DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA QWERTY S.A.

FILANDERSON GARCÍA GÓMEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FUSAGASUGÁ, CUNDINAMARCA
2019

DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA QWERTY S.A.

FILANDERSON GARCÍA GÓMEZ

PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

ASESOR
ALEXANDER LARRAHONDO NUÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FUSAGASUGÁ, CUNDINAMARCA
2019

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Fusagasugá. 14 de julio de 2020.

DEDICATORIA

A mis Padres, esposa y compañeros de trabajo que me han apoyo de una u otra manera durante este proceso de aprendizaje que me permite fortalecerme como profesional y ser humano.

AGRADECIMIENTOS

A Dios y mis padres que me dieron la vida, a mi esposa por su apoyo incondicional durante este tiempo de lleno de sacrificios y esfuerzos requeridos para culminar con éxito este objetivo de avanzar profesionalmente.

A todos los directores, tutores y compañeros de los diferentes cursos que integraron este posgrado, los cuales contribuyeron totalmente al éxito en este proceso de aprendizaje mediante sus realimentaciones, opiniones, punto de vista, etc., aspectos que hicieron sin duda de este proceso una gran experiencia.

CONTENIDO

pág.

LISTADO DE TABLAS

Pág.

LISTADO DE FIGURAS

Pág.

ANEXOS

GLOSARIO

ACTIVO es un bien o servicio que cumple una función específica dentro una organización.

AMENAZA acción que surge de la explotación de una vulnerabilidad presente en algún activo.

ANÁLISIS DE RIESGO Proceso que considera la dimensión de los riesgos a los que está expuesta una organización.

AUTENTICIDAD característica que garantiza el origen o la fuente de los datos enviados.

CICLO PHVA en castellano (Planificar, hacer, verificar y actuar) estrategia de mejora continua.

CONFIDENCIALIDAD garantizar que la información no esté disponible a las personas que no tengan acceso.

CONTROL mecanismo que reduce el riesgo sobre un activo o un proceso específico de la organización.

DIMENSIONES DE SEGURIDAD valores de medición de activos que puedan afectar los pilares de la información.

DISPONIBILIDAD garantizar que la información esté disponible en el momento que se necesite.

EVALUACIÓN DEL RIESGO valores que se determinan para establecer el impacto de este.

GESTIÓN DEL RIESGO Actividades enfocadas en eliminar o controlar el riesgo encontrado.

IMPACTO Consecuencia que recae sobre un activo.

INFRAESTRUCTURA medios técnicos para el desarrollo de las actividades propias de la organización.

INTEGRIDAD proceso por el cual se busca garantizar que algo no ha sido alterado u modificado.

ISO 27001 norma que busca implementar los pilares de la seguridad de la información.
MAGERIT Metodología de análisis y gestión de riesgos de los sistemas de información.

NO REPUDIO participación de las partes en la comunicación garantizando el envío del mensaje sin negar que es el emisor de este.

POLÍTICA DE SEGURIDAD normas y protocolos que velan por la seguridad de la información.

RIESGO estado en el que se puede encontrar un activo después de una amenaza.

SGSI sistema de gestión de seguridad de la información.

SISTEMAS DE INFORMACIÓN grupo de componentes informáticos que recolectan, almacenan y procesan los datos.

TRAZABILIDAD asegurar quien realizo que y en qué momento.

RESUMEN

La seguridad informática representa un gran reto para las compañías u organizaciones en general, y aún más para aquellas que hacen parte en forma directa del sector, como las compañías dedicadas a fomentar las tecnologías de información y comunicación, estas compañías llevan a cuesta una gran responsabilidad toda vez que cumplen la función de evangelizar su uso y por ende deben dar ejemplo en la aplicación de las normas, metodologías y estrategias que buscan fortalecer su avance.

QWERTY S.A como una compañía del sector tecnológico debe asumir un rol ejemplificador en lo concerniente a la seguridad de la información, dado que resulta ser el activo más importante en la mayoría de las compañías u organizaciones, por este motivo se busca que mediante el diseño de un SGSI estandarizar los procesos inmersos en la administración de la información con el objetivo de garantizar su confidencialidad, integridad y disponibilidad, teniendo claro que no existe la seguridad absoluta.

PALABRAS CLAVE: SGSI, ISO/IEC 27001:2013, DISEÑO.

ABSTRACT

Computer security represents a great challenge for companies in general, and even more so for social networks in the future, such as companies dedicated to the promotion of information and communication technologies. The function of evangelizing its use and its work. For example, in the application of standards, methodologies and strategies that seek to strengthen their progress.

QWERTY SA is a company in the technology sector that must assume an exemplary role in terms of information security, given that it is the most important asset in most of the activities of the companies, for this reason the state of an information security management system (ISMS) to standardize immersion processes in information management with the aim of guaranteeing their confidentiality, integrity and availability, taking into account that there is no absolute security.

KEYWORDS: SGSI, ISO / IEC 27001: 2013, IMPLEMENTATION.

INTRODUCCIÓN

El avance que presenta la tecnología en actualidad y su integración total con la información da un claro indicio de la importancia de este activo en todos los ambientes aplicados a los seres humanos en su diario vivir, razón por la cual no es de extrañar que en un ambiente como el laboral su valor sea priorizado frente a otros activos. Es tan importante garantizar su confidencialidad, integridad y disponibilidad que se han generado normas y estándares que buscan aplicar los mejores controles en busca de lograr dicho objetivo, aunque existe una gran cantidad de modelos, estructuras, guías, etc., cuya razón de ser obedece al cumplimiento de este objetivo, el principal referente para la implementación de un SGSI es la norma ISO/IEC 27001 en su versión 2013 a tal punto que se ha convertido en el estándar de aplicación general en todo el mundo.

Partiendo de la relación directa entre la tecnología y la administración en general de información es posible afirmar que, las organizaciones que centralizan su modelo de negocio en el sector tecnológico están obligadas a cumplir un rol ejemplarizante frente a los demás sectores en lo referente a la protección de la información. QWERTY S.A encasilla en la anterior afirmación, por lo cual debe optar sin duda por una implementación de la norma ISO/IEC 27001 en la totalidad de sus procesos.

La puesta en marcha de dicha implementación en la empresa QWERTY S.A conlleva a una serie de esfuerzos de índole organizativo, financiero, de infraestructura, etc., que sin lugar a duda presentan un enorme reto al considerar las limitaciones que pueden existir en cualquiera de estos aspectos. Aspectos que se deben afrontar con decisión para logar cumplir el objetivo.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Según el escenario planteado QWERTY S.A a pesar de pertenecer al sector tecnológico no cuenta con una política clara que le permita estandarizar los procesos inmersos en la administración de la información, lo cual representa una gran dificultad técnica y a su vez moral, si se toma en cuenta que su principal objetivo busca el desarrollo tecnológico en comunidades colombianas, este enfoque evangelizador no surtirá efecto si la compañía no refleje un compromiso real en aplicación de la norma que aporte al avance de la tecnología sirviendo como modelo para los demás.

Los problemas presentes en una compañía que no estandariza sus procesos inmersos en la administración de la información pueden ir desde lo más básico, como la falta de un sistema de control de acceso a sus instalaciones e infraestructura tecnológica a nivel hardware y software que no cumple con requisitos técnicos mínimos, hasta aspectos vitales como la no caracterización del personal y su nivel de acceso a la información.

Los riesgos presentes ante la omisión de esta política de estandarización se pueden ver reflejados en un sin número de eventos adversos que puede afectar el núcleo de la compañía, entiéndase como núcleo la información, lo cual resultaría devastador para su modelo de negocio en todos los niveles.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo diseñar de un SGSI que permita estandarizar los procesos inmersos en la administración de la información en la empresa QWERTY S.A.?

2 JUSTIFICACIÓN

Todos los actores que integran los procesos de las tecnologías de información y comunicación conocen la importancia de establecer mecanismos y/o metodologías que aporten al fortalecimiento de seguridad en cada uno de sus componentes, aún más cuando se trata de compañías que cuyo modelo de negocio se centra en el desarrollo tecnológico. Estas entienden el valor de la información y la importancia de garantizar su confidencialidad, integridad y disponibilidad mediante la implementación de políticas, estándares, metodologías, etc., que aporten a resguardarla.

En la actualidad las compañías se enfrentan a una enorme cantidad de riesgos que tienen origines muy variados, los cuales tienden a avanzar al mismo ritmo que los desarrollos tecnológicos, los ciberdelincuentes son los primeros en actualizarse en busca de detectar nuevas vulnerabilidades que les permitan generar un beneficio particular.

Partiendo de la inexistencia de una seguridad absoluta, se deben aumentar los esfuerzos por disminuir las causales de riesgos y/o posibles vulnerabilidades que pueden existir en la compañía, es aquí donde el Sistemas de Gestión de la Seguridad de la Información toma el protagonismo teniendo en cuenta que su objetivo es precisamente la atenuación de los riesgos de seguridad de la información a los que se exponen diariamente las compañías y organizaciones y a las que puede acarrearles consecuencias negativas.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un SGSI bajo la norma ISO/IEC 27001:2013 para la compañía QWERTY S.A en busca de establecer un control sobre de los riesgos de seguridad de la información en sus procesos de administración.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar un análisis de la infraestructura tecnológica para identificar y clasificar los activos de compañía.

- Realizar un análisis evaluativo de las amenazas, vulnerabilidades y riesgos presentes en los activos de compañía.

- Definir las políticas de seguridad de la información de acuerdo con lo establecido la Norma ISO 27001:2013.

- Establecer una propuesta que contenga los controles que permitan la mitigación de los riesgos.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

El sistema de gestión de calidad busca gestionar el portafolio de servicios desde la planeación, el control y la mejora continua, integrando todos los procesos de la organización, los cuales de no estar en óptimas condiciones impactan directamente en la satisfacción del consumidor y por ende en los resultados esperados, de ahí la importancia de apostar por la mejora continua de cada uno de los procesos.

La seguridad informática busca prevenir y detectar el uso no autorizado de un sistema informático, involucrando procesos de protección contra intrusos que buscan acceder a nuestros recursos informáticos con intenciones maliciosas, en la mayoría de los casos con el objetivo de obtener un beneficio propio que genere una “ganancia”. A continuación, se representa gráficamente los procesos sugeridos para establecer un buen sistema de seguridad:

Figura 1. Procesos de Sistemas de Seguridad

Fuente: Elaboración Propia

- Asegurar: El objetivo es garantizar que como mínimo los sistemas informáticos y la información contenida en ellos este respalda, para esto existen técnicas de aseguramiento adicionales como: codificar la información, monitorizar la red, establecer cortafuegos, antivirus. Etc.
- Preparar: Establece un plan u metodología para realizar el análisis, detección, respuesta y mejorara ante las vulnerabilidades.
- Detectar: Teniendo en cuenta el plan u metodología establecido, se identifica, evalúa y prioriza el riego encontrado en la vulnerabilidad.
- Responder: Se aplican las medidas de protección concernientes, tomando como base las vulnerabilidades detectadas.
- Mejorar: Revisión continua de los procesos anteriores para fortalecer las medidas ya tomadas e identificar nuevas vulnerabilidades.

La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, toda vez que los sistemas informáticos usan la información como insumo base para la ejecución de sus procesos, razón por la cual se deben establecer mecanismos de control de seguridad que integren las cuatro áreas principales que cubre la seguridad informática:

- Confidencialidad: Sólo quien cuente con autorización accede al recurso.
- Integridad: Sólo quien cuente con autorización puede modificar los datos.
- Disponibilidad: Datos accesibles a los usuarios cuando estos lo requieran.
- Autenticación: Garantizar la identidad de los usuarios.
- No repudio: Identifica quien ejecuto la acción en sus dos variantes.

    - No repudio en origen: Es imposible que el emisor desmienta que lo remitió. La prueba la crea el propio emisor y la recibe el destinatario.
    - No repudio en destino: Es imposible que el receptor refute la recepción del mensaje debido a que el emisor tiene pruebas del envió. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

La seguridad informática y de la información ha evolucionado a la par de los avances tecnológicos que han aumentado de manera alarmante la cantidad de usuarios y datos a administrar, obligando a las compañías u organizaciones a redoblar los esfuerzos en busca garantizar la protección de estos. el SGSI cuenta con años de trabajo que se ven reflejados en una estructura robusta y una experiencia envidiable, al igual que con actualizaciones periódicas que lo convierten en la mejor opción a usar.

4.1.1 ¿Qué es un SGSI?: Un Sistema de Gestión de Seguridad de la Información consiste en establecer de forma clara las reglas de "juego" para la correcta administración de la información en una organización. También se puede definir como un conjunto de políticas de administración de la información.[1]

4.1.2 ¿Para qué sirve un SGSI?: A grandes rasgos sirve para identificar y mitigar o eliminar los riesgos que pueden llegar a afectar la información de la organización, esto mediante la aplicación de controles que integran las mejores prácticas a la hora de tratar esas vulnerabilidades de seguridad, es importante saber que se requiere de un proceso de auditoría y certificación externa para garantizar su correcta implementación.

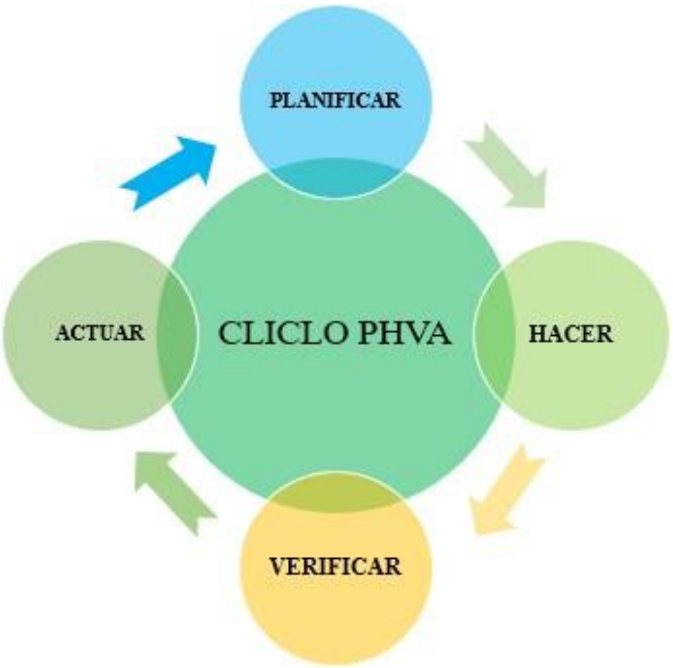
La norma ISO/IEC 27001, Fortalece los procesos inmersos en la administración de la información y de los actores que interactúan con ella, busca clasificar mediante procesos evaluativos los riesgos para lograr su mitigación o eliminación.

