1.5	1.5
	[A.6] Abuso de privilegios de acceso	2	4	4	4	1	1	8	8	8	2	2	Aceptar	Detectivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 7.2.3. Proceso disciplinario 7.3.1. Terminación o cambio de responsabilidades de empleo 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.2.5. Revisión de los derechos de acceso de usuarios 9.3.1.Uso de información secreta 9.4.1. Restricción de acceso a información	4	2.0	2.0	2.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															13.2.4. Acuerdos de confidencialidad o de no divulgación 15.1.1. Política de seguridad de la información para las relaciones con proveedores								
	[A.7] Uso no previsto	1	4	3	3	1	1	4	3	3	1	1	Aceptar	Detectivo	6.1.2. Separación de deberes 7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 9.4.1. Restricción de acceso a información 13.2.4. Acuerdos de confidencialidad o de no divulgación	4	1.0	0.8	0.8	0.3	0.3
	Almacenamiento de copias de seguridad se realiza de manera local y en la nube																				

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.5] Avería de origen físico o lógico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Detectivo	8.2.1. Clasificación de la Información 8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 8.3.3. Transferencia de medios de soporte físicos 9.1.1. Política de Control de Acceso. 18.1.3. Protección de registros.	4	2.5	0.5	0.5	0.5	0.5
	[I.10] Degradación de los soportes de almacenamiento de la información	2	4	4	1	1	1	8	8	2	2	2	Controlar	Preventivo	8.2.1. Clasificación de la Información 8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 8.3.3. Transferencia de medios de soporte físicos 9.1.1. Política de Control de Acceso. 18.1.3. Protección de registros.	4	2.0	2.0	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.1] Errores de los usuarios	5	4	3	2	1	1	20	15	10	5	5	Controlar	Correctivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información	3	6.7	5.0	3.3	1.7	1.7
	[E.2] Errores del administrador	3	5	3	4	1	1	15	9	12	3	3	Controlar	Preventivo	5.1.1. Políticas para la Seguridad de la Información 6.1.1. Seguridad de la Información Roles y Responsabilidades 15.1.1. Política de seguridad de la información para las relaciones con proveedores	3	5.0	3.0	4.0	1.0	1.0
	[E.4] Errores de configuración	2	3	4	4	4	1	6	8	8	8	2	Transferir	Detectivo	5.1.1. Políticas para la Seguridad de la Información 6.1.1. Seguridad de la Información Roles y Responsabilidades 12.4.1. Registro de eventos 12.6.1. Gestión de las vulnerabilidades técnicas. 15.1.1. Política de seguridad de la	3	2.0	2.7	2.7	2.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															información para las relaciones con proveedores						
	[E.24] Caída del sistema por agotamiento de recursos	4	5	2	1	1	1	20	8	4	4	4	Controlar	Detectivo	8.2.3. Manejo de Activos 11.2.3. Seguridad del cableado 12.1.3. Gestión de Capacidad	4	5.0	2.0	1.0	1.0	1.0
ACTIVOS DE SOFTWARE	**Sistemas Operativos**																				
	[I.5] Avería de origen físico o lógico	2	4	2	1	1	1	8	4	2	2	2	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	2.0	1.0	0.5	0.5	0.5
	[E.2] Errores del administrador	1	5	4	3	1	1	5	4	3	1	1	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	1.7	1.3	1.0	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.8] Difusión de software dañino	1	4	4	4	1	1	4	4	4	1	1	Controlar	Preventivo	13.1.1. Controles de redes 13.1.2. Seguridad de los servicios de red 15.2.1. Seguimiento y revisión de los servicios de los proveedores	4	1.0	1.0	1.0	0.3	0.3
	[E.20] Vulnerabilidades de los programas (software)	3	4	5	4	2	1	12	15	12	6	3	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	4.0	5.0	4.0	2.0	1.0
	[E.21] Errores de mantenimiento / actualización de programas	2	4	4	2	1	1	8	8	4	2	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	2.0	2.0	1.0	0.5	0.5
	SQL Server 2008R2																				

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.5] Avería de origen físico o lógico	2	4	2	1	1	1	8	4	2	2	2	Aceptar	Preventivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	2.0	1.0	0.5	0.5	0.5
	[E.2] Errores del administrador	2	5	4	3	1	1	10	8	6	2	2	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	3.3	2.7	2.0	0.7	0.7
	[E.8] Difusión de software dañino	1	4	4	4	1	1	4	4	4	1	1	Controlar	Preventivo	13.1.1. Controles de redes 13.1.2. Seguridad de los servicios de red 15.2.1. Seguimiento y revisión de los servicios de los proveedores	4	1.0	1.0	1.0	0.3	0.3
	[E.15] Alteración accidental de la información	3	4	5	4	3	1	12	15	12	9	3	Controlar	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información	4	3.0	3.8	3.0	2.3	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros						
	[E.19] Fugas de información	2	2	4	5	1	1	4	8	10	2	2	Aceptar	Correctivo	8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 8.2.2. Etiquetado de la Información 8.3.2. Disposición de los medios de soporte	3	1.3	2.7	3.3	0.7	0.7
	[E.20] Vulnerabilidades de los programas (software)	2	4	5	4	2	1	8	10	8	4	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	2.7	3.3	2.7	1.3	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.21] Errores de mantenimiento / actualización de programas	2	4	4	2	1	1	8	8	4	2	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	2.0	2.0	1.0	0.5	0.5
	[A.5] Suplantación de la identidad del usuario	2	4	5	5	2	2	8	10	10	4	4	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	2.0	2.5	2.5	1.0	1.0
	[A.6] Abuso de privilegios de acceso	4	4	5	5	2	2	16	20	20	8	8	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 18.2.1. Revisión independiente de la seguridad de la información	3	5.3	6.7	6.7	2.7	2.7
	[A.7] Uso no previsto	2	4	5	5	1	1	8	10	10	2	2	Controlar	Correctivo	5.1.2. Revisión de las Políticas para seguridad de la información 6.1.2. Separación de deberes A.8.1.3. Uso Aceptable de los Activos	3	2.7	3.3	3.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															8.2.1. Clasificación de la Información 18.2.1. Revisión independiente de la seguridad de la información							
	[A.11] Acceso no autorizado	2	3	5	5	2	2	6	10	10	4	4	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	1.5	2.5	2.5	1.0	1.0
	[A.15] Modificación deliberada de la información	2	2	5	2	1	1	4	10	4	2	2	Transferir	Correctivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	1.0	2.5	1.0	0.5	0.5
	[A.18] Destrucción de información	1	5	2	1	1	1	5	2	1	1	1	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de	4	1.3	0.5	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros							
	[A.19] Divulgación de información	3	2	1	5	4	1	6	3	15	12	3	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de la información de registro 18.1.3. Protección de registros	4	1.5	0.8	3.8	3.0	0.8
	PostgreSQL																				
	[I.5] Avería de origen físico o lógico	1	4	2	1	1	1	4	2	1	1	1	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	1.0	0.5	0.3	0.3	0.3
	[E.2] Errores del administrador	1	5	4	3	1	1	5	4	3	1	1	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información	3	1.7	1.3	1.0	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos							
	[E.15] Alteración accidental de la información	2	4	5	4	3	1	8	10	8	6	2	Transferir	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	2.0	2.5	2.0	1.5	0.5
	[E.19] Fugas de información	1	2	4	5	1	1	2	4	5	1	1	Aceptar	Correctivo	8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 8.2.2. Etiquetado de la Información 8.3.2. Disposición de los medios de soporte	3	0.7	1.3	1.7	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.20] Vulnerabilidades de los programas (software)	2	4	5	4	2	1	8	10	8	4	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	2.7	3.3	2.7	1.3	0.7
	[E.21] Errores de mantenimiento / actualización de programas	1	4	4	2	1	1	4	4	2	1	1	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	1.0	1.0	0.5	0.3	0.3
	[A.5] Suplantación de la identidad del usuario	2	4	5	5	2	2	8	10	10	4	4	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	2.0	2.5	2.5	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.7] Uso no previsto	1	4	5	5	1	1	4	5	5	1	1	Controlar	Detectivo	5.1.2. Revisión de las Políticas para seguridad de la información 6.1.2. Separación de deberes A.8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 18.2.1. Revisión independiente de la seguridad de la información	3	1.3	1.7	1.7	0.3	0.3
	[A.11] Acceso no autorizado	1	3	5	5	2	2	3	5	5	2	2	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	0.8	1.3	1.3	0.5	0.5
	[A.15] Modificación deliberada de la información	1	2	5	2	1	1	2	5	2	1	1	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	0.5	1.3	0.5	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.18] Destrucción de información	1	5	2	1	1	1	5	2	1	1	1	Transferir	Correctivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	1.3	0.5	0.3	0.3	0.3
	[A.19] Divulgación de información	2	2	1	5	4	1	4	2	10	8	2	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de la información de registro 18.1.3. Protección de registros	4	1.0	0.5	2.5	2.0	0.5
	MySQL																				
	[I.5] Avería de origen físico o lógico	1	4	2	1	1	1	4	2	1	1	1	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	1.0	0.5	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.2] Errores del administrador	2	5	4	3	1	1	10	8	6	2	2	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	3.3	2.7	2.0	0.7	0.7
	[E.15] Alteración accidental de la información	1	4	5	4	3	1	4	5	4	3	1	Transferir	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	1.0	1.3	1.0	0.8	0.3
	[E.19] Fugas de información	1	2	4	5	1	1	2	4	5	1	1	Transferir	Detectivo	8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 8.2.2. Etiquetado de la Información 8.3.2. Disposición de los medios de soporte	3	0.7	1.3	1.7	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.20] Vulnerabilidades de los programas (software)	2	4	5	4	2	1	8	10	8	4	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	2.7	3.3	2.7	1.3	0.7
	[E.21] Errores de mantenimiento / actualización de programas	2	4	4	2	1	1	8	8	4	2	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	2.0	2.0	1.0	0.5	0.5
	[A.5] Suplantación de la identidad del usuario	2	4	5	5	2	2	8	10	10	4	4	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	2.0	2.5	2.5	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.6] Abuso de privilegios de acceso	1	4	5	5	2	1	4	5	5	2	1	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 18.2.1. Revisión independiente de la seguridad de la información	3	1.3	1.7	1.7	0.7	0.3
	[A.7] Uso no previsto	1	4	5	5	1	1	4	5	5	1	1	Aceptar	Detectivo	5.1.2. Revisión de las Políticas para seguridad de la información 6.1.2. Separación de deberes A.8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 18.2.1. Revisión independiente de la seguridad de la información	3	1.3	1.7	1.7	0.3	0.3
	[A.11] Acceso no autorizado	2	2	5	2	1	1	4	10	4	2	2	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	1.0	2.5	1.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.15] Modificación deliberada de la información	1	2	5	2	1	1	2	5	2	1	1	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	0.5	1.3	0.5	0.3	0.3
	[A.18] Destrucción de información	1	5	2	1	1	1	5	2	1	1	1	Transferir	Correctivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	1.3	0.5	0.3	0.3	0.3
	[A.19] Divulgación de información	1	2	1	5	4	1	2	1	5	4	1	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de	4	0.5	0.3	1.3	1.0	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															la información de registro 18.1.3. Protección de registros						
	Vmware																				
	[I.5] Avería de origen físico o lógico	3	4	2	1	1	1	12	6	3	3	3	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	3.0	1.5	0.8	0.8	0.8
	[E.2] Errores del administrador	3	5	4	3	1	1	15	12	9	3	3	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	5.0	4.0	3.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.15] Alteración accidental de la información	3	4	5	4	3	1	12	15	12	9	3	Transferir	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	3.0	3.8	3.0	2.3	0.8
	[E.20] Vulnerabilidades de los programas (software)	2	4	5	4	2	1	8	10	8	4	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	2.7	3.3	2.7	1.3	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.21] Errores de mantenimiento / actualización de programas	2	4	4	2	1	1	8	8	4	2	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	2.0	2.0	1.0	0.5	0.5
	[A.5] Suplantación de la identidad del usuario	1	4	5	5	2	2	4	5	5	2	2	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	1.0	1.3	1.3	0.5	0.5
	[A.6] Abuso de privilegios de acceso	1	4	5	5	2	2	4	5	5	2	2	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 18.2.1. Revisión independiente de la seguridad de la información	3	1.3	1.7	1.7	0.7	0.7
	[A.11] Acceso no autorizado	1	3	5	5	2	2	3	5	5	2	2	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de	4	0.8	1.3	1.3	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															Gestión de Contraseñas						
	Dinámica Gerencial Hospitalaria – DGH.NET																				
	[I.5] Avería de origen físico o lógico	4	4	2	1	1	1	16	8	4	4	4	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	4.0	2.0	1.0	1.0	1.0
	[E.1] Errores de los usuarios	4	4	5	4	1	1	16	20	16	4	4	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información	4	4.0	5.0	4.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.2] Errores del administrador	2	5	4	3	1	1	10	8	6	2	2	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	3.3	2.7	2.0	0.7	0.7
	[E.15] Alteración accidental de la información	3	4	5	4	3	1	12	15	12	9	3	Transferir	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	3.0	3.8	3.0	2.3	0.8
	[E.19] Fugas de información	3	2	4	5	1	1	6	12	15	3	3	Transferir	Detectivo	8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 8.2.2. Etiquetado de la Información 8.3.2. Disposición de los medios de soporte	3	2.0	4.0	5.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.20] Vulnerabilidades de los programas (software)	4	4	5	4	2	1	16	20	16	8	4	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	5.3	6.7	5.3	2.7	1.3
	[E.21] Errores de mantenimiento / actualización de programas	4	4	4	2	1	1	16	16	8	4	4	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	4.0	4.0	2.0	1.0	1.0
	[A.5] Suplantación de la identidad del usuario	3	4	5	5	2	2	12	15	15	6	6	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	3.0	3.8	3.8	1.5	1.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.6] Abuso de privilegios de acceso	3	4	5	5	2	1	12	15	15	6	3	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 18.2.1. Revisión independiente de la seguridad de la información	3	4.0	5.0	5.0	2.0	1.0
	[A.7] Uso no previsto	2	4	5	5	1	1	8	10	10	2	2	Aceptar	Detectivo	5.1.2. Revisión de las Políticas para seguridad de la información 6.1.2. Separación de deberes A.8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 18.2.1. Revisión independiente de la seguridad de la información	4	2.0	2.5	2.5	0.5	0.5
	[A.11] Acceso no autorizado	3	2	5	2	1	1	6	15	6	3	3	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	1.5	3.8	1.5	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.15] Modificación deliberada de la información	2	2	5	2	1	1	4	10	4	2	2	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	1.0	2.5	1.0	0.5	0.5
	[A.18] Destrucción de información	1	5	2	1	1	1	5	2	1	1	1	Transferir	Correctivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	1.3	0.5	0.3	0.3	0.3
	[A.19] Divulgación de información	4	2	1	5	4	1	8	4	20	16	4	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de	4	2.0	1.0	5.0	4.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															la información de registro 18.1.3. Protección de registros						
	SIEP Documental																				
	[I.5] Avería de origen físico o lógico	3	4	2	1	1	1	12	6	3	3	3	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	3.0	1.5	0.8	0.8	0.8
	[E.1] Errores de los usuarios	2	4	5	4	1	1	8	10	8	2	2	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información	4	2.0	2.5	2.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.2] Errores del administrador	2	5	4	3	1	1	10	8	6	2	2	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	3.3	2.7	2.0	0.7	0.7
	[E.15] Alteración accidental de la información	2	4	5	4	3	1	8	10	8	6	2	Transferir	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	2.0	2.5	2.0	1.5	0.5
	[E.19] Fugas de información	2	2	4	5	1	1	4	8	10	2	2	Transferir	Detectivo	8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 8.2.2. Etiquetado de la Información 8.3.2. Disposición de los medios de soporte	3	1.3	2.7	3.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.20] Vulnerabilidades de los programas (software)	3	4	5	4	2	1	12	15	12	6	3	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	4.0	5.0	4.0	2.0	1.0
	[E.21] Errores de mantenimiento / actualización de programas	3	4	4	2	1	1	12	12	6	3	3	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	3.0	3.0	1.5	0.8	0.8
	[A.5] Suplantación de la identidad del usuario	2	4	5	5	2	2	8	10	10	4	4	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	2.0	2.5	2.5	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.6] Abuso de privilegios de acceso	2	4	5	5	2	1	8	10	10	4	2	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 18.2.1. Revisión independiente de la seguridad de la información	3	2.7	3.3	3.3	1.3	0.7
	[A.7] Uso no previsto	1	4	5	5	1	1	4	5	5	1	1	Aceptar	Detectivo	5.1.2. Revisión de las Políticas para seguridad de la información 6.1.2. Separación de deberes A.8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 18.2.1. Revisión independiente de la seguridad de la información	4	1.0	1.3	1.3	0.3	0.3
	[A.11] Acceso no autorizado	1	2	5	2	1	1	2	5	2	1	1	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información	4	0.5	1.3	0.5	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															18.1.3. Protección de registros						
	[A.15] Modificación deliberada de la información	1	2	5	2	1	1	2	5	2	1	1	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	0.5	1.3	0.5	0.3	0.3
	[A.19] Divulgación de información	2	2	1	5	4	1	4	2	10	8	2	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de la información de registro 18.1.3. Protección de registros	4	1.0	0.5	2.5	2.0	0.5
	Contratación																				

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.5] Avería de origen físico o lógico	3	4	2	1	1	1	12	6	3	3	3	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	3.0	1.5	0.8	0.8	0.8
	[E.1] Errores de los usuarios	4	4	5	4	1	1	16	20	16	4	4	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información	4	4.0	5.0	4.0	1.0	1.0
	[E.2] Errores del administrador	3	5	4	3	1	1	15	12	9	3	3	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y	3	5.0	4.0	3.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															decisiones sobre ellos						
	[E.8] Difusión de software dañino	1	4	4	4	1	1	4	4	4	1	1	Aceptar	Detectivo	13.1.1. Controles de redes 13.1.2. Seguridad de los servicios de red 15.2.1. Seguimiento y revisión de los servicios de los proveedores	4	1.0	1.0	1.0	0.3	0.3
	[E.15] Alteración accidental de la información	2	4	5	4	3	1	8	10	8	6	2	Transferir	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	2.0	2.5	2.0	1.5	0.5
	[E.19] Fugas de información	3	2	4	5	1	1	6	12	15	3	3	Transferir	Detectivo	8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 8.2.2. Etiquetado de la Información 8.3.2. Disposición de los medios de soporte	3	2.0	4.0	5.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.20] Vulnerabilidades de los programas (software)	4	4	5	4	2	1	16	20	16	8	4	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	5.3	6.7	5.3	2.7	1.3
	[E.21] Errores de mantenimiento / actualización de programas	3	4	4	2	1	1	12	12	6	3	3	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	3.0	3.0	1.5	0.8	0.8
	[A.5] Suplantación de la identidad del usuario	2	4	5	5	2	2	8	10	10	4	4	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	2.0	2.5	2.5	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.6] Abuso de privilegios de acceso	2	4	5	5	2	1	8	10	10	4	2	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 18.2.1. Revisión independiente de la seguridad de la información	3	2.7	3.3	3.3	1.3	0.7
	[A.7] Uso no previsto	2	4	5	5	1	1	8	10	10	2	2	Aceptar	Detectivo	5.1.2. Revisión de las Políticas para seguridad de la información 6.1.2. Separación de deberes A.8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 18.2.1. Revisión independiente de la seguridad de la información	4	2.0	2.5	2.5	0.5	0.5
	[A.11] Acceso no autorizado	1	2	5	2	1	1	2	5	2	1	1	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información	4	0.5	1.3	0.5	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															18.1.3. Protección de registros						
	[A.15] Modificación deliberada de la información	1	2	5	2	1	1	2	5	2	1	1	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	0.5	1.3	0.5	0.3	0.3
	[A.19] Divulgación de información	2	2	1	5	4	1	4	2	10	8	2	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de la información de registro 18.1.3. Protección de registros	4	1.0	0.5	2.5	2.0	0.5
	Aplicativo Inventario Único Documental																				