La implementación satisfactoria de un SGSI no solo aporta a mejorar la protección de datos, significa una diferenciación respecto al resto, debido a que mejora la competitividad y la imagen de una organización al permitir optar por una certificación de ámbito internacional, la cual cuenta de gran prestigio a nivel mundial.

[1] [1] Wikipedia, Sistema de gestión de la seguridad de la información, 2019. [En línea].

Generalmente un SGSI planeta un enfoque metodológico del Ciclo de Deming: Planificar – Hacer – Verificar – Actuar (PHVA), con el que busca fortalecer el flujo de trabajo y hacerlo continuo, esto como parte de su gran estructura la cual va más allá de lo mencionado hasta ahora.

Figura 2. Ciclo PVHA



Fuente: Elaboración Propia

El enfoque metodológico del Ciclo de Deming: Planificar – Hacer – Verificar – Actuar (PHVA), a continuación, se detalla en forma general cada proceso:

- Planificar: Se diseña el SGSI, con sus respectivas políticas, objetivos, inventario de activos, metodología de riesgos, Etc.
- Hacer: Se implementa el SGSI según el diseño aprobado con anterioridad.
- Verificar: Se evalúan los resultados con el objetivo de comprobar que lo diseñado sea lo implementado y se identifican los problemas no resueltos.
- Actuar: Se ejecutan las acciones correctivas y mejoras del SGSI.

4.2 MARCO CONCEPTUAL

La información como base fundamental de la humanidad busca entre otras cosas dar soporte a una acción que se ejecutó tomando en cuenta una previa decisión, en otras palabras, se puede decir que la información es vital para generar conocimientos que nos permitan avanzar en el desarrollo de nuestras actividades cotidianas tanto desde el ámbito laboral como personal.

Si analizamos el concepto anterior es posible deducir la importancia de la información y su fuerte incidencia en la vida de los seres humanos, toda vez que el comportamiento de un individuo se define por sus acciones, las cuales generalmente son promovidas por una decisión. Si trascendemos este concepto al ámbito laboral no debería sorprender que la información en las compañías u organizaciones se catalogue quizás como el activo más importante en su modelo de negocio.

Entender la importancia de información es vital para justificar los esfuerzos inmersos en su protección, los cuales van desde la seguridad de los recursos que conforman la infraestructura tecnológica, seguridad física, gestión de recursos humanos, la protección legal, organización, procesos, etc. Es decir que abarca todos los riesgos presentes en la compañía u organización sin importar su origen con el objetivo de establecer controles que anulen se amenaza,

Cumplir con este objetivo requiere de un sistema de gestión robusto, que cuente con una gran estructura que sea transversal y trascienda entre todas la áreas y procesos de la compañía u organización, realizar un sistema propio es una opción, pero debido a su complejidad de diseño e implementación podría tomar años para implantarse, además de no contar con la garantía de éxito, la opción recomendada para cumplir este objetivo es la implementación de un SGSI.

4.3 MARCO LEGAL

- Ley 1582 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales”.[2]

- Ley 1266 de 2008 “por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en las bases de datos personales, en especial la financiera, crediticia, comercial, deservicios y la proveniente de terceros países y se dictan otras disposiciones"[3]

- Ley 1273 de 2009 “"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "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, entre otras disposiciones".[4]

- Ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras”. [5]

- Ley estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales.” [6]

[2] [3] CONGRESO, República de Colombia, Ley 1582 de 2012. [En linea].
[3] [2] CONGRESO, República de Colombia, Ley estatutaria 1266 de 2008. [En linea].
[4] [4] CONGRESO, República de Colombia, Ley 1273 de 2009. [En linea].
[5] [5] CONGRESO, Republica de Colombia, Ley 527 de 1999. [En línea].
[6] [6] CONGRESO, Republica de Colombia, Ley estatutaria 1581 de 2012. [En línea].

5 DISEÑO METODOLÓGICO

5.1 METODOLOGÍA DE DESARROLLO

Para el desarrollo de la propuesta de diseño de un SGSI según la norma ISO/IEC 27001 en su versión 2013 para la empresa QWERTY S.A se propone una Investigación inicial en aras de explorar el estado actual de los procesos.

De acuerdo con las normas y estándares nombrados con anterioridad se obtiene una base sólida de información que permite de forma metódica aplicar las medidas de seguridad enfocadas a anular el accionar de las amenazas, esto en la norma ISO/IEC 27001 se conoce como controles.

A continuación, se detallan las etapas y actividades inmersas en marco metodológico:

- Etapa 1: Identificar y clasificar los activos de información de la empresa QWERTY S.A.
    - Analizar la documentación entregada con el propósito de identificar los activos, su cantidad, tipo, características, etc.
- Etapa 2: Llevar a cabo un análisis de riesgos basado en amenazas y vulnerabilidades.
    - Estimación de los activos según dimensiones de valoración de la metodología MAGERIT.
    - Establecer que amenazas y vulnerabilidades pueden afectar los activos.
    - Estimar los niveles de afectación del riesgo.

- Etapa 3: Indagar sobre las medidas de seguridad ya implementadas para mitigar los riesgos.

    - Analizar la documentación entregada con el propósito de consultar el estado de la infraestructura tecnológica, los procesos y procedimientos del área de tecnología de la empresa.

- Etapa 4: Definir las políticas de seguridad de la información de acuerdo con lo establecido la Norma ISO 27001:2013.

    - Establecer una propuesta que contenga los controles que permitan la mitigación de los riesgos.

También se dio uso de material bibliográfico como proyectos, tesis, trabajos en diferentes repositorios de universidades.

5.2 ENFOQUE METODOLÓGICO

El enfoque metodológico que se aplicará en este proyecto será basado en la metodología MAGERIT versión 3, donde se podrán encontrar los pasos a seguir para el análisis y gestión de riesgos, esta metodología está laborada por el “Consejo Superior de Administración Electrónica”.

Los objetivos de esta metodología son:

- Concientizar a los usuarios de las vulnerabilidades y riesgos a los que la información puede estar expuesta.
- Realizar un análisis de riesgos.

Se evidencia que en la empresa QWERTY S.A. se está haciendo un uso regular de los medios de información por esta razón se requiere diseñar un SGSI donde se aplique el paso a paso de la metodología MAGERIT versión 3 que buscara conseguir los objetivos anteriormente expuestos y así dar una solución a la empresa.

6 DESARROLLO DE LOS OBJETIVOS

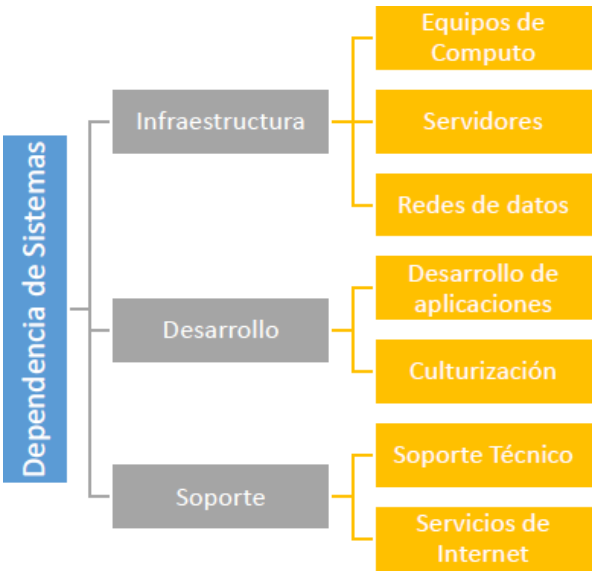
6.1 ANÁLISIS DE LA INFRAESTRUCTURA TECNOLÓGICA PARA IDENTIFICAR Y CLASIFICAR LOS ACTIVOS DE COMPAÑÍA.

6.1.1 Estado actual de la empresa

La Empresa QWERTY S.A. es una empresa del sector tecnológico que busca el desarrollo tecnológico en comunidades colombianas a través del uso de Tecnologías de Información. Actualmente cuenta con 120 colaboradores entre directivos, administrativos y operativos, quienes hacen uso de forma regular de los medios de información para consulta de datos, los cuales se usan como base para ejecución se de sus actividades diarias. Para dar respuesta a este requerimiento tecnológico, el centro de estudios cuenta con una dependencia de sistemas que brinda soporte a la infraestructura tecnológica 24/7, con el objetivo de garantizar la disponibilidad de todos los servicios inmersos en la lógica de negocio de la empresa.

6.1.2 Estructura dependencia de sistemas

Figura 3. Estructura dependencia de sistemas



Fuente: Escenario Dos (Enfoque Directivo - Administrativo)

Tabla 1. Funciones de las áreas

Área	Funciones
Infraestructura	• Soporte al acceso a la red interna y a internet • Revisión de diseños de cableado estructurado
Desarrollo	• Apoyo técnico a las dependencias de la organización del centro en desarrollo de medios eficientes para lograr actividades basadas en usos de las TIC'S.
Soporte	• Mantenimiento de computadores. • Generación de conceptos técnicos. • Realiza copias de seguridad de los sistemas de información y servidores virtuales que se encuentran en las dependencias de la empresa QWERTY S.A.

Fuente: Escenario Dos (Enfoque Directivo - Administrativo)

Tabla 2. Asistencia para directivos, administrativos y operativos.

Proceso	Descripción
Apoya el servicio de correo electrónico institucional	• Comunicación con otros miembros de la entidad • Compartir archivos • Recibir comunicados oficiales • Brindar espacio de almacenamiento ilimitado • Dar prioridad a las actividades propuestas por el desarrollo académico del programa
Apoyo en la gestión y mantenimiento de activos informáticos	• Equipos de cómputo de escritorio, móviles y servidores, televisores, video proyectores • Software operativo y aplicativo • Servicio de Internet • Todo el equipamiento que se requiera para ayudar a dar cumplimiento al objeto social.

Tabla 2. (Continuación)

Apoyo en la gestión de usuarios y contraseñas	• **Correo Electrónico** • **Sistema de gestión de calidad**
Apoyo a la dependencia de nómina y facturación	• Generación de nómina de trabajadores • Generación de recibos de pago • Creación, alimentación y custodia de Hojas de vida. • Control del seguimiento al talento humano • Generación certificados laborales y relacionados con el modelo de negocio.
Dependencia de Sistemas	• Gestión del canal de ancho de banda dedicado.

Fuente: Escenario Dos (Enfoque Directivo - Administrativo)

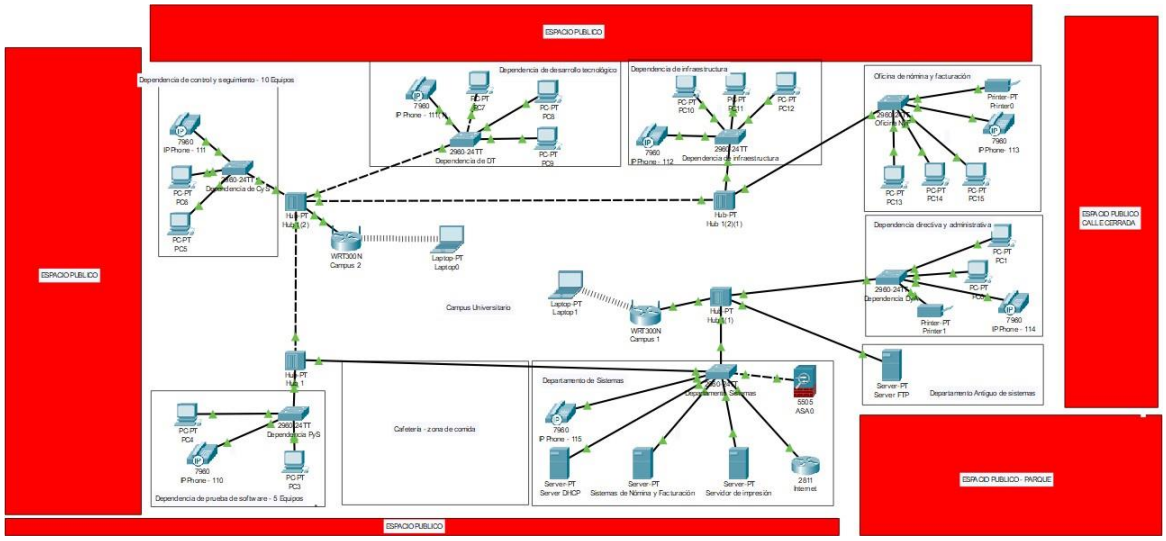
6.1.3 Distribución física de activos y de red de datos

QWERTY S.A cuenta con una serie de activos que le permiten soportan los servicios requeridos por su lógica de negocio y que permite a su personal entre otras cosas establecer una comunicación asertiva accediendo a su red de datos y servidores que almacena la información de cada una de las dependencias.

La infraestructura tecnológica de QWERTY S.A se encuentra dispuesta físicamente en sus instalaciones a excepción de unos pocos servicios que, contratado mediante terceros, tal y como ocurre con el servicio de correo electrónico corporativo y el alojamiento de la página web, entre otros.

A continuación, se presenta una estructura simulada de la distribución de los activos y red de datos.

Figura 4. Distribución de red



Fuente: Escenario Dos (Enfoque Directivo - Administrativo)

Entre los aspectos más importantes a tener cuenta de la actual distribución de activos y red de datos están:

- QWERY S.A. no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control de ingreso y egreso de los clientes internos y externos.
- Los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización optimas.
- La configuración de la red se encuentra en el mismo segmento.
- Aunque los equipos de cómputo cuentan con sistemas de antivirus actualizado, no se hace un seguimiento a sus actualizaciones o estado.
- Debido al alto flujo en la oficina de nómina y facturación, la alimentación de la información en el sistema en ocasiones la diligencia personal de prácticas de otras dependencias o contratos de aprendizaje.
- Aunque existe un Cortafuegos Cisco ASA 5505, este no cuenta con reglas implementadas para la autorización o denegación de conexiones o transmisión de datos.