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.5] Avería de origen físico o lógico	1	4	2	1	1	1	4	2	1	1	1	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	1.0	0.5	0.3	0.3	0.3
	[E.1] Errores de los usuarios	2	4	5	4	1	1	8	10	8	2	2	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información	4	2.0	2.5	2.0	0.5	0.5
	[E.2] Errores del administrador	1	5	4	3	1	1	5	4	3	1	1	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y	3	1.7	1.3	1.0	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															decisiones sobre ellos						
	[E.15] Alteración accidental de la información	1	4	5	4	3	1	4	5	4	3	1	Transferir	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	1.0	1.3	1.0	0.8	0.3
	[E.20] Vulnerabilidades de los programas (software)	3	4	5	4	2	1	12	15	12	6	3	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad	3	4.0	5.0	4.0	2.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															dentro de los acuerdos con proveedores						
	[E.21] Errores de mantenimiento / actualización de programas	2	4	4	2	1	1	8	8	4	2	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	2.0	2.0	1.0	0.5	0.5
	[A.5] Suplantación de la identidad del usuario	1	4	5	5	2	2	4	5	5	2	2	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	1.0	1.3	1.3	0.5	0.5
	[A.15] Modificación deliberada de la información	2	2	5	2	1	1	4	10	4	2	2	Controlar	Detectivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información	4	1.0	2.5	1.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															18.1.3. Protección de registros						
	[A.19] Divulgación de información	1	2	1	5	4	1	2	1	5	4	1	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de la información de registro 18.1.3. Protección de registros	4	0.5	0.3	1.3	1.0	0.3
	Contratación Electrónica																				
	[I.5] Avería de origen físico o lógico	1	4	2	1	1	1	4	2	1	1	1	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	1.0	0.5	0.3	0.3	0.3
	[E.1] Errores de los usuarios	2	4	5	4	1	1	8	10	8	2	2	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia,	4	2.0	2.5	2.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información							
	[E.2] Errores del administrador	1	5	4	3	1	1	10	8	6	2	2	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	3.3	2.7	2.0	0.7	0.7
	[E.15] Alteración accidental de la información	1	4	5	4	3	1	4	5	4	3	1	Transferir	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas	4	1.0	1.3	1.0	0.8	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros						
	[E.19] Fugas de información	1	2	4	5	1	1	2	4	5	1	1	Transferir	Detectivo	8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 8.2.2. Etiquetado de la Información 8.3.2. Disposición de los medios de soporte	3	0.7	1.3	1.7	0.3	0.3
	[E.20] Vulnerabilidades de los programas (software)	2	4	5	4	2	1	8	10	8	4	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	2.7	3.3	2.7	1.3	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.21] Errores de mantenimiento / actualización de programas	1	4	4	2	1	1	4	4	2	1	1	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	1.0	1.0	0.5	0.3	0.3
	[A.5] Suplantación de la identidad del usuario	1	4	5	5	2	2	4	5	5	2	2	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	1.0	1.3	1.3	0.5	0.5
	[A.19] Divulgación de información	1	2	1	5	4	1	2	1	5	4	1	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de la información de registro 18.1.3. Protección de registros	4	0.5	0.3	1.3	1.0	0.3
	Plataforma E-learning																				
	[I.5] Avería de origen físico o lógico	1	4	2	1	1	1	4	2	1	1	1	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos	4	1.0	0.5	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.						
	[E.1] Errores de los usuarios	4	4	5	4	1	1	16	20	16	4	4	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información	4	4.0	5.0	4.0	1.0	1.0
	[E.2] Errores del administrador	2	5	4	3	1	1	10	8	6	2	2	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	3.3	2.7	2.0	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.8] Difusión de software dañino	2	4	4	4	1	1	8	8	8	2	2	Aceptar	Detectivo	13.1.1. Controles de redes 13.1.2. Seguridad de los servicios de red 15.2.1. Seguimiento y revisión de los servicios de los proveedores	4	2.0	2.0	2.0	0.5	0.5
	[E.20] Vulnerabilidades de los programas (software)	1	4	5	4	2	1	4	5	4	2	1	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	1.3	1.7	1.3	0.7	0.3
	[E.21] Errores de mantenimiento / actualización de programas	1	4	4	2	1	1	4	4	2	1	1	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	1.0	1.0	0.5	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.19] Divulgación de información	1	2	1	5	4	1	2	1	5	4	1	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de la información de registro 18.1.3. Protección de registros	4	0.5	0.3	1.3	1.0	0.3
	Antivirus																				
	[I.5] Avería de origen físico o lógico	1	4	2	1	1	1	4	2	1	1	1	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	1.0	0.5	0.3	0.3	0.3
	[E.1] Errores de los usuarios	2	4	5	4	1	1	8	10	8	2	2	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso	4	2.0	2.5	2.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															12.7.1. Controles sobre auditorías de Sistemas de Información							
	[E.2] Errores del administrador	1	5	4	3	1	1	10	8	6	2	2	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	3.3	2.7	2.0	0.7	0.7
	[E.20] Vulnerabilidades de los programas (software)	1	4	5	4	2	1	4	5	4	2	1	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los	3	1.3	1.7	1.3	0.7	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															acuerdos con proveedores						
	[E.21] Errores de mantenimiento / actualización de programas	1	4	4	2	1	1	4	4	2	1	1	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	1.0	1.0	0.5	0.3	0.3
	Ofimática																				
	[I.5] Avería de origen físico o lógico	3	4	2	1	1	1	12	6	3	3	3	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	3.0	1.5	0.8	0.8	0.8
	[E.1] Errores de los usuarios	4	4	5	4	1	1	16	20	16	4	4	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de	4	4.0	5.0	4.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información							
	[E.2] Errores del administrador	1	5	4	3	1	1	5	4	3	1	1	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	1.7	1.3	1.0	0.3	0.3
	[E.19] Fugas de información	2	2	4	5	1	1	4	8	10	2	2	Transferir	Detectivo	8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 8.2.2. Etiquetado de la Información 8.3.2. Disposición de los medios de soporte	3	1.3	2.7	3.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.20] Vulnerabilidades de los programas (software)	2	4	5	4	2	1	8	10	8	4	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	2.7	3.3	2.7	1.3	0.7
	[E.21] Errores de mantenimiento / actualización de programas	2	4	4	2	1	1	8	8	4	2	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	2.0	2.0	1.0	0.5	0.5
	[A.5] Suplantación de la identidad del usuario	1	4	5	5	2	2	4	5	5	2	2	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	1.0	1.3	1.3	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.7] Uso no previsto	3	4	5	5	1	1	12	15	15	3	3	Aceptar	Detectivo	5.1.2. Revisión de las Políticas para seguridad de la información 6.1.2. Separación de deberes A.8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 18.2.1. Revisión independiente de la seguridad de la información	4	3.0	3.8	3.8	0.8	0.8
	[A.11] Acceso no autorizado	3	2	5	2	1	1	6	15	6	3	3	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	1.5	3.8	1.5	0.8	0.8
	Spark																				
	[I.5] Avería de origen físico o lógico	3	4	2	1	1	1	12	6	3	3	3	Aceptar	Correctivo	8.3.1. Gestión de medios de Soporte Removibles 8.2.3. Manejo de Activos 8.3.2. Disposición de los medios de soporte 18.1.3. Protección de registros.	4	3.0	1.5	0.8	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.1] Errores de los usuarios	1	4	5	4	1	1	4	5	4	1	1	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información	4	1.0	1.3	1.0	0.3	0.3
	[E.2] Errores del administrador	2	5	4	3	1	1	10	8	6	2	2	Transferir	Correctivo	6.1.2. Separación de deberes 14.2.8. Pruebas de seguridad de sistemas 16.1.2. Informe de eventos de seguridad de la información 16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	3	3.3	2.7	2.0	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.15] Alteración accidental de la información	2	4	5	4	3	1	8	10	8	6	2	Transferir	Correctivo	7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.4.1. Restricción de acceso a información 12.1.1. Procedimientos de operación documentadas 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	4	2.0	2.5	2.0	1.5	0.5
	[E.21] Errores de mantenimiento / actualización de programas	1	4	4	2	1	1	4	4	2	1	1	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	1.0	1.0	0.5	0.3	0.3
	[A.5] Suplantación de la identidad del usuario	2	4	5	5	2	2	8	10	10	4	4	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	2.0	2.5	2.5	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.11] Acceso no autorizado	2	2	5	2	1	1	4	10	4	2	2	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.3.1. Copias de respaldo de la información 18.1.3. Protección de registros	4	1.0	2.5	1.0	0.5	0.5
	[A.19] Divulgación de información	2	2	1	5	4	1	4	2	10	8	2	Transferir	Correctivo	7.1.2. Términos y condiciones del empleo 7.3.1. Terminación o cambio de responsabilidades de empleo 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas 12.4.2. Protección de la información de registro 18.1.3. Protección de registros	4	1.0	0.5	2.5	2.0	0.5
	Navegadores																				
	[E.1] Errores de los usuarios	2	4	5	4	1	1	8	10	8	2	2	Controlar	Detectivo	7.1.2. Términos y condiciones del empleo 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 8.1.3. Uso Aceptable	4	2.0	2.5	2.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															de los Activos 8.2.3. Manejo de Activos 9.1.1. Política de Control de Acceso 12.7.1. Controles sobre auditorías de Sistemas de Información						
	[E.19] Fugas de información	2	2	4	5	1	1	4	8	10	2	2	Transferir	Detectivo	8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 8.2.2. Etiquetado de la Información 8.3.2. Disposición de los medios de soporte	3	1.3	2.7	3.3	0.7	0.7
	[E.20] Vulnerabilidades de los programas (software)	3	4	5	4	2	1	12	15	12	6	3	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones 15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	3	4.0	5.0	4.0	2.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.21] Errores de mantenimiento / actualización de programas	2	4	4	2	1	1	8	8	4	2	2	Controlar	Preventivo	14.2.2. Procedimiento de control de cambios en sistemas 14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	4	2.0	2.0	1.0	0.5	0.5
	[A.5] Suplantación de la identidad del usuario	1	4	5	5	2	2	4	5	5	2	2	Controlar	Preventivo	9.1.1. Política de Control de Acceso. 9.2.1. Registro y cancelación del registro de usuarios 9.2.2. Suministro de acceso de usuarios 9.4.3. Sistema de Gestión de Contraseñas	4	1.0	1.3	1.3	0.5	0.5
	[A.6] Abuso de privilegios de acceso	1	4	5	5	2	1	4	5	5	2	1	Controlar	Detectivo							
	[A.7] Uso no previsto	2	4	5	5	1	1	8	10	10	2	2	Aceptar	Detectivo	5.1.2. Revisión de las Políticas para seguridad de la información 6.1.2. Separación de deberes A.8.1.3. Uso Aceptable de los Activos 8.2.1. Clasificación de la Información 18.2.1. Revisión independiente de la seguridad de la información	4	2.0	2.5	2.5	0.5	0.5
ACTIVOS DE HARDWARE	**Servidor principal (EVANS)**																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	4	5	2	1	1	1	20	8	4	4	4	Aceptar	Correctivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 12.1.3. Gestión de Capacidad 12.6.1. Gestión de las vulnerabilidades técnicas 11.2.4 Mantenimiento de los equipos 17.1.1. Planificación de la continuidad de la seguridad de la información 17.2.1. Disponibilidad de instalaciones de procesamiento de información	4	5.0	2.0	1.0	1.0	1.0
	[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	1.3	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.2] Errores del administrador	1	5	5	4	3	3	5	5	4	3	3	Controlar	Detectivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la información 18.1.3. Protección de registros 18.2.2. Cumplimiento con las políticas y normas de seguridad	4	1.3	1.3	1.0	0.8	0.8
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	2	1	1	1	15	6	3	3	3	Controlar	Correctivo	8.2.3. Manejo de Activos 11.2.4. Mantenimiento de equipos. 12.1.1. Procedimientos de operación documentadas 12.2.1. Controles contra códigos maliciosos	4	3.8	1.5	0.8	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.24] Caída del sistema por agotamiento de recursos	4	5	2	1	1	1	20	8	4	4	4	Controlar	Correctivo	11.2.4. Mantenimiento de equipos. 12.1.3. Gestión de Capacidad 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de procesamiento de información.	4	5.0	2.0	1.0	1.0	1.0
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	11.2.8. Equipos sin supervisión de los usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos 11.2.1. Ubicación y protección de los equipos 1.2.8. Equipos sin supervisión de los usuarios	3	1.3	0.7	1.3	0.7	0.7
	[A.24] Denegación de servicio	4	5	2	1	1	1	20	8	4	4	4	Controlar	Detectivo	12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones sobre la instalación de Software 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información.	4	5.0	2.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															17.1.2. Implementación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de procesamiento de información.							
	Servidor de archivos (CEGDOC)																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 12.1.3. Gestión de Capacidad 12.6.1. Gestión de las vulnerabilidades técnicas 11.2.4 Mantenimiento de los equipos 17.1.1. Planificación de la continuidad de la seguridad de la información 17.2.1. Disponibilidad de instalaciones de procesamiento de información	4	1.3	0.5	0.3	0.3	0.3
	[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	1.3	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.2] Errores del administrador	1	5	5	4	3	3	5	5	4	3	3	Controlar	Detectivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la información 18.1.3. Protección de registros 18.2.2. Cumplimiento con las políticas y normas de seguridad	4	1.3	1.3	1.0	0.8	0.8
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	2	1	1	1	15	6	3	3	3	Controlar	Correctivo	8.2.3. Manejo de Activos 11.2.4. Mantenimiento de equipos. 12.1.1. Procedimientos de operación documentadas 12.2.1. Controles contra códigos maliciosos	4	3.8	1.5	0.8	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.24] Caída del sistema por agotamiento de recursos	2	5	2	1	1	1	10	4	2	2	2	Controlar	Correctivo	11.2.4. Mantenimiento de equipos. 12.1.3. Gestión de Capacidad 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de procesamiento de información.	4	2.5	1.0	0.5	0.5	0.5
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	11.2.8. Equipos sin supervisión de los usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos 11.2.1. Ubicación y protección de los equipos 1.2.8. Equipos sin supervisión de los usuarios	3	1.3	0.7	1.3	0.7	0.7
	[A.24] Denegación de servicio	2	5	2	1	1	1	10	4	2	2	2	Controlar	Detectivo	12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones sobre la instalación de Software 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información.	4	2.5	1.0	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															17.1.2. Implementación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de procesamiento de información.						
	Servidor de Dominio (MSCD1)																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 12.1.3. Gestión de Capacidad 12.6.1. Gestión de las vulnerabilidades técnicas 11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															17.1.1. Planificación de la continuidad de la seguridad de la información 17.2.1. Disponibilidad de instalaciones de procesamiento de información							
	[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	1.3	0.3	0.3	0.3	0.3
	[E.2] Errores del administrador	1	5	5	4	3	3	5	5	4	3	3	Controlar	Detectivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la	4	1.3	1.3	1.0	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															información 18.1.3. Protección de registros 18.2.2. Cumplimiento con las políticas y normas de seguridad							
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	2	1	1	1	15	6	3	3	3	Controlar	Correctivo	8.2.3. Manejo de Activos 11.2.4. Mantenimiento de equipos. 12.1.1. Procedimientos de operación documentadas 12.2.1. Controles contra códigos maliciosos	4	3.8	1.5	0.8	0.8	0.8
	[E.24] Caída del sistema por agotamiento de recursos	2	5	2	1	1	1	10	4	2	2	2	Controlar	Correctivo	11.2.4. Mantenimiento de equipos. 12.1.3. Gestión de Capacidad 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información.	4	2.5	1.0	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															17.2.1. Disponibilidad de instalaciones de procesamiento de información.						
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	11.2.8. Equipos sin supervisión de los usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos 11.2.1. Ubicación y protección de los equipos 1.2.8. Equipos sin supervisión de los usuarios	3	1.3	0.7	1.3	0.7	0.7
	[A.24] Denegación de servicio	2	5	2	1	1	1	10	4	2	2	2	Controlar	Detectivo	12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones sobre la instalación de Software 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implementación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de	4	2.5	1.0	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															procesamiento de información.						
	SAN HP																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 12.1.3. Gestión de Capacidad 12.6.1. Gestión de las vulnerabilidades técnicas	4	2.5	1.0	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															11.2.4 Mantenimiento de los equipos 17.1.1. Planificación de la continuidad de la seguridad de la información 17.2.1. Disponibilidad de instalaciones de procesamiento de información						
	[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	1.3	0.3	0.3	0.3	0.3
	[E.2] Errores del administrador	2	5	5	4	3	3	10	10	8	6	6	Controlar	Detectivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la	4	2.5	2.5	2.0	1.5	1.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															información 18.1.3. Protección de registros 18.2.2. Cumplimiento con las políticas y normas de seguridad							
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	2	1	1	1	15	6	3	3	3	Controlar	Correctivo	8.2.3. Manejo de Activos 11.2.4. Mantenimiento de equipos. 12.1.1. Procedimientos de operación documentadas 12.2.1. Controles contra códigos maliciosos	4	3.8	1.5	0.8	0.8	0.8
	[E.24] Caída del sistema por agotamiento de recursos	4	5	2	1	1	1	20	8	4	4	4	Controlar	Correctivo	11.2.4. Mantenimiento de equipos. 12.1.3. Gestión de Capacidad 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información.	4	5.0	2.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															17.2.1. Disponibilidad de instalaciones de procesamiento de información.						
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	11.2.8. Equipos sin supervisión de los usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos 11.2.1. Ubicación y protección de los equipos 1.2.8. Equipos sin supervisión de los usuarios	3	1.3	0.7	1.3	0.7	0.7
	[A.24] Denegación de servicio	4	5	2	1	1	1	20	8	4	4	4	Controlar	Detectivo	12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones sobre la instalación de Software 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implementación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de	4	5.0	2.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															procesamiento de información.						
	FORTIGATE 300C																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	1	4	1	1	1	1	4	1	1	1	1	Controlar	Preventivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 11.2.4 Mantenimiento de los equipos	4	1.0	0.3	0.3	0.3	0.3
	[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	6.1.2. Separación de deberes. 8.1.3. Uso Aceptable de los Activos 11.1.4. Protección contra amenazas externas y ambientales 12.1.3. Gestión de Capacidad 12.6.1. Gestión de las vulnerabilidades técnicas 11.2.4 Mantenimiento de los equipos 17.1.1. Planificación de la continuidad de la seguridad de la información 17.2.1. Disponibilidad de instalaciones de procesamiento de información	4	1.3	0.5	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	1.3	0.3	0.3	0.3	0.3
	[E.2] Errores del administrador	3	5	5	4	3	3	15	15	12	9	9	Controlar	Detectivo	6.1.2. Separación de deberes 7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información 9.1.1. Política de Control de Acceso 9.2.3. Gestión de derechos de acceso privilegiado 9.4.1. Restricción de acceso a información 9.4.4. Uso de programas utilitarios privilegiados 12.1.1. Procedimientos de operación documentadas 16.1.3. Informe de debilidades de seguridad de la información 18.1.3. Protección de registros 18.2.2. Cumplimiento con las políticas y normas de seguridad	4	3.8	3.8	3.0	2.3	2.3
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	2	1	1	1	15	6	3	3	3	Controlar	Correctivo	8.2.3. Manejo de Activos 11.2.4. Mantenimiento de equipos. 12.1.1. Procedimientos de operación	4	3.8	1.5	0.8	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															documentadas 12.2.1. Controles contra códigos maliciosos						
	[E.24] Caída del sistema por agotamiento de recursos	3	5	2	1	1	1	15	6	3	3	3	Controlar	Correctivo	11.2.4. Mantenimiento de equipos. 12.1.3. Gestión de Capacidad 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de procesamiento de información.	4	3.8	1.5	0.8	0.8	0.8
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	11.2.8. Equipos sin supervisión de los usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos 11.2.1. Ubicación y protección de los equipos 1.2.8. Equipos sin supervisión de los usuarios	3	1.3	0.7	1.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.24] Denegación de servicio	4	5	2	1	1	1	20	8	4	4	4	Controlar	Detectivo	12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones sobre la instalación de Software 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implementación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de procesamiento de información.	4	5.0	2.0	1.0	1.0	1.0
	PC Control Interno de gestión																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de	3	4.0	4.0	5.0	3.0	2.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															seguridad de la información						
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
	PC Revisoría Fiscal																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
	PC Gerencia																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
	Portátil Gerencia																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
	[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	1.3	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.25] Pérdida de equipos	1	5	1	5	2	1	5	1	5	2	1	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	1.7	0.3	1.7	0.7	0.3
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	PC Jurídica administrativa																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas	4	2.5	0.5	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.7	1.3	1.3	0.3	0.3
	PC Jurídica laboral																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.7	1.3	1.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
PC gabys																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.7	1.3	1.3	0.3	0.3
PC PLANEACION																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
	PORTATIL PLANEACION																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
	[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	1.3	0.3	0.3	0.3	0.3
	[E.25] Pérdida de equipos	1	5	1	5	2	1	5	1	5	2	1	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	1.7	0.3	1.7	0.7	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	PC SISTEMAS																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	5	2	1	1	1	5	2	1	1	1	Controlar	Correctivo	8.2.3. Manejo de Activos 11.2.4. Mantenimiento de equipos. 12.1.1. Procedimientos de operación documentadas 12.2.1. Controles contra códigos maliciosos	4	1.3	0.5	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.24] Caída del sistema por agotamiento de recursos	2	5	2	1	1	1	10	4	2	2	2	Controlar	Correctivo	11.2.4. Mantenimiento de equipos. 12.1.3. Gestión de Capacidad 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de procesamiento de información.	4	2.5	1.0	0.5	0.5	0.5
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	11.2.8. Equipos sin supervisión de los usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos 11.2.1. Ubicación y protección de los equipos 1.2.8. Equipos sin supervisión de los usuarios	3	1.3	0.7	1.3	0.7	0.7
	[A.24] Denegación de servicio	1	5	2	1	1	1	5	2	1	1	1	Controlar	Detectivo	12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones sobre la instalación de Software 16.1.2. Informe de eventos de seguridad de la información. 17.1.1. Planificación de la continuidad de la seguridad de la información.	4	1.3	0.5	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															17.1.2. Implementación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones de procesamiento de información.							
	PORTATIL SISTEMAS																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
	[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	1.3	0.3	0.3	0.3	0.3
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	3.3	0.7	3.3	1.3	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
PC ESTADISTICA																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
PC PRENSA																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	1	4	1	1	1	1	4	1	1	1	1	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	1.0	0.3	0.3	0.3	0.3
[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
PC CEGDOC																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
	PC Subsalud																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
	Portátil Subsalud																				

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	1.3	0.3	0.3	0.3	0.3
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
PC Epidemiología																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
Portátil Epidemiología																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
[I.6] Corte del suministro eléctrico	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas	4	1.3	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	PC Docencia																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
	[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
PC SIAU																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
PC Medicina interna y especialidades - Piso 7																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.0	4.0	4.0	2.0	2.0
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
PC Medicina interna y especialidades - Piso 10																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.0	4.0	4.0	2.0	2.0
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
PC Pediatría																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los	3	2.0	4.0	4.0	2.0	2.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														derechos de acceso asignados a usuarios						
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
PC Pediatría administrativo																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	2	2	4	4	2	2	4	8	8	4	4	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	1.3	2.7	2.7	1.3	1.3
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
Portátil Pediatría																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.25] Robo	2	5	4	4	1	1	10	8	8	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	5.0	4.0	4.0	1.0	1.0
PC Pediatría quirúrgica																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.0	4.0	4.0	2.0	2.0
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
PC Banco de leche																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.0	4.0	4.0	2.0	2.0
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
Portátil Madre canguro																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	4	1	1	1	1	8	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.0	0.5	0.5	0.5	0.5
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.25] Pérdida de equipos	3	5	1	5	2	1	15	3	15	6	3	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	5.0	1.0	5.0	2.0	1.0
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.25] Robo	4	5	4	4	1	1	20	16	16	4	4	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	10.0	8.0	8.0	2.0	2.0
PC Sala cuna - Neonatos																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
PC Cirugía general																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
	[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
	[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.0	4.0	4.0	2.0	2.0
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
	Portátil Cirugía general																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
	[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
PC Endoscopia																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas	4	3.8	0.8	0.8	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.0	4.0	4.0	2.0	2.0
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
	PC Cirugía general piso 9																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
	[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
	[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.0	4.0	4.0	2.0	2.0
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
Portátil Cirugía general piso 9																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de	2	2.5	2.0	2.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															seguridad de la información						
	PC Neuro																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
	[I.5] Avería de origen físico o lógico	4	5	2	1	1	1	20	8	4	4	4	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	5.0	2.0	1.0	1.0	1.0
	[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.0	4.0	4.0	2.0	2.0
	[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
	Portátil Neuro																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	1	5	2	1	1	1	5	2	1	1	1	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.5	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
PC Ginecología-obstetricia																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.25] Pérdida de equipos	1	5	1	5	2	1	5	1	5	2	1	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	1.7	0.3	1.7	0.7	0.3
[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
[A.11] Acceso no autorizado	1	2	4	4	2	2	2	4	4	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	0.7	1.3	1.3	0.7	0.7
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Correctivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
PC Sala de partos																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
[I.5] Avería de origen físico o lógico	4	5	2	1	1	1	20	8	4	4	4	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	5.0	2.0	1.0	1.0	1.0
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	2.7	2.7	3.3	2.0	1.3
[A.11] Acceso no autorizado	2	2	4	4	2	2	4	8	8	4	4	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	1.3	2.7	2.7	1.3	1.3
[A.23] Manipulación de los equipos	1	4	2	4	2	2	4	2	4	2	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	1.3	0.7	1.3	0.7	0.7
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos	2	2.5	2.0	2.0	0.5	0.5