6.1.4 Identificación y clasificación de los activos de información

Para la identificación de los activos de la empresa QWERTY S.A. se tomó como referencia el libro II, catálogo de elementos de la Metodología de Análisis y Gestión de Riesgos MAGERIT en su versión 3 donde determina cada activo dentro de un grado de jerarquía y de esta manera proceder a realizar una clasificación más adecuada que conlleve a ser más precisa sobre amenazas y salvaguardas que se deban desplegar en función de cada activo.

Tabla 3. Clasificación de Activos Metodología MAGERIT

Id	Tipo de activo	Detalle
[D]	Datos/Información	Ficheros, copias de respaldo, datos de configuración, registro de actividad, código fuente, código ejecutable, datos de prueba, etc.
[S]	Servicios	Función que satisface una necesidad de los usuarios.
[SW]	Software	Programas, aplicativos, desarrollos, etc.
[HW]	Hardware	Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
[COM]	Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros
[M]	Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o temporal.
[AUX]	Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[L]	Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.
[P]	Personal	Personal relacionado con los sistemas de información.

Fuente: MAGERIT Libro ll

Tabla 4. Activos QWERTY S.A.

Activo	Función	Ubicación	Cantidad
Servidor Dell tipo torre referencia PowerEdge T440	Servidor de impresión	Dependencia de sistemas	1
Impresora HP LaserJet Enterprise serie 600	Impresión de archivos del área.	Oficina de nómina y facturación	1
Impresora SMART MultiXpress M4370LX	Impresión y escaneo de archivos del área.	Dependencia directiva y administrativa	1
Servidor Dell tipo torre referencia PowerEdge T130	Servidor de archivos FTP	Oficina antigua de sistemas	1
Página Web	Alojamiento	Servidor externo	1
Servidor Dell tipo torre referencia PowerEdge T440	Servidor de nómina y Facturación.	Dependencia de sistemas.	2
Servidor Dell tipo torre referencia PowerEdge T440	Servidor DHCP	Dependencia de sistemas.	1
Equipos de cómputo tipo escritorio.	Gestión del sistema online	Dependencia de desarrollo tecnológico	3
Cortafuegos Cisco ASA 5505	Sistema de protección frente a intrusiones a la red	Dependencia de sistemas.	1

Tabla 4. (Continuación)

Equipos de cómputo sistemas operativos Windows 10 Pro	Equipos destinados para el desarrollo del objeto social	Dependencia de infraestructura	**3**
Equipos de cómputo sistemas operativos Windows 10 Pro	Equipos destinados para el desarrollo del objeto social	Dependencia de control y seguimiento	10
Equipos de Computo	Equipos destinados para el desarrollo del objeto social	Dependencia de prueba de software	5
Puntos de acceso alámbricos (Hub)	Dispositivos de red encargados de la interconexión de la red de datos.	Red de datos del centro	4
Switches cisco Catalyst 2960	Dispositivos de red encargados de la interconexión de la red de datos.	Red de datos del Centro	6
Técnicos de mantenimiento	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de cómputo.	Dependencia de Sistemas	2

Tabla 4. (Continuación)

Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP, que comunica las oficinas y departamentos del centro	Dependencias del centro	**6**
Puntos de acceso	Puntos de acceso al servicio de internet en el campus universitario.	Dependencia de sistemas	2
Ficheros	Organización de información.	Todas las dependencias	
Sistema operativo	Software requerido para administrar el hardware y demás programas de uso cotidiano.	Todas las dependencias	
Servidor de aplicaciones	Ejecutar los servicios requeridos para el correcto funcionamiento del sistema de información de registro y control.	Dependencia de sistemas.	1

Tabla 4. (Continuación)

Edificio	Resguardar todos los activos tangibles e intangibles de la organización		**1**
Centro de datos	Servir de espacio para la centralización de los equipos informáticos y de red.	Dependencia de sistemas.	1
Red de datos	Conjunto de instalaciones cableadas que permiten la comunicación entre las dependencias de la organización.	Todas las dependencias	1
Red inalámbrica	Conjunto de ondas electromagnéticas que permiten la comunicación entre las dependencias de la organización.		2
Internet	Interconectar la organización con red global.	Todas las dependencias	

Tabla 4. (Continuación)

Cable eléctrico	Conjunto de instalaciones cableadas que permiten la distribución controlada de la electricidad.	Todas las dependencias	**1**
Datos de control de acceso	Gestionar las autorizaciones de acceso a los activos.	Dependencia de sistemas.	
Correo electrónico	Permitir el intercambio de información de forma electrónica.	Servidor externo.	
Antivirus	Proteger los equipos informáticos de software malicioso.	Todas las dependencias	1

Fuente: Escenario Dos (Enfoque Directivo - Administrativo)

Como resultado del proceso de revisión de activos de la empresa se inicia con su respectiva clasificación y tipificación como se muestra en la siguiente tabla:

Tabla 5. Clasificación y tipificación de Activos QWERTY S.A.

Clasificación	Tipo	Activo
[D] DATOS	[files]	Ficheros
	[acl]	Datos de control de acceso
[S] SERVICIOS	[www]	Página Web
	[email]	Correo electrónico

Tabla 5. (Continuación)

[SW] SOFTWARE	[os]	Sistema operativo
	[app]	Servidor de aplicaciones
	[file]	Servidor de ficheros
[HW] EQUIPAMENTO INFORMÁTICO	[host]	Servidor Dell tipo torre PowerEdge T440
	[print]	Impresora HP LaserJet Enterprise serie 600
	[print]	Impresora SMART MultiXpress M4370LX
	[host]	Servidor Dell tipo torre PowerEdge T130
	[host]	Servidor Dell tipo torre PowerEdge T440
	[host]	Servidor Dell tipo torre PowerEdge T440
	[pc]	Equipos de cómputo tipo escritorio.
	[firewall]	Cortafuegos Cisco ASA 5505
	[pc]	Equipos de cómputo S.O Windows 10 Pro
	[pc]	Equipos de cómputo S.O Windows 10 Pro
	[pc]	Equipos de cómputo S.O Windows 10 Pro
	[Hub]	Puntos de acceso (Hub)
	[switch]	Switches cisco Catalyst 2960
	[ipphone]	Teléfonos IP
	[wap]	Puntos de acceso alámbricos
[COM] REDES DE COMUNICACIONES	[X25]	Red de datos
	[wifi]	Red inalámbrica
	[Internet]	Internet
[AUX] EQUIPAMENTO AUXILIAR	[wire]	Cable eléctrico
[L] INSTALACIONES	[building]	Edificio
[P] PERSONAL	[op]	Técnicos de mantenimiento

Fuente: Elaboración Propia

6.2 ANÁLISIS EVALUATIVO DE LAS AMENAZAS, VULNERABILIDADES Y RIESGOS PRESENTES EN LOS ACTIVOS DE COMPAÑÍA.

6.2.1 Análisis de gestión de riesgos

El análisis de riesgos nos permite determinar los riesgos que puede sufrir la empresa QWERTY S.A. identificando los activos de la organización y su valor operacional, a su vez estableciendo a que tipos de amenazas pueden estar expuesto los activos.

Tabla 6. Lista de referencia de amenazas

Generalidad	Detalle
[E] Errores y fallos no intencionados: Fallos no intencionales causados por las personas. Origen: Humano (accidental).	• [E.1] Errores de los usuarios: equivocaciones de las personas cuando usan los servicios, datos, etc. • [E.2] Errores del administrador: equivocaciones de personas con responsabilidades de instalación y operación. • [E.8] Difusión de software dañino: propagación inocente de virus, espías, gusanos, troyanos, bombas lógicas, etc. • [E.9] Errores de [re-]encaminamiento: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido. • [E.10] Errores de secuencia: alteración accidental del orden de los mensajes transmitidos. • [E.15] Alteración accidental de la información: Esta amenaza sólo se identifica sobre datos.

Tabla 6. (Continuación)

[E] Errores y fallos no intencionados: Fallos no intencionales causados por las personas. Origen: Humano (accidental).	• [E.18] Destrucción de información: Esta amenaza sólo se identifica sobre datos en general. • [E.19] Fugas de información: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. • [E.20] Vulnerabilidades de los programas (software): defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario. • [E.21] Errores de mantenimiento / actualización de programas (software): defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. • [E.23] Errores de mantenimiento / actualización de equipos (hardware): defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. • [E.24] Caída del sistema por agotamiento de recursos: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Tabla 6. (Continuación)

	• [E.25] Pérdida de equipos: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. • [E.28] Indisponibilidad del personal: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, Etc.
[A] Ataques intencionados: Fallos deliberados causados por las personas. Origen: Humano (deliberado).	• [A.5] Suplantación de la identidad del usuario: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. • [A.6] Abuso de privilegios de acceso: cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. • [A.7] Uso no previsto: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal. • [A.8] Difusión de software dañino: propagación intencionada de virus, espías, gusanos, troyanos, bombas lógicas, etc. • [A.9] [Re-]encaminamiento de mensajes: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido.

Tabla 6. (Continuación)

[A] Ataques intencionados: Fallos deliberados causados por las personas. Origen: Humano (deliberado).	• [A.10] Alteración de secuencia: alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos. • [A.11] Acceso no autorizado: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. • [A.12] Análisis de tráfico: el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. • [A.14] Interceptación de información (escucha): el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. • [A.15] Modificación deliberada de la información: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. • [A.18] Destrucción de información: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

Tabla 6. (Continuación)

[A] Ataques intencionados: Fallos deliberados causados por las personas. Origen: Humano (deliberado).	• [A.19] Divulgación de información: revelación de información. • [A.22] Manipulación de programas: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. • [A.24] Denegación de servicio: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. • [A.25] Robo: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. • [A.26] Ataque destructivo: vandalismo, terrorismo, acción militar, Etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. • [A.27] Ocupación enemiga: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo. • [A.28] Indisponibilidad del personal: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bloqueo de los accesos, Etc.

Tabla 6. (Continuación)

	• [A.29] Extorsión: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. • [A.30] Ingeniería social (picaresca): abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.
[I] De origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	• [I.1] Fuego: incendio: posibilidad de que el fuego acabe con los recursos del sistema. • [I.2] Daños por agua: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. • [I.*] Desastres industriales: otros desastres debidos a la actividad humana: explosiones, derrumbes, sobrecarga eléctrica, fluctuaciones eléctricas, Etc. • [I.3] Contaminación mecánica: vibraciones, polvo, suciedad, Etc. • [I.4] Contaminación electromagnética: interferencias de radio, campos magnéticos, luz ultravioleta, Etc. • [I.5] Avería de origen físico o lógico: 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. • [I.6] Corte del suministro eléctrico: cese de la alimentación de potencia.

Tabla 6. (Continuación)

	• [I.7] Condiciones inadecuadas de temperatura o humedad. • [I.8] Fallo de servicios de comunicaciones: cese de la capacidad de transmitir datos de un sitio a otro. • [I.9] Interrupción de otros servicios y suministros esenciales: otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante, Etc.
[N] Desastres naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta. Origen: Natural (accidental)	• [N.1] Fuego: incendios: posibilidad de que el fuego acabe con recursos del sistema • [N.2] Daños por agua: inundaciones: posibilidad de que el agua acabe con recursos del sistema. • [N.*] Desastres naturales: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.

Fuente: MAGERIT Libro ll

A continuación, el análisis de riesgos de cada uno de los activos de la empresa relacionados con anterioridad en donde se detalla las vulnerabilidades encontradas y las respectivas amenazas relacionadas, además de las respectivas salvaguardas recomendadas por la metodología.

Tabla 7. vulnerabilidades, amenazas y salvaguardas.

CLASIFICACIÓN	[D] DATOS
TIPO	[FILES]
ACTIVO	FICHEROS
VULNERABILIDADES	• No identificar y clasificar el nivel de confidencialidad de los ficheros. • No identificar y clasificar el personal con acceso a ficheros de contenido confidencial. • Exponer ficheros de contenido confidencial por medios no seguros.
AMENAZAS	• [E]: [E.1] [E.15] [E.18] [E.19] [E.14] • [A]: [A.15] [A.18] [A.19]
SALVAGUARDAS	• D Protección de la Información • D.A Copias de seguridad de los datos (backup) • D.I Aseguramiento de la integridad • D.C Cifrado de la información • D.DS Uso de firmas electrónicas • D.TS Uso de servicios de fechado electrónico
CLASIFICACIÓN	[D] DATOS
TIPO	[ACL]
ACTIVO	DATOS DE CONTROL DE ACCESO
VULNERABILIDADES	• No llevar control en la asignación de usuarios, roles y permisos. • No establecer una política de socialización de credenciales de acceso seguras y su importancia. • Activos sin control de acceso físico y electrónico. • Exponer ficheros de contenido confidencial por medios no seguros.
AMENAZAS	• [E]: [E.2] [E.14] • [A]: [A.5] [A.6] [A.11] [A.19]
SALVAGUARDAS	• D Protección de la Información (no divulgación) • D.I Aseguramiento de la integridad (no permitir el cambio de las credenciales) • D.C Cifrado de la información (Contraseñas) • D.DS Uso de firmas electrónicas

Tabla 7. (Continuación)

CLASIFICACIÓN	[S] SERVICIOS
TIPO	[WWW]
ACTIVO	PÁGINA WEB
VULNERABILIDADES	• Ausencia de un comité técnico interdisciplinario que establezca entre otras cosas la asignación de roles y permisos, el tipo de contenido, publicación, etc. • Equivocaciones accidentales en la publicación de contenido confidencial en un entorno público. • Gestor de contenidos desactualizado, propicio para ataques ya cocidos de esa versión que permiten el acceso y borrado de información confidencial. • No se evidencia ningún documento que garantice que el plan contratado soportará las peticiones de conexión, lo cual puede verse reflejado en una caída del servicio. • El plan indicado no contempla la ejecución de copias de seguridad, el cual es un servicio ofertado como adicional por el proveedor. • Compromiso de credenciales de acceso al ser un servicio que funciona en cualquier lugar y equipo.
AMENAZAS	• [E]: [E.1] [E.2] [E.9] [E.14] [E.19] [E.24] • [A]: [A.7] [A.9] [A.19] [A.24]
SALVAGUARDAS	• S Protección de los Servicios • S.A Aseguramiento de la disponibilidad • S.start Aceptación y puesta en operación • S.SC Se aplican perfiles de seguridad • S.op Explotación • S.CM Gestión de cambios (actualización CMS) • S.end Terminación (Descarga del contenido y borrado del servidor externo) • S.www Protección de servicios y aplicaciones web • S.dir Protección del directorio • S.dns Protección del servidor de DNS.