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														12.3.1 Copias de seguridad de la información						
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Correctivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Consulta externa																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	4	4	1	1	1	1	16	4	4	4	4	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	4.0	1.0	1.0	1.0	1.0
[I.5] Avería de origen físico o lógico	3	5	2	1	1	1	15	6	3	3	3	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	3.8	1.5	0.8	0.8	0.8
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.25] Pérdida de equipos	1	5	1	5	2	1	5	1	5	2	1	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	1.7	0.3	1.7	0.7	0.3
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.11] Acceso no autorizado	2	2	4	4	2	2	4	8	8	4	4	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	1.3	2.7	2.7	1.3	1.3
[A.23] Manipulación de los equipos	2	4	2	4	2	2	8	4	8	4	4	Controlar	Detectivo	9.1.1 Política de control de accesos	3	2.7	1.3	2.7	1.3	1.3
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Correctivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
PC Consulta externa administrativo																				
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.25] Pérdida de equipos	1	5	1	5	2	1	5	1	5	2	1	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física.	3	1.7	0.3	1.7	0.7	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.							
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	2	2	4	4	2	2	4	8	8	4	4	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	1.3	2.7	2.7	1.3	1.3
	[A.23] Manipulación de los equipos	2	4	2	4	2	2	8	4	8	4	4	Controlar	Detectivo	9.1.1 Política de control de accesos	3	2.7	1.3	2.7	1.3	1.3
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Correctivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
	PC Consulta externa - urología																				
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	6.1.3. Contacto con las autoridades 8.1.2. Propiedad de los activos. 8.2.3. Manejo de Activos. 11.1.1. Perímetro de Seguridad Física. 11.1.2. Controles Físicos de entrada 11.1.3. Seguridad de oficinas, salones e instalaciones.	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.0	4.0	4.0	2.0	2.0
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Detectivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	PC Urgencias adultos y cuidados intermedios																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Aceptar	Correctivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Detectivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Aceptar	Correctivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Urgencias adultos administrativo																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento /	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	actualización de equipos (hardware)																				
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Urgencias pediatría																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación	2	5.0	1.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															de la legislación aplicable						
	PC Referencia																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	3	5	1	1	1	1	15	3	3	3	3	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	3.8	0.8	0.8	0.8	0.8
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	3	5	1	5	2	1	15	3	15	6	3	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	5.0	1.0	5.0	2.0	1.0
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los	3	4.0	4.0	5.0	3.0	2.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														derechos de acceso asignados a usuarios						
[A.11] Acceso no autorizado	4	2	5	5	2	2	8	20	20	8	8	Transferir	Preventivo	9.1.1 Política de control de accesos	4	2.0	5.0	5.0	2.0	2.0
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Quirófanos																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	1	5	1	5	2	1	5	1	5	2	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	1.7	0.3	1.7	0.7	0.3
[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.7	2.7	3.3	2.0	1.3
[A.11] Acceso no autorizado	2	2	4	4	2	2	4	8	8	4	4	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.0	2.0	2.0	1.0	1.0
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
PC Quirófanos Administrativo																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	1	5	1	5	2	1	5	1	5	2	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	1.7	0.3	1.7	0.7	0.3
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	2	2	4	4	2	2	4	8	8	4	4	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.0	2.0	2.0	1.0	1.0
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de	2	2.5	2.0	2.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															seguridad de la información						
	[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
	PC Esterilización																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	1	5	1	5	2	1	5	1	5	2	1	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de	3	1.7	0.3	1.7	0.7	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															seguridad de la información						
	[A.7] Uso no previsto	2	4	4	5	3	2	8	8	10	6	4	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	2.7	2.7	3.3	2.0	1.3
	[A.11] Acceso no autorizado	2	2	4	4	2	2	4	8	8	4	4	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.0	2.0	2.0	1.0	1.0
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
	PC Apoyo a la atención																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Radiología																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Ecografía																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Laboratorio Clínico																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	5.0	1.0	2.0	1.0	1.0
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos	4	3.0	3.0	3.8	2.3	1.5
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	3	2.0	4.0	4.0	2.0	2.0
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	6.0	3.0	6.0	3.0	3.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información	4	2.5	0.5	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															18.1.1 Identificación de la legislación aplicable						
	PC Banco de Sangre																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	5.0	1.0	2.0	1.0	1.0
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los	3	3.3	0.7	3.3	1.3	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															derechos de acceso asignados a usuarios						
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos	4	3.0	3.0	3.8	2.3	1.5
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	3	2.0	4.0	4.0	2.0	2.0
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	6.0	3.0	6.0	3.0	3.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	4	2.5	0.5	0.5	0.5	0.5
	PC Patología																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Radioterapia																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														externas y ambientales.						
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Rehabilitación																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Farmacia Administrativo																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
PC Farmacia Principal																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Farmacia 2piso																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Coordinación de enfermería																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información	2	5.0	1.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															18.1.1 Identificación de la legislación aplicable						
	PC Nutrición																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los	3	4.0	4.0	5.0	3.0	2.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															derechos de acceso asignados a usuarios						
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Subgerencia Administrativa																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	2	5	4	4	1	1	10	8	8	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	5.0	4.0	4.0	1.0	1.0
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
Portátil Subgerencia Administrativa																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	2	5	4	4	1	1	10	8	8	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de	2	5.0	4.0	4.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															seguridad de la información						
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Financiera																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de	3	3.3	0.7	3.3	1.3	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															seguridad de la información						
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Facturación																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	5	5	2	2	6	15	15	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.8	3.8	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	2	5	4	4	1	1	10	8	8	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	5.0	4.0	4.0	1.0	1.0
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Cartera - Auditoría de cuentas																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos	2	2.5	2.0	2.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															12.3.1 Copias de seguridad de la información						
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Contratación y mercadeo																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Talento Humano																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información	2	5.0	1.0	1.0	1.0	1.0
PC Nomina																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos	2	2.5	2.0	2.0	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															12.3.1 Copias de seguridad de la información						
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Recursos físicos																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos	3	3.3	0.7	3.3	1.3	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														12.3.1 Copias de seguridad de la información						
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Almacén																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
PC Biomedicina																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															externas y ambientales.						
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
	PC Mantenimiento																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	3	4	1	1	1	1	12	3	3	3	3	Controlar	Preventivo	11.2.4 Mantenimiento de los equipos	4	3.0	0.8	0.8	0.8	0.8
	[I.5] Avería de origen físico o lógico	2	5	2	1	1	1	10	4	2	2	2	Aceptar	Correctivo	11.2.4 Mantenimiento de los equipos	4	2.5	1.0	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	1	2	1	1	15	3	6	3	3	Controlar	Detectivo	11.2.4 Mantenimiento de los equipos	4	3.8	0.8	1.5	0.8	0.8