Tabla 7. (Continuación)

CLASIFICACIÓN	[S] SERVICIOS
TIPO	[EMAIL]
ACTIVO	CORREO ELECTRÓNICO
VULNERABILIDADES	• Almacenamiento de datos confidenciales en servidores externos y de terceros. • Exposición de información protegida ante errores involuntarios de envió a terceros no autorizados. • Limitación del recurso de almacenamiento que se reflejara en la disponibilidad del servicio a lo hora de recibir mensajes. • Envió y almacenamiento de información personal. • Compromiso de credenciales de acceso al ser un servicio que funciona en cualquier lugar y equipo.
AMENAZAS	• [E]: [E.1] [E.2] [E.9] [E.14] [E.19] [E.24] • [A]: [A.7] [A.9] [A.19]
SALVAGUARDAS	• S.email Protección del correo electrónico • S Protección de los Servicios • S.A Aseguramiento de la disponibilidad • S.start Aceptación y puesta en operación • S.SC Se aplican perfiles de seguridad • S.end Terminación • S.www Protección de servicios y aplicaciones.
CLASIFICACIÓN	[S] SERVICIOS
TIPO	[WWW]
ACTIVO	PLAN CLOUD PLUS
VULNERABILIDADES	• Almacenamiento de datos confidenciales en servidores externos y de terceros. • Procesamiento y almacenamiento de información personal o terceros. • Compromiso de credenciales de acceso al ser un servicio que funciona en cualquier lugar y equipo.
AMENAZAS	• [E]: [E.1] [E.2] [E.14] • [A]: [A.7] [A.19]
SALVAGUARDAS	• S Protección de los Servicios • S.A Aseguramiento de la disponibilidad • S.start Aceptación y puesta en operación • S.SC Se aplican perfiles de seguridad • S.op Explotación

Tabla 7. (Continuación)

	• S.CM Gestión de cambios (mejoras y sustituciones) • S.end Terminación • S.www Protección de servicios y aplicaciones.
CLASIFICACIÓN	[SW] SOFTWARE
TIPO	[OS]
ACTIVO	SISTEMA OPERATIVO
VULNERABILIDADES	• No identificación y clasificación de los usuarios. • Instalación de software malicioso de manera involuntaria. • Equipos con software desactualizado, sin política de actualización, incluidas pruebas de funcionalidad. • Utilización del activo para actividades personales.
AMENAZAS	• [E]: [E.1] [E.2] [E.8] [E.20] [E.21] • [A]: [A.5] [A.7] [A.8] [A.22]
SALVAGUARDAS	• SW Protección de las Aplicaciones Informáticas • SW.A Copias de seguridad (backup) • SW.start Puesta en producción • SW.SC Se aplican perfiles de seguridad • SW.op Explotación / Producción • SW.CM Cambios (actualización y mantenimientos) • SW.end Terminación
CLASIFICACIÓN	[SW] SOFTWARE
TIPO	[APP]
ACTIVO	SERVIDOR DE APLICACIONES (REGISTRO Y CONTROL ACADÉMICO)
VULNERABILIDADES	• No identificación y clasificación de los usuarios. • Alteración de la información en forma involuntaria. • Acceso al sistema de información por parte de terceros mediante códigos “cedidos”. • Defectos de funcionalidad del sistema de información provocados por excepciones no controladas. • Equipos con software desactualizado, sin política de actualización, incluidas pruebas de funcionalidad.

Tabla 7. (Continuación)

	• Exposición de puertos y rutas que permitan a los ataques acceder a la información protegida. • Áreas físicas con poca protección lo cual facilita el acceso a los equipos y por ende al sistema operativo, sistema de información, red, etc. • Compromiso de credenciales de acceso al ser un servicio que funciona en cualquier lugar y equipo.
AMENAZAS	• [E]: [E.1] [E.2] [E.8] [E.20] [E.21] • [A]: [A.5] [A.6] [A.7] [A.11] [A.22]
SALVAGUARDAS	• SW Protección de las Aplicaciones Informáticas • SW.A Copias de seguridad (backup) • SW.start Puesta en producción • SW.SC Se aplican perfiles de seguridad • SW.op Explotación / Producción • SW.CM Cambios. • SW.end Terminación
CLASIFICACIÓN	[SW] SOFTWARE
TIPO	[FILE]
ACTIVO	SERVIDOR DE FICHEROS FTP
VULNERABILIDADES	• No identificar y clasificar el nivel de confidencialidad de los ficheros. • No identificar y clasificar el personal con acceso a ficheros de contenido confidencial. • Exponer ficheros de contenido confidencial por medios no seguros, accesos no autorizados. • Uso de inapropiado del espacio de almacenamiento, por ejemplo, archivos personales. • Permitir el almacenamiento de software malicioso. • No realizar actualizaciones periódicas del software
AMENAZAS	• [I]: [I.5] • [E]: [E.1] [E.2] [E.9] [E.20] [E.21] • [A]: [A.7] [A.8] [A.11]
SALVAGUARDAS	• SW Protección de las Aplicaciones Informáticas • SW.A Copias de seguridad (backup) • SW.start Puesta en producción

Tabla 7. (Continuación)

	• SW.SC Se aplican perfiles de seguridad • SW.op Explotación / Producción • SW.CM Cambios (actualizar y mantener) • SW.end Terminación
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[HOST]
ACTIVO	SERVIDOR DELL TIPO POWEREDGE T440 – IMPRESIÓN.
VULNERABILIDADES	• Falta de control de acceso físico. • Uso para procesamiento de documentos personales. • Condiciones de disposición con riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de un cableado eléctrico regulado con sus respectivas UPS. • No se establece ningún mecanismo de control de temperatura. • No se evidencia cronograma de mantenimiento ni de actualización de hardware.
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios (actualizaciones y mantenimiento) • HW.end Terminación
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[PRINT]
ACTIVO	IMPRESORA HP LASERJET ENTERPRISE SERIE 600
VULNERABILIDADES	• Falta de control de acceso físico. • Riegos de afectación por desastres naturales, industriales y ataques intencionados.

Tabla 7. (Continuación)

	• Ausencia de regulador de voltaje. • Impresión de documentos personales y/o de terceros sin relación con la organización. • No se evidencia cronograma de mantenimiento ni de actualización de hardware.
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.25] • [A]: [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios (actualizaciones y mantenimiento) • HW.end Terminación • HW.print Reproducción de documentos
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[PRINT]
ACTIVO	IMPRESORA SMART MULTIXPRESS M4370LX
VULNERABILIDADES	• Falta de control de acceso físico. • Riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de regulador de voltaje. • Impresión de documentos personales y/o de terceros sin relación con la organización. • No se evidencia cronograma de mantenimiento ni de actualización de hardware.
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.25] • [A]: [A.7] [A.11] [A.25] [A.26]

Tabla 7. (Continuación)

SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios (actualizaciones y mantenimiento) • HW.end Terminación • HW.print Reproducción de documentos.
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[HOST]
ACTIVO	SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T130 - FTP
VULNERABILIDADES	• Falta de control de acceso físico. • Uso para el almacenamiento de documentos personales. • Ubicación que propicia robo, acceso no autorizado o destrucción del activo. • Condiciones de disposición con riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de un cableado eléctrico regulado con sus respectivas UPS. • No se establece ningún mecanismo de control de temperatura. • No se evidencia cronograma de mantenimiento ni de actualización de hardware.
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios (actualizaciones y mantenimiento) • HW.end Terminación.

Tabla 7. (Continuación)

CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[HOST]
ACTIVO	SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T440 – PLATAFORMA DE REGISTRO Y CONTROL.
VULNERABILIDADES	• Falta de control de acceso físico. • Uso para ejecución de procesos de personales. • Condiciones de disposición con riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de un cableado eléctrico regulado con sus respectivas UPS. • No se establece ningún mecanismo de control de temperatura. • No se evidencia cronograma de mantenimiento ni de actualización de hardware.
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios (actualizaciones y mantenimiento) • HW.end Terminación
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[HOST]
ACTIVO	SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T440 – DCHP
VULNERABILIDADES	• Falta de control de acceso físico. • Ubicación que propicia robo, acceso no autorizado o destrucción del activo. • Condiciones de disposición con riegos de afectación por desastres naturales, industriales y ataques intencionados.

Tabla 7. (Continuación)

	• Ausencia de un cableado eléctrico regulado con sus respectivas UPS. • No se establece ningún mecanismo de control de temperatura. • No se evidencia cronograma de mantenimiento ni de actualización de hardware.
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios (actualizaciones y mantenimiento) • HW.end Terminación
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[PC]
ACTIVO	EQUIPOS DE CÓMPUTO TIPO ESCRITORIO - OFICINA DE CONTABILIDAD
VULNERABILIDADES	• Falta de control de acceso físico. • Riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de regulador de voltaje. • No se evidencia cronograma de mantenimiento ni de actualización de hardware. • Ejecución de tareas personales y/o de terceros sin relación con la organización.
AMENAZAS	• N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad

Tabla 7. (Continuación)

	• HW.op Operación • HW.CM Cambios. • HW.end Terminación.
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[FIREWALL]
ACTIVO	CORTAFUEGOS CISCO ASA 5505
VULNERABILIDADES	• Falta de control de acceso físico. • Condiciones de disposición con riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de un cableado eléctrico regulado con sus respectivas UPS. • No se evidencia cronograma de mantenimiento. • Ejecución de tareas personales y/o de terceros sin relación con la organización.
AMENAZAS	• N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios • HW.end Terminación
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[PC]
ACTIVO	EQUIPOS DE CÓMPUTO TIPO ESCRITORIO - OFICINA DE REGISTRO Y CONTROL ACADÉMICO.
VULNERABILIDADES	• Falta de control de acceso físico. • Riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de regulador de voltaje. • No se evidencia cronograma de mantenimiento ni de actualización de hardware. • Ejecución de tareas personales y/o de terceros sin relación con la organización.

Tabla 7. (Continuación)

AMENAZAS	• N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios (actualizaciones y mantenimiento) • HW.end Terminación
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[PC]
ACTIVO	EQUIPOS DE CÓMPUTO TIPO ESCRITORIO - SALA DE INTERNET.
VULNERABILIDADES	• Falta de control de acceso físico. • Riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de regulador de voltaje. • No se evidencia cronograma de mantenimiento ni de actualización de hardware. • Ejecución de tareas personales y/o de terceros sin relación con la organización.
AMENAZAS	• N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios (actualizaciones y mantenimiento) • HW.end Terminación.

Tabla 7. (Continuación)

CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[PC]
ACTIVO	EQUIPOS DE CÓMPUTO TIPO ESCRITORIO - SALA DE SISTEMAS.
VULNERABILIDADES	• Falta de control de acceso físico. • Riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de regulador de voltaje. • No se evidencia cronograma de mantenimiento. • Ejecución de tareas personales y/o de terceros sin relación con la organización.
AMENAZAS	• N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios • HW.end Terminación
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[HUB]
ACTIVO	PUNTOS DE ACCESO (HUB)
VULNERABILIDADES	• Falta de control de acceso físico. • Condiciones de disposición con riegos de afectación por desastres naturales, industriales y ataques intencionados. • Ausencia de un cableado eléctrico regulado con sus respectivas UPS. • No se evidencia cronograma de mantenimiento. • Ejecución de tareas personales y/o de terceros sin relación con la organización.
AMENAZAS	• N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]

Tabla 7. (Continuación)

SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios • HW.end Terminación
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[SWITCH]
ACTIVO	SWITCHES CISCO CATALYST 2960
VULNERABILIDADES	• Falta de control de acceso físico. • Condiciones de disposición con riegos de afectación por desastres naturales e industriales. • Ausencia de un cableado eléctrico regulado con sus respectivas UPS. • No se evidencia cronograma de mantenimiento. • Ejecución de tareas personales y/o de terceros sin relación con la organización.
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios • HW.end Terminación
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[IPPHONE]
ACTIVO	TELÉFONOS IP
VULNERABILIDADES	• Falta de control de acceso físico. • Riegos de afectación por desastres naturales, industriales y ataques intencionados. • Realización de llamadas personales y/o de terceros sin relación con la organización. • No se evidencia cronograma de mantenimiento.

Tabla 7. (Continuación)

AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.25] • [A]: [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios (actualizaciones y mantenimiento) • HW.end Terminación • HW.pabx Protección de la centralita telefónica (PABX)
CLASIFICACIÓN	[HW] EQUIPAMENTO INFORMÁTICO
TIPO	[WAP]
ACTIVO	PUNTOS DE ACCESO ALÁMBRICOS
VULNERABILIDADES	• Falta de control de acceso físico. • Condiciones de disposición con riegos de afectación por desastres naturales, industriales y ataques intencionados. • No se evidencia cronograma de mantenimiento. • Ejecución de tareas personales y/o de terceros sin relación con la organización.
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] • [E]: [E.2] [E.23] [E.24] [E.25] • [A]: [A.6] [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• HW Protección de los Equipos Informáticos • HW.start Puesta en producción • HW.SC Se aplican perfiles de seguridad • HW.A Aseguramiento de la disponibilidad • HW.op Operación • HW.CM Cambios • HW.end Terminación

Tabla 7. (Continuación)

CLASIFICACIÓN	[COM] REDES DE COMUNICACIONES
TIPO	[X25]
ACTIVO	RED DE DATOS

VULNERABILIDADES	• Destrucción involuntaria o premeditada del medio físico (Hub, Switch y cable).
	• Arquitectura y configuraciones débiles frente amenazas.
	• Saturación de los medios de trasporte de datos.
	• Hardware de seguridad sin configurar adecuadamente.
	• Falta de segmentación de red que propicia:
	  ○ Accesos no autorizados
	  ○ Suplantaciones
	  ○ Abuso de privilegios
	  ○ Usos no previstos
	  ○ Interceptación de información
	  ○ Entre otros.

AMENAZAS	• [I]: [I.8] • [E]: [E.2] [E.9] [E.10] [E.24] • [A]: [A.5] [A.6] [A.7] [A.9] [A.10] [A.11] [A.12] [A.14] [A.24]
SALVAGUARDAS	• COM Protección de las Comunicaciones • COM.start Entrada en servicio • COM.SC Se aplican perfiles de seguridad • COM.A Aseguramiento de la disponibilidad • COM.aut Autenticación del canal • COM.I Protección de la integridad de los datos intercambiados • COM.op Operación • COM.CM Cambios • COM.end Terminación • COM.DS Segregación de las redes en dominios
CLASIFICACIÓN	[COM] REDES DE COMUNICACIONES
TIPO	[WIFI]
ACTIVO	RED INALÁMBRICA
VULNERABILIDADES	• Destrucción involuntaria o premeditada del medio físico (Router). • Configuraciones de seguridad débiles frente amenazas.

Tabla 7. (Continuación)

	• Saturación de los medios de trasporte de datos. • Hardware de seguridad sin configurar adecuadamente. • Falta de segmentación de red que propicia: o Accesos no autorizados o Suplantaciones o Abuso de privilegios o Usos no previstos o Interceptación de información • Entre otros.
AMENAZAS	• [I]: [I.8] • [E]: [E.2] [E.9] [E.10] [E.24] • [A]: [A.5] [A.6] [A.7] [A.9] [A.10] [A.11] [A.12] [A.14] [A.24]
SALVAGUARDAS	• COM Protección de las Comunicaciones • COM.start Entrada en servicio • COM.SC Se aplican perfiles de seguridad • COM.A Aseguramiento de la disponibilidad • COM.aut Autenticación del canal • COM.I Protección de la integridad de los datos intercambiados • COM.op Operación • COM.CM Cambios • COM.end Terminación • COM.wifi Seguridad Wireless (WiFi) • COM.DS Segregación de las redes en dominios
CLASIFICACIÓN	[COM] REDES DE COMUNICACIONES
TIPO	[INTERNET]
ACTIVO	INTERNET
VULNERABILIDADES	• Gestión de ancho de banda. • Hardware de seguridad sin configurar adecuadamente para bloqueo de conexiones entrantes y salientes.
AMENAZAS	• [I]: [I.8] • [E]: [E.2] [E.9] [E.10] [E.24] • [A]: [A.5] [A.6] [A.7] [A.9] [A.10] [A.11] [A.12] [A.14] [A.24]

Tabla 7. (Continuación)

SALVAGUARDAS	• COM Protección de las Comunicaciones • COM.start Entrada en servicio • COM.SC Se aplican perfiles de seguridad • COM.A Aseguramiento de la disponibilidad • COM.aut Autenticación del canal • COM.I Protección de la integridad de los datos intercambiados • COM.op Operación • COM.CM Cambios • COM.end Terminación
CLASIFICACIÓN	[AUX] EQUIPAMENTO AUXILIAR
TIPO	[WIRE]
ACTIVO	CABLE ELÉCTRICO
VULNERABILIDADES	• Afectación total a los demás recursos en caso de falla, no se evidencia fuente de alimentación alterna. • Ausencia de protecciones físicas que eviten afectaciones climáticas y accesos físicos malintencionados.
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] [I.3] [I.4] [I.5] [I.6] [I.7] [I.9] • [E]: [E.2] [E.25] • [A]: [A.7] [A.11] [A.25] [A.26]
SALVAGUARDAS	• AUX Elementos Auxiliares • AUX.A Aseguramiento de la disponibilidad • AUX.start Instalación • AUX.power Suministro eléctrico • AUX.wires Protección del cableado
CLASIFICACIÓN	[L] INSTALACIONES
TIPO	[BUILDING]
ACTIVO	EDIFICIO
VULNERABILIDADES	• Ausencia de seguridad perimetral personal externo. • Ausencia de controles para el acceso físico de los miembros de organización
AMENAZAS	• [N]: [N.1] [N.2] [N.*] • [I]: [I.1] [I.2] [I.*] • [A]: [A.7] [A.11]

Tabla 7. (Continuación)

SALVAGUARDAS	• AUX Elementos Auxiliares • AUX.A Aseguramiento de la disponibilidad • AUX.start Instalación • AUX.power Suministro eléctrico • AUX.wires Protección del cableado
CLASIFICACIÓN	[P] PERSONAL
TIPO	[OP]
ACTIVO	TÉCNICOS DE MANTENIMIENTO
VULNERABILIDADES	• Manual de proceso y procedimientos. • Ausencia de controles fiscos. • Ausencia de plan de disponibilidad y apoyo.
AMENAZAS	• [E]: [E.7] [E.19] [E.28] • [A]: [A.28] [A.29] [A.30]
SALVAGUARDAS	• PS Gestión del Personal • PS.AT Formación y concienciación • PS.A Aseguramiento de la disponibilidad

Fuentes: Propia y de MAGERIT, libro II - Catálogo de elementos.

6.2.2 Valoración Activos

Con la información recopilado hasta este punto es posible realizar un proceso de valoración que permita a la organización identificar el nivel de riesgo y así atacar las vulnerabilidades que al ser explotadas por una amenaza representen el mayor impacto sobre el activo y las operaciones de esta.

Tabla 8. Dimensiones de Valoración

Dimensión	Identificación	Descripción
DISPONIBILIDAD	[D]	Propiedad de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieran.
INTEGRIDAD	[I]	Propiedad consistente en que el activo de información no ha sido alterado de manera no autorizada.
CONFIDENCIALIDAD	[C]	Propiedad consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
AUTENTICIDAD	[A]	Propiedad consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
TRAZABILIDAD	[T]	Propiedad consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Fuente: Fuente: MAGERIT, libro II - Catálogo de elementos.

Una vez determinadas las dimensiones se establece la escala de valoración para evaluarlas, la cual para este escenario se realizará en forma cualitativa, simplificado la tabla original establecida por MAGERIT quedando esta de la siguiente manera:

- B = Bajo
- M = Medio
- A = Alto

A continuación, se aplicará los criterios y dimensiones de valoración de los activos identificados en la empresa QWERTY S.A.

Tabla 9. Valoración de Activos

CLASIFICACIÓN	TIPO	ACTIVO	DIMENSIONES				
			D	I	C	A	T
[D] DATOS	[FILES]	FICHEROS	A	A	A	A	A
	[ACL]	DATOS DE CONTROL DE ACCESO	A	A	A	A	A
[S] SERVICIOS	[WWW]	PÁGINA WEB	A	M	M	A	A
	[EMAIL]	CORREO ELECTRÓNICO	A	A	A	A	A
	[WWW]	PLAN CLOUD PLUS	A	A	A	A	A
[SW] SOFTWARE	[OS]	SISTEMA OPERATIVO	A	A	A	A	A
	[APP]	SERVIDOR DE APLICACIONES	A	A	A	A	A
	[FILE]	SERVIDOR DE FICHEROS	A	A	A	A	A
[HW] EQUIPAMENTO INFORMÁTICO	[HOST]	SERVIDOR DELL REFERENCIA POWEREDGE T440	A	A	A	A	A
	[PRINT]	IMPRESORA HP LASERJET ENTERPRISE SERIE 600	B	A	B	A	A
	[PRINT]	IMPRESORA SMART MULTIXPRESS M4370LX	B	A	B	A	A
	[HOST]	SERVIDOR DELL REFERENCIA POWEREDGE T130	A	A	A	A	A
	[HOST]	SERVIDOR DELL REFERENCIA POWEREDGE T440	A	A	A	A	A
	[HOST]	SERVIDOR DELL REFERENCIA POWEREDGE T440	A	A	A	A	A
	[PC]	EQUIPOS DE CÓMPUTO TIPO ESCRITORIO.	A	A	A	A	A
	[FIREWALL]	CORTAFUEGOS CISCO ASA 5505	A	A	A	A	A
	[PC]	EQUIPOS DE CÓMPUTO S.O WINDOWS 10 PRO	A	A	A	A	A
	[PC]	EQUIPOS DE CÓMPUTO S.O WINDOWS 10 PRO	A	A	A	A	A
	[PC]	EQUIPOS DE CÓMPUTO S.O WINDOWS 10 PRO	A	A	A	A	A

Tabla 9. (Continuación)

[HW] EQUIPAMENTO INFORMÁTICO	[HUB]	PUNTOS DE ACCESO (HUB)	A	A	A	A	A
	[SWITCH]	CISCO CATALYST 2960	A	A	A	A	A
	[IPPHONE]	TELÉFONOS IP	M	M	M	A	M
	[WAP]	PUNTOS DE ACCESO ALÁMBRICOS	A	A	A	A	M
[COM] REDES DE COMUNICACIONES	[X25]	RED DE DATOS	A	A	A	A	A
	[WIFI]	RED INALÁMBRICA	A	A	A	A	M
	[INTERNET]	INTERNET	A	A	A	A	A
[AUX] EQUIPAMENTO AUXILIAR	[WIRE]	CABLE ELÉCTRICO	A	A	A	A	A
[L] INSTALACIONES	[BUILDING]	EDIFICIO	M	A	A	A	A
[P] PERSONAL	[OP]	TÉCNICOS	A	A	A	A	A

Fuente: Elaboración propia.

6.2.3 Probabilidad de ocurrencia

Para este escenario la probabilidad se realizará aplicando la nomenclatura establecida por MAGERIT, pero en su versión simplificada la cual se detalla a continuación:

- B = Bajo
- M = Medio
- A = Alto

Tabla 10. Probabilidad del riesgo

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: MAGERIT Libro I Método

6.2.4 Impacto

Para este escenario la probabilidad se realizará aplicando el rango Leve, Moderado y Catastrófico, simplificado así la tabla original establecida por MAGERIT.

Tabla 11. Impacto

Nomenclatura	Categoría	Valoración
B	Leve	2
M	Moderado	3
MA	Catastrófico	4

Fuente: MAGERIT Libro III Guía Técnica

6.2.5 Informe sobre evaluación de riesgos

Tabla 12. Amenazas, probabilidad y degradación.

ACTIVO	AMENAZA	P	DIMENSIONES					I
			D	I	C	A	T	
[D] - [FILES] FICHEROS.	[E1]	4	A	A	A	A	A	MA
	[E14]	4	A	A	A	A	A	MA
	[E15]	3	A	A	A	A	A	MA
	[E18]	3	A	A	A	A	A	MA
	[E19]	4	A	A	A	A	A	MA
	[A15]	4	A	A	A	A	A	MA
	[A18]	4	A	A	A	A	A	MA
	[A19]	4	A	A	A	A	A	MA
[D] - [ACL] DATOS DE CONTROL DE ACCESO.	[E14]	4	A	A	A	A	A	MA
	[A5]	4	A	A	A	A	A	MA
	[A6]	4	A	A	A	A	A	MA
	[A11]	4	A	A	A	A	A	MA
	[A19]	4	A	A	A	A	A	MA
	[E14]	4	A	A	A	A	A	MA
[S] - [WWW] PÁGINA WEB.	[E1]	4	A	M	M	A	A	MA
	[E2]	3	A	M	M	A	A	MA
	[E9]	4	A	M	M	A	A	MA
	[E14]	4	A	M	M	A	A	MA
	[E19]	4	A	M	M	A	A	MA
	[A19]	4	A	M	M	A	A	MA
	[E24]	3	A	M	M	A	A	MA
	[A7]	4	A	M	M	A	A	MA

Tabla 12. (Continuación)

	[A9]	4	A	M	M	A	A	MA
	[A19]	4	A	M	M	A	A	MA
	[A24]	3	A	M	M	A	A	MA
[S] - [EMAIL] CORREO ELECTRÓNICO.	[E1]	4	A	A	A	A	A	MA
	[E2]	3	A	A	A	A	A	MA
	[E9]	3	A	A	A	A	A	MA
	[E14]	4	A	A	A	A	A	MA
	[E19]	4	A	A	A	A	A	MA
	[A19]	4	A	A	A	A	A	MA
	[E24]	3	A	A	A	A	A	MA
	[A7]	4	A	A	A	A	A	MA
	[A9]	4	A	A	A	A	A	MA
	[A19]	4	A	A	A	A	A	MA
	[A24]	4	A	A	A	A	A	MA
[S] - [WWW] PLAN CLOUD PLUS.	[E1]	4	A	A	A	A	A	MA
	[E2]	3	A	A	A	A	A	MA
	[E14]	4	A	A	A	A	A	MA
	[A7]	4	A	A	A	A	A	MA
	[A19]	4	A	A	A	A	A	MA
[SW] - [OS] SISTEMA OPERATIVO.	[E1]	4	A	A	A	A	A	MA
	[E2]	3	A	A	A	A	A	MA
	[E8]	4	A	A	A	A	A	MA
	[E20]	4	A	A	A	A	A	MA
	[E21]	4	A	A	A	A	A	MA
	[A5]	3	A	A	A	A	A	MA
	[A7]	4	A	A	A	A	A	MA
	[A8]	4	A	A	A	A	A	MA
	[A22]	4	A	A	A	A	A	MA
[SW] - [APP] SERVIDOR DE APLICACIONES.	[E1]	3	A	A	A	A	A	MA
	[E2]	3	A	A	A	A	A	MA
	[E8]	3	A	A	A	A	A	MA
	[E20]	4	A	A	A	A	A	MA
	[E21]	4	A	A	A	A	A	MA
	[A5]	4	A	A	A	A	A	MA
	[A6]	4	A	A	A	A	A	MA
	[A7]	4	A	A	A	A	A	MA
	[A11]	4	A	A	A	A	A	MA
	[A22]	4	A	A	A	A	A	MA
[SW] - [FILE] SERVIDOR DE FICHEROS.	[I5]	3	A	A	A	A	A	MA

Tabla 12. (Continuación)