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.25] Pérdida de equipos	2	5	1	5	2	1	10	2	10	4	2	Controlar	Detectivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	1.3	0.7
	[A.7] Uso no previsto	3	4	4	5	3	2	12	12	15	9	6	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	4.0	4.0	5.0	3.0	2.0
	[A.11] Acceso no autorizado	3	2	4	4	2	2	6	12	12	6	6	Transferir	Preventivo	9.1.1 Política de control de accesos	4	1.5	3.0	3.0	1.5	1.5
	[A.23] Manipulación de los equipos	3	4	2	4	2	2	12	6	12	6	6	Controlar	Preventivo	9.1.1 Política de control de accesos	3	4.0	2.0	4.0	2.0	2.0
	[A.25] Robo	1	5	4	4	1	1	5	4	4	1	1	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	2.5	2.0	2.0	0.5	0.5
	[A.26] Ataque destructivo	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	5.0	1.0	1.0	1.0	1.0
ACTIVOS DE RED	**CORE**																				
	[I.8] Fallo de servicios de comunicaciones	3	5	1	1	1	1	15	3	3	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	1.0	1.0	1.0
	[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
	[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
	[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	1	1	1	1	15	3	3	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	1.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.15] Modificación deliberada de la información	2	1	5	3	2	1	2	10	6	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	0.7
	[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
	SW SERVIDORES																				
	[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
	[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
	[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
	[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
	[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
	[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	0.7	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														13.1.3 Segregación de redes						
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW URG_ADULTOS																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW URG_PEDIATRIA																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red.	3	5.0	1.0	2.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															13.1.3 Segregación de redes						
	[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
	[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
	[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
	[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
	[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
	[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
	[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
	[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
	[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.3	0.3	1.7	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														asociados a servicios en red						
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW URG_RAYOSX																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW BANCO_DE_SANGRE																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad	3	3.3	0.7	1.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															asociados a servicios en red						
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
	[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
	[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
	[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
	[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
	[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
	[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
	[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
	[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.7	3.3	2.0	1.3	1.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														asociados a servicios en red						
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW LABORATORIO																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
SW ESTADISTICA																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW CONTABILIDAD1																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.3	1.7	1.0	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														asociados a servicios en red						
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW CONTABILIDAD2																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.7	1.3	3.3	1.3	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														asociados a servicios en red						
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW VIGILANCIA																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW CARTERA																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW ALMACEN1																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red.	3	5.0	1.0	2.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															13.1.3 Segregación de redes						
	[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
	[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
	[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
	[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
	[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
	[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
	[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
	[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
	[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.3	0.3	1.7	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														asociados a servicios en red						
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW ALMACEN2																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW MANTENIMIENTO																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad	3	3.3	0.7	1.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															asociados a servicios en red						
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
	[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
	[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
	[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
	[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
	[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
	[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
	[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
	[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.7	3.3	2.0	1.3	1.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														asociados a servicios en red						
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW RADIOTERAPIA																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
SW CENTRAL																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW PISO3																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.3	1.7	1.0	0.3	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														asociados a servicios en red						
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW PISO5																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.7	1.3	3.3	1.3	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														asociados a servicios en red						
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW PISO6																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW PISO7																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW PISO8																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red.	3	5.0	1.0	2.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															13.1.3 Segregación de redes						
	[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
	[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
	[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
	[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
	[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
	[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
	[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
	[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
	[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.3	0.3	1.7	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															asociados a servicios en red						
	[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
	[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
	[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
	[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
	[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
	SW PISO9																				
	[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
	[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
	[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW PISO9-2																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad	3	3.3	0.7	1.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															asociados a servicios en red						
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
	[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
	[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
	[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
	[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
	[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
	[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
	[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
	[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.7	3.3	2.0	1.3	1.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
														asociados a servicios en red						
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW PISO10																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
SW PISO11																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
SW PISO12																				
[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.3	1.7	1.0	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															asociados a servicios en red						
	[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	0.7	3.3	3.3	0.7	0.7
	[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	1.3	0.7
	[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
	[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
	ACCESS POINT INALAMBRICO																				
	[I.8] Fallo de servicios de comunicaciones	3	5	1	2	1	1	15	3	6	3	3	Controlar	Preventivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	1.0	2.0	1.0	1.0
	[E.2] Errores del administrador	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.4.4 Uso de herramientas de administración de sistemas	2	5.0	5.0	5.0	1.0	1.0
	[E.9] Errores de re-encaminamiento	2	1	2	5	1	1	2	4	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	1.3	3.3	0.7	0.7
	[E.10] Errores de Secuencia	1	1	5	2	2	1	1	5	2	2	1	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	0.7	0.7	0.3

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.15] Alteración accidental de la información	2	1	5	2	2	1	2	10	4	4	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	1.3	1.3	0.7
[E.18] Destrucción de información	2	5	1	2	1	1	10	2	4	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	1.3	0.7	0.7
[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
[E.24] Caída del sistema por agotamiento de recursos	3	5	2	2	1	1	15	6	6	3	3	Controlar	Detectivo	13.1.1 Controles de red. 13.1.3 Segregación de redes	3	5.0	2.0	2.0	1.0	1.0
[A.5] Suplantación de la identidad del usuario	2	1	5	5	5	1	2	10	10	10	2	Controlar	Preventivo	9.4.2 Procedimientos seguros de inicio de sesión	3	0.7	3.3	3.3	3.3	0.7
[A.6] Abuso de privilegios de acceso	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
[A.9] [Re-]encaminamiento de mensajes	1	1	1	5	1	1	1	1	5	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	0.3	1.7	0.3	0.3
[A.10] Alteración de secuencia	1	1	5	3	1	1	1	5	3	1	1	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.3	1.7	1.0	0.3	0.3
[A.11] Acceso no autorizado	3	1	5	5	1	1	3	15	15	3	3	Controlar	Preventivo	9.1.1 Política de control de accesos	3	1.0	5.0	5.0	1.0	1.0
[A.12] Análisis de tráfico	2	1	2	5	2	1	2	4	10	4	2	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad	3	0.7	1.3	3.3	1.3	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															asociados a servicios en red						
	[A.15] Modificación deliberada de la información	2	1	5	3	2	2	2	10	6	4	4	Controlar	Detectivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	2.0	1.3	1.3
	[A.24] Denegación de servicio	2	5	1	3	1	1	10	2	6	2	2	Controlar	Preventivo	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	3	3.3	0.7	2.0	0.7	0.7
ACTIVOS DE INSTALACIÓN	**CENTRAL DE DATOS**																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[E.15] Alteración accidental de la información	2	1	5	1	1	1	2	10	2	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	0.7	0.7	0.7
	[E.18] Destrucción de información	1	5	1	1	1	1	5	1	1	1	1	Controlar	Preventivo	9.2.3. Gestión de derechos de acceso privilegiado 12.3.1. Copias de respaldo de la información	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															A.18.1.3. Protección de registros						
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
	[A.7] Uso no previsto	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
	[A.11] Acceso no autorizado	2	5	5	1	1	1	10	10	2	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos	4	2.5	2.5	0.5	0.5	0.5
	[A.15] Modificación deliberada de la información	2	1	5	1	1	1	2	10	2	2	2	Controlar	Preventivo	12.3.1 Copias de seguridad de la información. 12.6.1 Gestión de las vulnerabilidades técnicas	3	0.7	3.3	0.7	0.7	0.7
	[A.18] Destrucción de información	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	9.2.3. Gestión de derechos de acceso privilegiado 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	3	1.7	0.3	0.3	0.3	0.3
	[A.19] Divulgación de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	18.1.3 Protección de los registros de la organización. 18.1.4 Protección de datos y privacidad de la información personal	2	1.0	1.0	5.0	1.0	1.0
	[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación	2	2.5	0.5	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															de la legislación aplicable						
	CENTRALES DE CABLEADO																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.11] Emanaciones electromagnéticas	1	1	1	5	1	1	1	1	5	1	1	Controlar	Preventivo	11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Seguridad del cableado	3	0.3	0.3	1.7	0.3	0.3
	[E.15] Alteración accidental de la información	2	1	5	1	1	1	2	10	2	2	2	Controlar	Preventivo	13.1.2 Mecanismos de seguridad asociados a servicios en red	3	0.7	3.3	0.7	0.7	0.7
	[E.18] Destrucción de información	1	5	1	1	1	1	5	1	1	1	1	Controlar	Preventivo	9.2.3. Gestión de derechos de acceso privilegiado 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	3	1.7	0.3	0.3	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Detectivo	13.1.2 Mecanismos de seguridad asociados a servicios en red 13.1.3 Segregación de redes	3	0.7	0.7	3.3	0.7	0.7
	[A.7] Uso no previsto	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios	3	3.3	3.3	3.3	0.7	0.7
	[A.11] Acceso no autorizado	3	5	5	1	1	1	15	15	3	3	3	Transferir	Preventivo	9.1.1 Política de control de accesos	4	3.8	3.8	0.8	0.8	0.8
	[A.15] Modificación deliberada de la información	2	1	5	1	1	1	2	10	2	2	2	Controlar	Preventivo	12.3.1 Copias de seguridad de la información. 12.6.1 Gestión de las vulnerabilidades técnicas	3	0.7	3.3	0.7	0.7	0.7
	[A.18] Destrucción de información	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	9.2.3. Gestión de derechos de acceso privilegiado 12.3.1. Copias de respaldo de la información A.18.1.3. Protección de registros	3	1.7	0.3	0.3	0.3	0.3
	[A.19] Divulgación de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	18.1.3 Protección de los registros de la organización. 18.1.4 Protección de datos y privacidad de la información personal	2	1.0	1.0	5.0	1.0	1.0
	[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
ACTI	**EQUIPOS DE CLIMATIZACION -**																				