	[E1]	3	A	A	A	A	A	MA
	[E2]	3	A	A	A	A	A	MA
	[E9]	4	A	A	A	A	A	MA
	[E20]	4	A	A	A	A	A	MA
	[E21]	4	A	A	A	A	A	MA
	[A7]	4	A	A	A	A	A	MA
	[A8]	4	A	A	A	A	A	MA
	[A11]	4	A	A	A	A	A	MA
[HW] - [HOST] SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T440 – IMPRESIÓN.	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA
	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [PRINT] IMPRESORA HP LASERJET ENTERPRISE SERIE 600	[N1]	3	B	A	B	A	A	MA
	[N2]	3	B	A	B	A	A	MA
	[N*]	3	B	A	B	A	A	MA
	[I1]	3	B	A	B	A	A	MA
	[I2]	3	B	A	B	A	A	MA
	[I*]	3	B	A	B	A	A	MA
	[I3]	3	B	A	B	A	A	MA
	[I4]	3	B	A	B	A	A	MA
	[I5]	3	B	A	B	A	A	MA
	[I6]	4	B	A	B	A	A	MA
	[I7]	3	B	A	B	A	A	MA
	[E2]	3	B	A	B	A	A	MA

Tabla 12. (Continuación)

	[E23]	4	B	A	B	A	A	MA
	[E25]	3	B	A	B	A	A	MA
	[A11]	3	B	A	B	A	A	MA
	[A11]	3	B	A	B	A	A	MA
	[A25]	4	B	A	B	A	A	MA
	[A26]	4	B	A	B	A	A	MA
[HW] - [PRINT] IMPRESORA SMART MULTIXPRESS M4370LX	[N1]	3	B	A	B	A	A	MA
	[N2]	3	B	A	B	A	A	MA
	[N*]	3	B	A	B	A	A	MA
	[I1]	3	B	A	B	A	A	MA
	[I2]	3	B	A	B	A	A	MA
	[I*]	3	B	A	B	A	A	MA
	[I3]	3	B	A	B	A	A	MA
	[I4]	3	B	A	B	A	A	MA
	[I5]	3	B	A	B	A	A	MA
	[I6]	4	B	A	B	A	A	MA
	[I7]	3	B	A	B	A	A	MA
	[E2]	3	B	A	B	A	A	MA
	[E23]	4	B	A	B	A	A	MA
	[E25]	3	B	A	B	A	A	MA
	[A6]	3	B	A	B	A	A	MA
	[A11]	3	B	A	B	A	A	MA
	[A25]	4	B	A	B	A	A	MA
	[A26]	4	B	A	B	A	A	MA
	[N1]	3	B	A	B	A	A	MA
[HW] - [HOST] SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T130	[N1]	3	A	A	A	A	A	MA
	[N2	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA

Tabla 12. (Continuación)

	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [HOST] SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T440 - RYC	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA
	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [HOST] SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T440 - DCHP	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA

Tabla 12. (Continuación)

	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [PC] EQUIPOS DE CÓMPUTO TIPO ESCRITORIO.	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA
	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [FIREWALL] CORTAFUEGOS CISCO ASA 5505	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA

Tabla 12. (Continuación)

	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [PC] EQUIPOS DE CÓMPUTO S.O WINDOWS 10 PRO	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA
	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [PC] EQUIPOS DE CÓMPUTO S.O WINDOWS 10 PRO	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA

Tabla 12. (Continuación)

	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [PC] EQUIPOS DE CÓMPUTO S.O WINDOWS 10 PRO	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA
	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [HUB] PUNTOS DE ACCESO (HUB)	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA

Tabla 12. (Continuación)

	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [SWITCH] SWITCHES CISCO CATALYST 2960	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	4	A	A	A	A	A	MA
	[I7]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E23]	4	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA
	[A6]	3	A	A	A	A	A	MA
	[A7]	3	A	A	A	A	A	MA
	[A11]	3	A	A	A	A	A	MA
	[A25]	3	A	A	A	A	A	MA
	[A26]	3	A	A	A	A	A	MA
[HW] - [IPPHONE] TELÉFONOS IP	[N1]	3	M	M	M	A	M	MA
	[N2]	3	M	M	M	A	M	MA
	[N*]	3	M	M	M	A	M	MA
	[I1]	3	M	M	M	A	M	MA
	[I2]	3	M	M	M	A	M	MA
	[I*]	3	M	M	M	A	M	MA
	[I3]	3	M	M	M	A	M	MA
	[I4]	3	M	M	M	A	M	MA
	[I5]	3	M	M	M	A	M	MA
	[I6]	4	M	M	M	A	M	MA
	[I7]	4	M	M	M	A	M	MA
	[E2]	4	M	M	M	A	M	MA
	[E23]	4	M	M	M	A	M	MA
	[E24]	4	M	M	M	A	M	MA
	[E25]	3	M	M	M	A	M	MA

Tabla 12. (Continuación)

	[A6]	3	M	M	M	A	M	MA
	[A7]	3	M	M	M	A	M	MA
	[A11]	3	M	M	M	A	M	MA
	[A25]	3	M	M	M	A	M	MA
	[A26]	3	M	M	M	A	M	MA
[HW] - [WAP] PUNTOS DE ACCESO ALÁMBRICOS	[N1]	3	A	A	A	A	M	MA
	[N2]	3	A	A	A	A	M	MA
	[N*]	3	A	A	A	A	M	MA
	[I1]	3	A	A	A	A	M	MA
	[I2]	3	A	A	A	A	M	MA
	[I*]	3	A	A	A	A	M	MA
	[I3]	3	A	A	A	A	M	MA
	[I4]	3	A	A	A	A	M	MA
	[I5]	3	A	A	A	A	M	MA
	[I6]	4	A	A	A	A	M	MA
	[I7]	4	A	A	A	A	M	MA
	[E2]	4	A	A	A	A	M	MA
	[E23]	4	A	A	A	A	M	MA
	[E24]	4	A	A	A	A	M	MA
	[E25]	3	A	A	A	A	M	MA
	[A6]	3	A	A	A	A	M	MA
	[A7]	3	A	A	A	A	M	MA
	[A11]	3	A	A	A	A	M	MA
	[A25]	3	A	A	A	A	M	MA
	[A26]	3	A	A	A	A	M	MA
[COM] - [X25] RED DE DATOS	[I8]	4	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E9]	3	A	A	A	A	A	MA
	[E10]	3	A	A	A	A	A	MA
	[E24]	4	A	A	A	A	A	MA
	[A5]	4	A	A	A	A	A	MA
	[A6]	4	A	A	A	A	A	MA
	[A7]	4	A	A	A	A	A	MA
	[A8]	4	A	A	A	A	A	MA
	[A9]	4	A	A	A	A	A	MA
	[A10]	4	A	A	A	A	A	MA
	[A11]	4	A	A	A	A	A	MA
	[A12]	4	A	A	A	A	A	MA
	[A14]	4	A	A	A	A	A	MA
	[A24]	4	A	A	A	A	A	MA

Tabla 12. (Continuación)

[COM] - [WIFI] RED INALÁMBRICA	[I8]	4	A	A	A	A	M	MA
	[E2]	4	A	A	A	A	M	MA
	[E9]	3	A	A	A	A	M	MA
	[E10]	3	A	A	A	A	M	MA
	[E24]	4	A	A	A	A	M	MA
	[A5]	4	A	A	A	A	M	MA
	[A6]	4	A	A	A	A	M	MA
	[A7]	4	A	A	A	A	M	MA
	[A8]	4	A	A	A	A	M	MA
	[A9]	4	A	A	A	A	M	MA
	[A10]	4	A	A	A	A	M	MA
	[A11]	4	A	A	A	A	M	MA
	[A12]	4	A	A	A	A	M	MA
	[A14]	4	A	A	A	A	M	MA
	[A24]	4	A	A	A	A	M	MA
[COM] - [INTERNET] INTERNET	[I8]	3	A	A	A	A	A	MA
	[E2]	4	A	A	A	A	A	MA
	[E9]	3	A	A	A	A	A	MA
	[E10]	3	A	A	A	A	A	MA
	[E24]	3	A	A	A	A	A	MA
	[A5]	4	A	A	A	A	A	MA
	[A6]	4	A	A	A	A	A	MA
	[A7]	4	A	A	A	A	A	MA
	[A8]	4	A	A	A	A	A	MA
	[A9]	4	A	A	A	A	A	MA
	[A10]	4	A	A	A	A	A	MA
	[A11]	4	A	A	A	A	A	MA
	[A12]	4	A	A	A	A	A	MA
	[A14]	4	A	A	A	A	A	MA
	[A24]	4	A	A	A	A	A	MA
[AUX] - [WIRE] CABLE ELÉCTRICO	[N1]	3	A	A	A	A	A	MA
	[N2]	3	A	A	A	A	A	MA
	[N*]	3	A	A	A	A	A	MA
	[I1]	3	A	A	A	A	A	MA
	[I2]	3	A	A	A	A	A	MA
	[I*]	3	A	A	A	A	A	MA
	[I3]	3	A	A	A	A	A	MA
	[I4]	3	A	A	A	A	A	MA
	[I5]	3	A	A	A	A	A	MA
	[I6]	3	A	A	A	A	A	MA

Tabla 12. (Continuación)

	[I7]	3	A	A	A	A	A	MA
	[I9]	3	A	A	A	A	A	MA
	[E2]	3	A	A	A	A	A	MA
	[E25]	3	A	A	A	A	A	MA
	[A7]	4	A	A	A	A	A	MA
	[A11]	4	A	A	A	A	A	MA
	[A25]	4	A	A	A	A	A	MA
	[A26]	4	A	A	A	A	A	MA
[L] - [BUILDING] EDIFICIO	[N1]	3	M	A	A	A	A	MA
	[N2]	3	M	A	A	A	A	MA
	[N*]	3	M	A	A	A	A	MA
	[I1]	3	M	A	A	A	A	MA
	[I2]	3	M	A	A	A	A	MA
	[I*]	3	M	A	A	A	A	MA
	[A7]	4	M	A	A	A	A	MA
	[A11]	4	M	A	A	A	A	MA
	[A27]	4	M	A	A	A	A	MA
[P] - [OP] TÉCNICOS DE MANTENIMIENTO	[E7]	4	A	A	A	A	A	MA
	[E19]	3	A	A	A	A	A	MA
	[E28]	3	A	A	A	A	A	MA
	[A28]	4	A	A	A	A	A	MA
	[A29]	1	A	A	A	A	A	MA
	[A30]	3	A	A	A	A	A	MA

Fuente: Propia

6.2.6 Ítems plan de tratamiento de riesgos

Tabla 13. ítems plan de tratamiento de riesgos

Código	Titulo	Descripción
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.

Tabla 13. (Continuación)

A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A6.1.2	Separación de deberes	Control: Los deberes 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
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

Tabla 13. (Continuación)

A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas 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.
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones 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.
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

Tabla 13. (Continuación)

A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
A8.1.1	Inventario de activos	Control: 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.
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.
A8.1.3	Uso aceptable de los activos	Control: 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.
A8.1.4	Devolución de activos	Control: 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.
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Tabla 13. (Continuación)

A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

Tabla 13. (Continuación)

A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A9.4.1	Restricción de acceso a la información	Control: 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.

Tabla 13. (Continuación)

A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

Tabla 13. (Continuación)

A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Tabla 13. (Continuación)

A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A11.2.9	Política de escritorio y pantalla limpios	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A12.1.2	Gestión de cambios	Control: 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.
A12.1.3	Gestión de capacidad	Control: 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.

Tabla 13. (Continuación)

A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A12.3.1	Respaldo de la información	Control: 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.
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A12.4.4	Sincronización de relojes	Control: 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.

Tabla 13. (Continuación)

A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos.
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.

Tabla 13. (Continuación)

A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A13.2.3	Mensajería electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: 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.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: 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 existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

Tabla 13. (Continuación)

A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

Tabla 13. (Continuación)

A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

Tabla 13. (Continuación)

A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.
A15.2.1	Seguimiento y revisión servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.
A16.1.1	Responsabilidades y procedimientos	Control: 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.
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

Tabla 13. (Continuación)

A16.1.4	Evaluación de eventos de seguridad de la información.	Control: 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.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A16.1.6	Aprendizaje Disponible en los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: 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.

Tabla 13. (Continuación)

A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información.
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual.
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.

Tabla 13. (Continuación)

A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación, se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: 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.
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: ISO 27002 - Controles de seguridad

Tabla 14. Plan de tratamiento de riesgo por activo.

ACTIVO	AMENAZA	P	I	CONTROL
[D] - [FILES] FICHEROS.	[E1]	4	MA	A8.3.3
	[E14]	4	MA	A8.2.1
	[E15]	3	MA	A9.4.1
	[E18]	3	MA	A8.2.3
	[E19]	4	MA	A8.2.1
	[A15]	4	MA	A9.4.1
	[A18]	4	MA	A9.4.1
	[A19]	4	MA	A13.2.4

Tabla 14. (Continuación)

[D] - [ACL] DATOS DE CONTROL DE ACCESO.	[E14]	4	MA	A6.1.1
	[A5]	4	MA	A8.3.3
	[A6]	4	MA	A9.1.1
	[A11]	4	MA	A6.1.2
	[A19]	4	MA	A6.1.2
	[E14]	4	MA	A6.1.2
[S] - [WWW] PÁGINA WEB.	[E1]	4	MA	A9.4.1
	[E2]	3	MA	A12.3.1
	[E9]	4	MA	A18.1.5
	[E14]	4	MA	A14,1,2
	[E19]	4	MA	A14,1,2
	[A19]	4	MA	A12.7.1
	[E24]	3	MA	A12.1.3
	[A7]	4	MA	A12.7.1
	[A9]	4	MA	A12.7.1
	[A19]	4	MA	A18.1.5
	[A24]	3	MA	A12.1.3
[S] - [EMAIL] CORREO ELECTRÓNICO.	[E1]	4	MA	A14.1.3
	[E2]	3	MA	A13.2.2
	[E9]	3	MA	A14.1.3
	[E14]	4	MA	A14,1,2
	[E19]	4	MA	A8.2.29
	[A19]	4	MA	A8.2.30
	[E24]	3	MA	A12.1.3
	[A7]	4	MA	A8.1.3
	[A9]	4	MA	A14,1,2
	[A19]	4	MA	A14,1,2
	[A24]	4	MA	A12.1.3
[S] - [WWW] PLAN CLOUD PLUS.	[E1]	4	MA	A14,1,2
	[E2]	3	MA	A13.2.2
	[E14]	4	MA	A14,1,2
	[A7]	4	MA	A18.1.4
	[A19]	4	MA	A14,1,2
[SW] - [OS] SISTEMA OPERATIVO.	[E1]	4	MA	A11.1.4
	[E2]	3	MA	A11.1.4
	[E8]	4	MA	A14.2.9
	[E20]	4	MA	A12.6.1
	[E21]	4	MA	A11.2.4
	[A5]	3	MA	A9.1.1
	[A7]	4	MA	A8.1.3

Tabla 14. (Continuación)

	[A8]	4	MA	A11.2.4
	[A22]	4	MA	A11.2.4
[SW] - [APP] SERVIDOR DE APLICACIONES.	[E1]	3	MA	A12.4.1
	[E2]	3	MA	A6.1.1
	[E8]	3	MA	A11.1.4
	[E20]	4	MA	A12.4.1
	[E21]	4	MA	A11.2.4
	[A5]	4	MA	A9.1.1
	[A6]	4	MA	A9.1.1
	[A7]	4	MA	A7.2.3
	[A11]	4	MA	A11.1.1
	[A22]	4	MA	A7.2.3
[SW] - [FILE] SERVIDOR DE FICHEROS.	[I5]	3	MA	A11.2.4
	[E1]	3	MA	A8.2.1
	[E2]	3	MA	A8.2.3
	[E9]	4	MA	A8.3.3
	[E20]	4	MA	A11.2.4
	[E21]	4	MA	A11.2.4
	[A7]	4	MA	A11.2.9
	[A8]	4	MA	A12.2.1
	[A11]	4	MA	A8.2.3
[HW] - [HOST] SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T440 – IMPRESIÓN.	[N1]	3	MA	A17.1.1
	[N2]	3	MA	A17.1.2
	[N*]	3	MA	A17.1.3
	[I1]	3	MA	A17.1.4
	[I2]	3	MA	A17.1.5
	[I*]	3	MA	A17.1.6
	[I3]	3	MA	A17.1.7
	[I4]	3	MA	A17.1.8
	[I5]	3	MA	A17.1.9
	[I6]	4	MA	A11.1.3
	[I7]	4	MA	A11.1.3
	[E2]	4	MA	A11.1.3
	[E23]	4	MA	A11.1.3
	[E24]	4	MA	A11.1.3
	[E25]	3	MA	A11.1.4
	[A6]	3	MA	A11.1.4
	[A7]	3	MA	A11.1.3
	[A11]	3	MA	A11.1.4
	[A25]	3	MA	A11.1.4

Tabla 14. (Continuación)

	[A26]	3	MA	A11.1.4
[HW] - [PRINT] IMPRESORA HP LASERJET ENTERPRISE SERIE 600	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4
	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.1.3
	[I7]	3	MA	A11.1.3
	[E2]	3	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E25]	3	MA	A11.1.3
	[A11]	3	MA	A11.1.3
	[A11]	3	MA	A11.1.3
	[A25]	4	MA	A11.1.3
	[A26]	4	MA	A11.1.3
[HW] - [PRINT] IMPRESORA SMART MULTIXPRESS M4370LX	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4
	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.2
	[I7]	3	MA	A11.2.2
	[E2]	3	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A11]	3	MA	A11.1.3
	[A25]	4	MA	A11.1.3
	[A26]	4	MA	A11.1.3
[HW] - [HOST] SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T130	[N1]	3	MA	A11.1.4
	[N2	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4

Tabla 14. (Continuación)

	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.3
	[I7]	4	MA	A11.2.2
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A8.1.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [HOST] SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T440 - RYC	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4
	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.3
	[I7]	4	MA	A11.2.2
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A7.2.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [HOST] SERVIDOR DELL TIPO TORRE REFERENCIA POWEREDGE T440 - DCHP	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4

Tabla 14. (Continuación)

	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.3
	[I7]	4	MA	A11.2.2
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [PC] EQUIPOS DE CÓMPUTO TIPO ESCRITORIO.	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4
	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.2
	[I7]	4	MA	A11.1.4
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [FIREWALL] CORTAFUEGOS CISCO ASA 5505	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4

Tabla 14. (Continuación)

	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.3
	[I7]	4	MA	A11.1.4
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [PC] EQUIPOS DE CÓMPUTO S.O WINDOWS 10 PRO	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4
	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.2
	[I7]	4	MA	A11.1.4
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [PC] EQUIPOS DE CÓMPUTO S.O WINDOWS 10 PRO	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4

Tabla 14. (Continuación)

	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.2
	[I7]	4	MA	A11.1.4
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [PC] EQUIPOS DE CÓMPUTO S.O WINDOWS 10 PRO	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4
	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.2
	[I7]	4	MA	A11.1.4
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [HUB] PUNTOS DE ACCESO (HUB)	[N1]	3	MA	A11.1.3
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4

Tabla 14. (Continuación)

	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.3
	[I7]	4	MA	A11.1.4
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [SWITCH] SWITCHES CISCO CATALYST 2960	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4
	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.2.3
	[I7]	4	MA	A11.1.4
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [IPPHONE] TELÉFONOS IP	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4

Tabla 14. (Continuación)

	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.1.4
	[I7]	4	MA	A11.1.4
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[HW] - [WAP] PUNTOS DE ACCESO ALÁMBRICOS	[N1]	3	MA	A11.1.4
	[N2]	3	MA	A11.1.4
	[N*]	3	MA	A11.1.4
	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.4
	[I*]	3	MA	A11.1.4
	[I3]	3	MA	A11.1.4
	[I4]	3	MA	A11.1.4
	[I5]	3	MA	A11.1.4
	[I6]	4	MA	A11.1.4
	[I7]	4	MA	A11.1.4
	[E2]	4	MA	A11.1.4
	[E23]	4	MA	A11.2.4
	[E24]	4	MA	A12.1.3
	[E25]	3	MA	A11.1.3
	[A6]	3	MA	A11.1.3
	[A7]	3	MA	A7.2.3
	[A11]	3	MA	A11.1.3
	[A25]	3	MA	A11.1.3
	[A26]	3	MA	A11.1.3
[COM] - [X25] RED DE DATOS	[I8]	4	MA	A11.2.3
	[E2]	4	MA	A13.1.3
	[E9]	3	MA	A.14.1.3

Tabla 14. (Continuación)

	[E10]	3	MA	A.14.1.3
	[E24]	4	MA	A12.1.3
	[A5]	4	MA	A13.1.1
	[A6]	4	MA	A9.1.1
	[A7]	4	MA	A9.1.1
	[A8]	4	MA	A9.1.1
	[A9]	4	MA	A9.1.2
	[A10]	4	MA	A9.1.3
	[A11]	4	MA	A9.1.4
	[A12]	4	MA	A9.1.5
	[A14]	4	MA	A9.1.6
	[A24]	4	MA	A12.1.3
[COM] - [WIFI] RED INALÁMBRICA	[I8]	4	MA	A11.2.1
	[E2]	4	MA	A13.1.3
	[E9]	3	MA	A9.1.5
	[E10]	3	MA	A9.1.6
	[E24]	4	MA	A12.1.3
	[A5]	4	MA	A9.1.6
	[A6]	4	MA	A9.1.7
	[A7]	4	MA	A9.1.1
	[A8]	4	MA	A9.1.2
	[A9]	4	MA	A9.1.7
	[A10]	4	MA	A9.1.8
	[A11]	4	MA	A9.1.9
	[A12]	4	MA	A9.1.10
	[A14]	4	MA	A9.1.11
	[A24]	4	MA	A12.1.3
[COM] - [INTERNET] INTERNET	[I8]	3	MA	A9.1.1
	[E2]	4	MA	A9.1.2
	[E9]	3	MA	A9.1.3
	[E10]	3	MA	A9.1.4
	[E24]	3	MA	A12.1.3
	[A5]	4	MA	A9.1.4
	[A6]	4	MA	A9.1.5
	[A7]	4	MA	A9.1.6
	[A8]	4	MA	A9.1.7
	[A9]	4	MA	A9.1.8
	[A10]	4	MA	A9.1.9
	[A11]	4	MA	A9.1.10
	[A12]	4	MA	A9.1.11

Tabla 14. (Continuación)

	[A14]	4	MA	A9.1.12
	[A24]	4	MA	A12.1.3
[AUX] - [WIRE] CABLE ELÉCTRICO	[N1]	3	MA	A11.2.19
	[N2]	3	MA	A11.2.19
	[N*]	3	MA	A11.2.19
	[I1]	3	MA	A11.2.5
	[I2]	3	MA	A11.2.6
	[I*]	3	MA	A11.2.7
	[I3]	3	MA	A11.2.8
	[I4]	3	MA	A11.2.9
	[I5]	3	MA	A11.2.10
	[I6]	3	MA	A11.2.11
	[I7]	3	MA	A11.2.12
	[I9]	3	MA	A11.2.13
	[E2]	3	MA	A11.2.14
	[E25]	3	MA	A11.2.15
	[A7]	4	MA	A11.2.16
	[A11]	4	MA	A11.2.17
	[A25]	4	MA	A11.2.18
	[A26]	4	MA	A11.2.19
[L] - [BUILDING] EDIFICIO	[N1]	3	MA	A11.1.1
	[N2]	3	MA	A11.1.2
	[N*]	3	MA	A11.1.3
	[I1]	3	MA	A11.1.4
	[I2]	3	MA	A11.1.5
	[I*]	3	MA	A11.1.6
	[A7]	4	MA	A11.1.2
	[A11]	4	MA	A11.1.3
	[A27]	4	MA	A11.1.4
[P] - [OP] TÉCNICOS DE MANTENIMIENTO	[E7]	4	MA	A12.1.1
	[E19]	3	MA	A11.1.3
	[E28]	3	MA	A12.1.1
	[A28]	4	MA	A12.1.1
	[A29]	1	MA	A12.1.1
	[A30]	3	MA	A12.1.1

Fuente: Elaboración propia.

DECLARACIÓN DE APLICABILIDAD

6.2.7 declaración de aplicabilidad: Legenda (Para controles seleccionados y razones de selección del control): **LR**: Requerimiento Legal, **CO**: Obligación Contractual, **BR/BP**: Requerimiento de Negocio/Mejores prácticas, **RRA**: resultado de evaluación de riesgo.

Legenda (Controles Existentes): **D**: Control implementado y Documentado, **MD**: Control Implementado sin Documentar, **RD**: Control no cumple con el estándar, **PND**: Control no implementado, NA Control no aplicable.

Tabla 15. Declaración de aplicabilidad

ISO/IEC 27001:2013 Anexo A Controles			Control	Razones para la selección del Control				Observaciones
				LR	CO	BR/BP	RRA	
Clausula	**Secuencia**	**Objetivo de Control**						
5 políticas de Seguridad	5,1	Dirección de gestión de seguridad de la información.						
	5.1.1	Políticas para la seguridad de la información	PND				X	No existe proceso o documento alguno que soporte su existencia.
	5.1.2	Revisión de las políticas para la seguridad de la información	PND				X	En consecuencia, de la ausencia del literal anterior esta tampoco se encuentra.

Tabla 15. (Continuación)

6 organización de la Seguridad de la Información	6,1	Organización Interna						
	6.1.1	Roles y responsabilidades para la seguridad de la Información	RD				X	Por lo descrito en los procesos se evidencia algún tipo implementación, pero no acorde con el estándar.
	6.1.2	Separación de Deberes	RD			X		Por lo descrito en los procesos se evidencia algún tipo implementación, pero no acorde con el estándar.
	6.1.3	Contacto con las Autoridades	PND	X				No existe proceso o documento alguno que soporte su existencia.
	6.1.4	Contacto con grupos de interés especial	PND			X		No existe proceso o documento alguno que soporte su existencia.
	6.1.5	Seguridad de la Información en la gestión de proyectos	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	6,2	Dispositivos Móviles y Teletrabajo						
	6.2.1	Política para Dispositivos Móviles	PND			X		No existe proceso o documento alguno que soporte su existencia.
	6.2.2	Teletrabajo	PND			X		No existe proceso o documento alguno que soporte su existencia.
7 seguridad del Recurso Humano	7,1	Antes de Asumir el Empleo						
	7.1.1	Selección	PND		X			No existe proceso o documento alguno que soporte su existencia.
	7.1.2	Términos y condiciones del empleo	PND		X			No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	7,2	Durante el empleo						
	7.2.1	Responsabilidades de la Dirección	PND		X			No existe proceso o documento alguno que soporte su existencia.
	7.2.2	Toma de conciencia, educación y formación en Seguridad	PND		X			No existe proceso o documento alguno que soporte su existencia.
	7.2.3	Proceso Disciplinario	PND		X			No existe proceso o documento alguno que soporte su existencia.
	7,3	Terminación y cambio de Empleo						
	7.3.1	Terminación o cambio de responsabilidades de Empleo	PND		X			No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

8 gestión de Activos	8,1	Responsabilidad por los Activos						
	8.1.1	Inventario de Activos	RD				X	Por lo descrito en los procesos se evidencia algún tipo implementación, pero no acorde con el estándar.
	8.1.2	Propiedad de los Activos	RD				X	Por lo descrito en los procesos se evidencia algún tipo implementación, pero no acorde con el estándar.
	8.1.3	Uso aceptable de los activos	PND		X			No existe proceso o documento alguno que soporte su existencia.
	8.1.4	Devolución de Activos	PND		X			No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	8,2	Clasificación de la Información						
	8.2.1	Clasificación de la Información	PND				X	No existe proceso o documento alguno que soporte su existencia.
	8.2.2	Etiquetado de la Información	PND				X	No existe proceso o documento alguno que soporte su existencia.
	8.2.3	Manejo de Activos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	8,3	Manejo de Medios						
	8.3.1	Gestión de medios removibles	PND				X	No existe proceso o documento alguno que soporte su existencia.
	8.3.2	Disposición de Medios	PND				X	No existe proceso o documento alguno que soporte su existencia.
	8.3.3	Transferencia de medios físicos	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

9 control de Acceso	9,1	Requisitos del Negocio para el control de acceso						
	9.1.1	Política del Control de Acceso	RD				X	Por lo descrito en los procesos se evidencia algún tipo implementación, pero no acorde con el estándar.
	9.1.2	Acceso a redes y servicios de red	PND				X	No existe proceso o documento alguno que soporte su existencia.
	9,2	Gestión de acceso de Usuarios						
	9.2.1	Registro y cancelación de acceso de usuarios	RD				X	Por lo descrito en los procesos se evidencia algún tipo implementación, pero no acorde con el estándar.
	9.2.2	Suministro de acceso de usuarios	RD				X	Por lo descrito en los procesos se evidencia algún tipo implementación, pero no acorde con el estándar.