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	AIRE ACONDICIONADO																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
	[I.4] Contaminación electromagnética	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.3	0.3	0.3	0.3
	[I.5] Avería de origen físico o lógico	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Correctivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.4.2 Protección de los registros de información. 11.2.1 Emplazamiento y protección de equipos	3	3.3	0.7	0.7	0.7	0.7

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[E.25] Pérdida de equipos	2	5	1	5	1	1	10	2	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	0.7	0.7
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos	4	2.5	0.5	2.5	0.5	0.5
[A.23] Manipulación de los equipos	2	5	1	5	1	1	10	2	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	3.3	0.7	3.3	0.7	0.7
[A.25] Robo	3	5	1	5	1	1	15	3	15	3	3	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	7.5	1.5	7.5	1.5	1.5
[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
UPS SERVIDORES																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[I.4] Contaminación electromagnética	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.3	0.3	0.3	0.3
	[I.5] Avería de origen físico o lógico	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
	[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Correctivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.4.2 Protección de los registros de información. 11.2.1 Emplazamiento y protección de equipos	3	3.3	0.7	0.7	0.7	0.7
	[E.25] Pérdida de equipos	2	5	1	5	1	1	10	2	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	0.7	0.7
	[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos	4	2.5	0.5	2.5	0.5	0.5
	[A.23] Manipulación de los equipos	2	5	1	5	1	1	10	2	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	3.3	0.7	3.3	0.7	0.7
	[A.25] Robo	3	5	1	5	1	1	15	3	15	3	3	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	7.5	1.5	7.5	1.5	1.5
	[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
	UPS SWITCHES																				

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
[I.4] Contaminación electromagnética	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.3	0.3	0.3	0.3
[I.5] Avería de origen físico o lógico	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Correctivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.4.2 Protección de los registros de información. 11.2.1 Emplazamiento y protección de equipos	3	3.3	0.7	0.7	0.7	0.7
[E.25] Pérdida de equipos	2	5	1	5	1	1	10	2	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos	3	3.3	0.7	3.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															12.3.1 Copias de seguridad de la información						
	[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos	4	2.5	0.5	2.5	0.5	0.5
	[A.23] Manipulación de los equipos	2	5	1	5	1	1	10	2	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	3.3	0.7	3.3	0.7	0.7
	[A.25] Robo	3	5	1	5	1	1	15	3	15	3	3	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	7.5	1.5	7.5	1.5	1.5
	[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
	SISTEMA DE ENERGIA ELECTRICA																				
	[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
	[I.3] Contaminación mecánica	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
[I.4] Contaminación electromagnética	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.3	0.3	0.3	0.3
[I.5] Avería de origen físico o lógico	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Correctivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.4.2 Protección de los registros de información. 11.2.1 Emplazamiento y protección de equipos	3	3.3	0.7	0.7	0.7	0.7
[E.25] Pérdida de equipos	2	5	1	5	1	1	10	2	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	0.7	0.7
[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos	4	2.5	0.5	2.5	0.5	0.5
[A.23] Manipulación de los equipos	2	5	1	5	1	1	10	2	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	3.3	0.7	3.3	0.7	0.7
[A.25] Robo	3	5	1	5	1	1	15	3	15	3	3	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	7.5	1.5	7.5	1.5	1.5
[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5

Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
		D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
SISTEMA DE ENERGIA ELECTRICA DE EMERGENCIA																				
[N.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.2] Desastres por agua	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[N.7] Fenómeno Sísmico	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.1] Fuego	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	3	1.7	0.3	0.3	0.3	0.3
[I.3] Contaminación mecánica	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
[I.4] Contaminación electromagnética	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	1.3	0.3	0.3	0.3	0.3
[I.5] Avería de origen físico o lógico	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	11.2.4 Mantenimiento de los equipos	4	2.5	0.5	0.5	0.5	0.5
[I.6] Corte del suministro eléctrico	2	5	1	1	1	1	10	2	2	2	2	Controlar	Correctivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	11.1.4 Protección contra las amenazas externas y ambientales.	4	2.5	0.5	0.5	0.5	0.5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	5	1	1	1	1	10	2	2	2	2	Transferir	Preventivo	12.4.2 Protección de los registros de información. 11.2.1 Emplazamiento y	3	3.3	0.7	0.7	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															protección de equipos						
	[E.25] Pérdida de equipos	2	5	1	5	1	1	10	2	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	3	3.3	0.7	3.3	0.7	0.7
	[A.11] Acceso no autorizado	2	1	5	5	1	1	2	10	10	2	2	Transferir	Preventivo	9.1.1 Política de control de accesos	4	2.5	0.5	2.5	0.5	0.5
	[A.23] Manipulación de los equipos	2	5	1	5	1	1	10	2	10	2	2	Controlar	Preventivo	9.1.1 Política de control de accesos	3	3.3	0.7	3.3	0.7	0.7
	[A.25] Robo	3	5	1	5	1	1	15	3	15	3	3	Transferir	Preventivo	9.1.1 Política de control de accesos 12.3.1 Copias de seguridad de la información	2	7.5	1.5	7.5	1.5	1.5
	[A.26] Ataque destructivo	1	5	1	1	1	1	5	1	1	1	1	Transferir	Preventivo	12.3.1 Copias de seguridad de la información 18.1.1 Identificación de la legislación aplicable	2	2.5	0.5	0.5	0.5	0.5
ACTIVOS DE PERSONAL	**USUARIOS INTERNOS**																				
	[E.7] Deficiencias en la organización	2	5	1	1	1	1	10	2	2	2	2	Controlar	Correctivo	5.1.1 Conjunto de políticas para la seguridad de la información 18.1.1 Protección de datos y privacidad de la información personal	3	3.3	0.7	0.7	0.7	0.7
	[E.19] Fugas de información	2	1	1	5	1	1	2	2	10	2	2	Controlar	Preventivo	5.1.1 Conjunto de políticas para la seguridad de la información. 6.1.3 Contacto con las autoridades. 18.1.1 Protección de datos y privacidad de la información	3	0.7	0.7	3.3	0.7	0.7

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															personal. 7.2.2 Concienciación, educación y capacitación en seg de la información						
	[E.28] Indisponibilidad del personal	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	7.1.2 Términos y condiciones de contratación. 7.2.1 Responsabilidades de gestión. 7.3.1 Cese o cambio de puesto de trabajo	3	3.3	0.7	0.7	0.7	0.7
	[A.28] Indisponibilidad del personal	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	17.1.1 Planificación de la continuidad de la seg de la información. 17.1.2 Implantación de la continuidad de la seg de la información	2	2.5	2.5	2.5	0.5	0.5
	[A.29] Extorsión	1	5	5	5	1	1	5	5	5	1	1	Controlar	Correctivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	2	2.5	2.5	2.5	0.5	0.5
	[A.30] Ingeniería social (picaresca)	1	5	5	5	1	1	5	5	5	1	1	Controlar	Preventivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	3	1.7	1.7	1.7	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	USUARIOS EXTERNOS																				
	[E.7] Deficiencias en la organización	1	5	1	1	1	1	5	1	1	1	1	Controlar	Correctivo	5.1.1 Conjunto de políticas para la seguridad de la información 18.1.1 Protección de datos y privacidad de la información personal	3	1.7	0.3	0.3	0.3	0.3
	[E.19] Fugas de información	1	1	1	5	1	1	1	1	5	1	1	Controlar	Preventivo	5.1.1 Conjunto de políticas para la seguridad de la información. 6.1.3 Contacto con las autoridades. 7.2.2 Concienciación, educación y capacitación en seg de la información 18.1.1 Protección de datos y privacidad de la información personal.	3	0.3	0.3	1.7	0.3	0.3
	ADMINISTRADOR DE SISTEMAS																				
	[E.7] Deficiencias en la organización	3	5	1	1	1	1	15	3	3	3	3	Controlar	Correctivo	5.1.1 Conjunto de políticas para la seguridad de la información 18.1.1 Protección de datos y privacidad de la información personal	3	5.0	1.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.19] Fugas de información	3	1	1	5	1	1	3	3	15	3	3	Controlar	Preventivo	5.1.1 Conjunto de políticas para la seguridad de la información. 6.1.3 Contacto con las autoridades. 18.1.1 Protección de datos y privacidad de la información personal. 7.2.2 Concienciación, educación y capacitación en seg de la información	3	1.0	1.0	5.0	1.0	1.0
	[E.28] Indisponibilidad del personal	3	5	1	1	1	1	15	3	3	3	3	Controlar	Preventivo	7.1.2 Términos y condiciones de contratación. 7.2.1 Responsabilidades de gestión. 7.3.1 Cese o cambio de puesto de trabajo	3	5.0	1.0	1.0	1.0	1.0
	[A.28] Indisponibilidad del personal	3	5	1	1	1	1	15	3	3	3	3	Controlar	Preventivo	17.1.1 Planificación de la continuidad de la seg de la información. 17.1.2 Implantación de la continuidad de la seg de la información	2	5.0	5.0	5.0	1.0	1.0
	[A.29] Extorsión	2	5	5	5	1	1	10	10	10	2	2	Controlar	Correctivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	2	5.0	5.0	5.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.30] Ingeniería social (picaresca)	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	3	3.3	3.3	3.3	0.7	0.7
	INGENIERO DE SISTEMAS																				
	[E.7] Deficiencias en la organización	3	5	1	1	1	1	15	3	3	3	3	Controlar	Correctivo	5.1.1 Conjunto de políticas para la seguridad de la información 18.1.1 Protección de datos y privacidad de la información personal	3	5.0	1.0	1.0	1.0	1.0
	[E.19] Fugas de información	3	1	1	5	1	1	3	3	15	3	3	Controlar	Preventivo	5.1.1 Conjunto de políticas para la seguridad de la información. 6.1.3 Contacto con las autoridades. 18.1.1 Protección de datos y privacidad de la información personal. 7.2.2 Concienciación, educación y capacitación en seg de la información	3	1.0	1.0	5.0	1.0	1.0
	[E.28] Indisponibilidad del personal	3	5	1	1	1	1	15	3	3	3	3	Controlar	Preventivo	7.1.2 Términos y condiciones de contratación. 7.2.1 Responsabilidades de gestión. 7.3.1 Cese o cambio de puesto de trabajo	3	5.0	1.0	1.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.28] Indisponibilidad del personal	3	5	1	1	1	1	15	3	3	3	3	Controlar	Preventivo	17.1.1 Planificación de la continuidad de la seg de la información. 17.1.2 Implantación de la continuidad de la seg de la información	2	5.0	5.0	5.0	1.0	1.0
	[A.29] Extorsión	2	5	5	5	1	1	10	10	10	2	2	Controlar	Correctivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	2	5.0	5.0	5.0	1.0	1.0
	[A.30] Ingeniería social (picaresca)	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	3	3.3	3.3	3.3	0.7	0.7
	TECNICOS DE SOPORTE																				
	[E.7] Deficiencias en la organización	3	5	1	1	1	1	15	3	3	3	3	Controlar	Correctivo	5.1.1 Conjunto de políticas para la seguridad de la información 18.1.1 Protección de datos y privacidad de la información personal	3	5.0	1.0	1.0	1.0	1.0
	[E.19] Fugas de información	3	1	1	5	1	1	3	3	15	3	3	Controlar	Preventivo	5.1.1 Conjunto de políticas para la seguridad de la información. 6.1.3 Contacto con las autoridades. 18.1.1 Protección de datos y privacidad de la	3	1.0	1.0	5.0	1.0	1.0

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
															información personal. 7.2.2 Concienciación, educación y capacitación en seg de la información						
	[E.28] Indisponibilidad del personal	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	7.1.2 Términos y condiciones de contratación. 7.2.1 Responsabilidades de gestión. 7.3.1 Cese o cambio de puesto de trabajo	3	3.3	0.7	0.7	0.7	0.7
	[A.28] Indisponibilidad del personal	2	5	1	1	1	1	10	2	2	2	2	Controlar	Preventivo	17.1.1 Planificación de la continuidad de la seg de la información. 17.1.2 Implantación de la continuidad de la seg de la información	2	5.0	5.0	5.0	1.0	1.0
	[A.29] Extorsión	2	5	5	5	1	1	10	10	10	2	2	Controlar	Correctivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	2	5.0	5.0	5.0	1.0	1.0
	[A.30] Ingeniería social (picaresca)	2	5	5	5	1	1	10	10	10	2	2	Controlar	Preventivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	3	3.3	3.3	3.3	0.7	0.7
	PROVEEDORES DE SOPORTE																				

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.7] Deficiencias en la organización	2	5	1	1	1	1	10	2	2	2	2	Controlar	Correctivo	5.1.1 Conjunto de políticas para la seguridad de la información 18.1.1 Protección de datos y privacidad de la información personal	3	3.3	0.7	0.7	0.7	0.7
	[E.19] Fugas de información	1	1	1	5	1	1	1	1	5	1	1	Controlar	Preventivo	5.1.1 Conjunto de políticas para la seguridad de la información. 6.1.3 Contacto con las autoridades. 18.1.1 Protección de datos y privacidad de la información personal. 7.2.2 Concienciación, educación y capacitación en seg de la información	3	0.3	0.3	1.7	0.3	0.3
	[E.28] Indisponibilidad del personal	1	5	1	1	1	1	5	1	1	1	1	Controlar	Preventivo	7.1.2 Términos y condiciones de contratación. 7.2.1 Responsabilidades de gestión. 7.3.1 Cese o cambio de puesto de trabajo	3	1.7	0.3	0.3	0.3	0.3
	[A.28] Indisponibilidad del personal	1	5	1	1	1	1	5	1	1	1	1	Controlar	Preventivo	17.1.1 Planificación de la continuidad de la seg de la información. 17.1.2 Implantación de la continuidad de la seg de la información	2	2.5	2.5	2.5	0.5	0.5

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[A.29] Extorsión	1	5	5	5	1	1	5	5	5	1	1	Controlar	Correctivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	2	2.5	2.5	2.5	0.5	0.5
	[A.30] Ingeniería social (picaresca)	1	5	5	5	1	1	5	5	5	1	1	Controlar	Preventivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	3	1.7	1.7	1.7	0.3	0.3
	PROVEEDORES DE SOFTWAREE																				
	[E.7] Deficiencias en la organización	2	5	1	1	1	1	10	2	2	2	2	Controlar	Correctivo	5.1.1 Conjunto de políticas para la seguridad de la información 18.1.1 Protección de datos y privacidad de la información personal	3	3.3	0.7	0.7	0.7	0.7
	[E.19] Fugas de información	1	1	1	5	1	1	1	1	5	1	1	Controlar	Preventivo	5.1.1 Conjunto de políticas para la seguridad de la información. 6.1.3 Contacto con las autoridades. 18.1.1 Protección de datos y privacidad de la información personal. 7.2.2 Concienciación, educación y capacitación en seg de la información	3	0.3	0.3	1.7	0.3	0.3

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial					TRATAMIENTO DE RIESGOS	TIPO DE CONTROL	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
			D	I	C	A	T	D	I	C	A	T					D	I	C	A	T
	[E.28] Indisponibilidad del personal	1	5	1	1	1	1	5	1	1	1	1	Controlar	Preventivo	7.1.2 Términos y condiciones de contratación. 7.2.1 Responsabilidades de gestión. 7.3.1 Cese o cambio de puesto de trabajo	3	1.7	0.3	0.3	0.3	0.3
	[A.28] Indisponibilidad del personal	1	5	1	1	1	1	5	1	1	1	1	Controlar	Preventivo	17.1.1 Planificación de la continuidad de la seg de la información. 17.1.2 Implantación de la continuidad de la seg de la información	2	2.5	2.5	2.5	0.5	0.5
	[A.29] Extorsión	1	5	5	5	1	1	5	5	5	1	1	Controlar	Correctivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	2	2.5	2.5	2.5	0.5	0.5
	[A.30] Ingeniería social (picaresca)	1	5	5	5	1	1	5	5	5	1	1	Controlar	Preventivo	18.1.1 Identificación de la legislación aplicable 18.1.3 Protección de los registros de la organización 18.1.5 Regulación de los controles criptográficos	3	1.7	1.7	1.7	0.3	0.3

Anexo C. Resumen Analítico Especializado – RAE

RESUMEN ANALITICO ESPECIALIZADO – RAE

1. Título
Diseño de un Sistema de Gestión de Seguridad de la Información para el área TI de la Ese Hospital Universitario Erasmo Meoz de Cúcuta basado en la norma ISO27001:2013

2. Autor
LEAL SANDOVAL, Cherly Liliana y TARAZONA ANTELIZ, Javier Ricardo

3. Edición
Primera

4. Fecha
Diciembre de 2017

5. Palabras Claves
Seguridad, Información, Informática, SGSI, ISO27001, política, Disponibilidad, Integridad, Confidencialidad, MAGERIT, hospital.

6. Descripción.
Proyecto de grado aplicado para obtener el título de Especialista en Seguridad Informática

7. Fuentes.
12 fuentes bibliográficas

8. Contenidos.
Con base en el soporte documental de un Sistema de Gestión de Seguridad de la Información, para *realizar el diagnóstico del estado actual de la seguridad informática en la entidad aplicando la norma ISO 27001:2013*, se cuenta con las siguientes actividades:

- Recolección de información a través de la observación y entrevistas a los funcionarios involucrados.
- Consulta de la normatividad vigente aplicable a la seguridad informática y relacionada con el sector salud al cual pertenece la entidad.

- Consulta de información y selección de la metodología adecuada para realizar el análisis de riesgos
- Realización de un diagnóstico inicial del estado de la seguridad de la información en la entidad.
- Realización del inventario de activos de la información
- Identificar amenazas, vulnerabilidades, y el impacto
- Aplicación de la metodología seleccionada para desarrollar la gestión de riesgos

Para e*stablecer un modelo de Sistema de Gestión de seguridad informática, teniendo en cuenta lo establecido en la fase de planear del ciclo PDCA según lo indica la norma ISO27001:2013*, se tiene prevista la ejecución de:

- Definir el alcance del SGSI
- Documentar el establecimiento de la política de seguridad de la información y revisar si está acorde a las necesidades institucionales, estableciendo responsabilidades para la aplicación, con un alcance determinando la población, áreas, procesos para su cumplimiento.
- Realizar el Inventario de Activos de la Información
- Aplicar la metodología para la gestión de riesgos; Identificar amenazas y vulnerabilidades e impacto
- Análisis y evaluación de riesgos
- Selección de Controles y SOA, verificando controles existentes que aplican la norma 27001 mediante un checklist
- Declaración de aplicabilidad, selección de los dominios y controles de la norma para contrarrestar las amenazas encontradas.

Finalmente, con la información obtenida de las actividades anteriores se realiza el *Diseño de la propuesta de solución planificada y de mejora continua bajo la norma ISO 27001*.

9. Metodología.

Se realiza un estudio descriptivo de la seguridad informática en la ESE Hospital Universitario Erasmo Meoz, recolectando información para realizar el análisis de riesgos de los activos informáticos usando la metodología MAGERIT para luego establecer los controles recomendados de acuerdo a la norma ISO270012013.

10. Conclusiones.

Es requerido pronto y oportunamente la aplicación de un Sistema de Gestión de Seguridad de la Información para garantizar la integridad, confidencialidad y disponibilidad de la información.

MAGERIT como metodología para el Análisis de Riesgos se basa en conocer a la empresa y saber qué le puede pasar. Aquí se detallan entonces cuales son los activos, se valoran, se detectan sus amenazas, se determina el impacto que tendrían, el riesgo y la selección de salvaguardas; después de este análisis se evidencia que los activos más importantes en la organización son los de Datos e Información y los de Servicios.

Un Sistema de Gestión de Seguridad de la Información (SGSI), se constituye en una excelente alternativa para contribuir efectivamente a la seguridad de la información. A través del SGSI el departamento de TI podrá tener herramientas para aplicar la política, establecer controles, realizar verificación y realizar ajustes cumpliendo con el proceso de PHVA. Se traducirá en un manejo responsable y seguro de la información y los recursos tecnológicos alrededor de la misma, mediante la aplicación de la metodología.

Que una Entidad prepare su Plan de Contingencia, supone un avance a la hora de contrarrestar cualquier eventualidad, que puedan acarrear importantes pérdidas y llegado el caso no solo materiales sino personales y de información.

11. Autor del RAE.

LEAL SANDOVAL, Cherly Liliana y TARAZONA ANTELIZ, Javier Ricardo