Tabla 15. (Continuación)

	9.2.3	Gestión de Derechos de acceso privilegiado	RD				X	Por lo descrito en los procesos se evidencia algún tipo implementación, pero no acorde con el estándar.
	9.2.4	Gestión de la Información secreta de autenticación de los usuarios	PND				X	No existe proceso o documento alguno que soporte su existencia.
	9.2.5	Revisión de los derechos de acceso de los usuarios	PND				X	No existe proceso o documento alguno que soporte su existencia.
	9.2.6	Retiro o ajustes de los derechos de los usuarios	PND				X	No existe proceso o documento alguno que soporte su existencia.
	9,3	Responsabilidades de los usuarios						
	9.3.1	Uso de información de autenticación secreta	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	9,4	Control de acceso a sistemas y aplicaciones						
	9.4.1	Restricción de acceso a la información	PND				X	No existe proceso o documento alguno que soporte su existencia.
	9.4.2	Procesamiento de Ingreso Seguro	RD				X	Por lo descrito en los procesos se evidencia algún tipo implementación, pero no acorde con el estándar.
	9.4.3	Sistema de Gestión de contraseñas	PND				X	No existe proceso o documento alguno que soporte su existencia.
	9.4.4	Uso de programas utilitarios privilegiados	PND				X	No existe proceso o documento alguno que soporte su existencia.
	9.4.5	Control de acceso a códigos fuente de programas	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

10 criptografía	10,1	Controles Criptográficos						
	10.1.1	Política sobre el uso de controles criptográficos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	10.1.2	Gestión de llaves	PND				X	No existe proceso o documento alguno que soporte su existencia.
11 seguridad Física y del Entorno	11,1	Áreas Seguras						
	11.1.1	Perímetro de Seguridad Física	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.1.2	Controles de acceso Físicos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.1.3	Seguridad de oficinas, recintos e instalaciones	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.1.4	Protección contra amenazas externas y ambientales	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	11.1.5	Trabajo en áreas seguras	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.1.6	Áreas de despacho y carga	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11,2	Equipos						
	11.2.1	Ubicación y protección de los equipos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.2.2	Servicios de suministro	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.2.3	Seguridad del cableado	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.2.4	Mantenimiento de equipos	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	11.2.5	Retiro de activos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.2.6	Seguridad de equipos y activos fuera de las instalaciones	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.2.7	Disposición segura o reutilización de equipos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.2.8	Equipo de usuario desatendido	PND				X	No existe proceso o documento alguno que soporte su existencia.
	11.2.9	Pantalla de escritorio y pantalla limpios	PND				X	No existe proceso o documento alguno que soporte su existencia.
12 seguridad de las Operaciones	12,1	Procedimientos operacionales y responsabilidades						
	12.1.1	Procedimientos de operación documentados	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	12.1.2	Gestión de cambios	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12.1.3	Gestión de capacidad	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12,2	Protección contra códigos maliciosos						
	12.2.1	Controles contra códigos maliciosos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12,3	Copias de Respaldo						
	12.3.1	Respaldo de la Información	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	12,4	Registro y monitoreo						
	12.4.1	Registro de eventos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12.4.2	Protección de la Información de Registro	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12.4.3	Registros del administrador y del operador	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12.4.4	Sincronización de relojes	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12,5	Control de Software Operacional						
	12.5.1	Instalación de software en sistemas operativos	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	12,6	Gestión de la Vulnerabilidad Técnica						
	12.6.1	Gestión de las Vulnerabilidades técnicas	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12.6.2	Restricciones sobre la instalación de software	PND				X	No existe proceso o documento alguno que soporte su existencia.
	12,7	Consideraciones sobre auditorias de sistemas de Información						
	12.7.1	Controles de auditorías de sistemas de Información	PND				X	No existe proceso o documento alguno que soporte su existencia.
13 seguridad de las Comunicaciones	13,1	Gestión de la seguridad de las redes						
	13.1.1	Controles de Redes	PND				X	No existe proceso o documento alguno que soporte su existencia.
	13.1.2	Seguridad de los servicios de Red	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	13.1.3	Separación de las Redes	PND				X	No existe proceso o documento alguno que soporte su existencia.
	13,2	Transferencia de Información						
	13.2.1	Políticas y procedimientos de transferencia de Información	PND				X	No existe proceso o documento alguno que soporte su existencia.
	13.2.2	Acuerdos sobre transferencia de información	PND				X	No existe proceso o documento alguno que soporte su existencia.
	13.2.3	Mensajería Electrónica	PND				X	No existe proceso o documento alguno que soporte su existencia.
	13.2.4	Acuerdos de Confidencialidad o no divulgación	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

14 adquisición, Desarrollo y Mantenimiento de Sistemas	14,1	Requisitos de Seguridad de los Sistemas de Información						
	14.1.1	Análisis y especificación de requisitos de seguridad.	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14.1.2	Seguridad de servicios de aplicaciones en redes Publicas	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14.1.3	Protección de los servicios de las aplicaciones transaccionales	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14,2	Seguridad de los procesos de desarrollo y soporte						
	14.2.1	Política de desarrollo seguro	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14.2.2	Procedimientos de control de cambios en sistemas	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14.2.4	Restricción en los cambios a los paquetes de software	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14.2.5	Principios de construcción de sistemas seguros	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14.2.6	Ambiente de desarrollo seguro	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14.2.7	Desarrollo contratado externamente	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	14.2.8	Pruebas de seguridad en sistemas	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14.2.9	Pruebas de aceptación de sistemas	PND				X	No existe proceso o documento alguno que soporte su existencia.
	14,3	Datos de Prueba						
	14.3.1	Protección de los datos de prueba	PND				X	No existe proceso o documento alguno que soporte su existencia.
15 relación con los proveedores	15,1	Seguridad de la Información en la relación con los proveedores						
	15.1.1	Política de seguridad de la información para las relaciones con los proveedores	PND				X	No existe proceso o documento alguno que soporte su existencia.
	15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	15.1.3	Cadena de Suministro de tecnología de información y comunicaciones	PND				X	No existe proceso o documento alguno que soporte su existencia.
	15,2	Gestión de la prestación de servicios de proveedores						
	15.2.1	Seguimiento y revisión de los servicios de los proveedores	PND				X	No existe proceso o documento alguno que soporte su existencia.
	15.2.2	Gestión de cambios en los servicios de los proveedores	PND				X	No existe proceso o documento alguno que soporte su existencia.
16 gestión de Incidentes de Seguridad de la Información	16,1	Gestión de incidentes y mejoras en la seguridad de la Información						
	16.1.1	Responsabilidades y procedimientos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	16.1.2	Reporte de eventos de seguridad de la información	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	16.1.3	Reportes de debilidades de seguridad de la información	PND				X	No existe proceso o documento alguno que soporte su existencia.
	16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	PND				X	No existe proceso o documento alguno que soporte su existencia.
	16.1.5	Respuesta a incidentes de seguridad de la Información	PND				X	No existe proceso o documento alguno que soporte su existencia.
	16.1.6	Aprendizaje Disponible en los incidentes de seguridad de la Información	PND				X	No existe proceso o documento alguno que soporte su existencia.

Tabla 15. (Continuación)

	16.1.7	Recolección de Evidencia	PND				X	No existe proceso o documento alguno que soporte su existencia.
17 aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	17,1	Continuidad de Seguridad de la Información						
	17.1.1	Planificación de la continuidad de la seguridad.	PND				X	No existe proceso o documento alguno que soporte su existencia.
	17.1.2	Implementación de la continuidad de la Seguridad.	PND				X	No existe proceso o documento alguno que soporte su existencia.
	17.1.3	Verificación, revisión y evaluación de la continuidad de seguridad.	PND				X	No existe proceso o documento alguno que soporte su existencia.
	17,2	Redundancias						
	17.2.1	Disponibilidad de instalaciones de procesamiento de información	PND				X	No existe proceso o documento alguno que soporte su existencia.

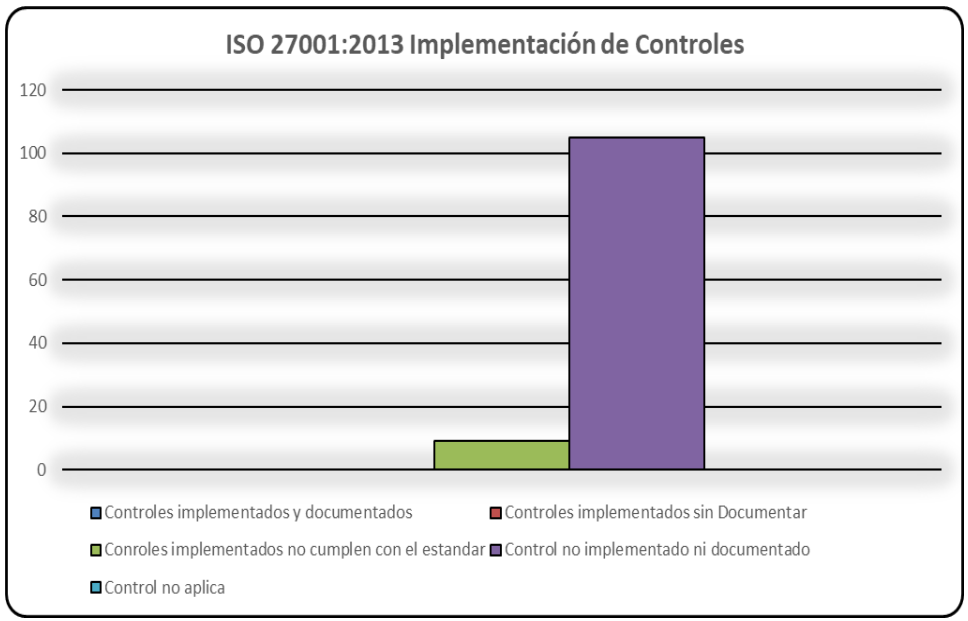
Tabla 15. (Continuación)

18 cumplimiento	18,1	Cumplimiento de requisitos legales y contractuales						
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	PND				X	No existe proceso o documento alguno que soporte su existencia.
	18.1.2	Derechos de propiedad Intelectual	PND				X	No existe proceso o documento alguno que soporte su existencia.
	18.1.3	Protección de Registros	PND				X	No existe proceso o documento alguno que soporte su existencia.
	18.1.4	Privacidad y protección de información de datos personales	PND				X	No existe proceso o documento alguno que soporte su existencia.
	18.1.5	Reglamentación de Controles Criptográficos	PND				X	No existe proceso o documento alguno que soporte su existencia.

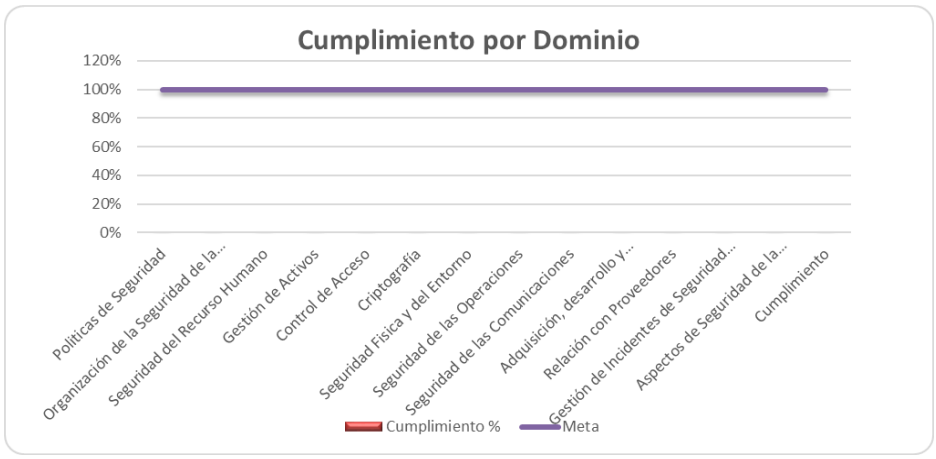
Tabla 15. (Continuación)

	18,2	Revisiones de Seguridad de la Información						
	18.2.1	Revisión Independiente de la Seguridad de la Información	PND				X	No existe proceso o documento alguno que soporte su existencia.
	18.2.2	Cumplimiento con las políticas y normas de seguridad	PND				X	No existe proceso o documento alguno que soporte su existencia.
	18.2.3	Revisión del cumplimiento técnico	PND				X	No existe proceso o documento alguno que soporte su existencia.


Cumplimiento ISO 27001 X Dominio
Cumplimiento %
Meta
Politicas de Seguridad
Organización de la Seguridad de la Información
Seguridad del Recurso Humano
Gestión de Activos
Control de Acceso
Criptografía
Seguridad Fisica y del Entorno
Seguridad de las Operaciones
Seguridad de las Comunicaciones
Adquisición, desarrollo y mantenimiento de sistemas
Relación con Proveedores
Gestión de Incidentes de Seguridad de la Información
Aspectos de Seguridad de la Información en la Gestión...
Cumplimiento
100%
80%
60%
40%
20%
0%


ISO 27001:2013 Implementación de Controles
120
100
80
60
40
20
0
Controles implementados y documentados
Controles implementados sin Documentar
Conroles implementados no cumplen con el estandar
Control no implementado ni documentado
Control no aplica


ISO 27001:2013 Implementación
0,0
0,0
0,0
7,9
92,1
Controles implementados y documentados
Controles implementados sin Documentar
Conroles implementados no cumplen con el estandar
Control no implementado ni documentado
Control no aplica


Cumplimiento por Dominio
120%
100%
80%
60%
40%
20%
0%
Politicas de Seguridad
Organización de la Seguridad de la...
Seguridad del Recurso Humano
Gestión de Activos
Control de Acceso
Criptografía
Seguridad Fisica y del Entorno
Seguridad de las Operaciones
Seguridad de las Comunicaciones
Adquisición, desarrollo y...
Relación con Proveedores
Gestión de Incidentes de Seguridad...
Aspectos de Seguridad de la...
Cumplimiento
Cumplimiento %
Meta

6.3 DEFINIR LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE ACUERDO CON LO ESTABLECIDO LA NORMA ISO 27001:2013.

6.3.1 Definición de roles y responsabilidades de seguridad

Es un proceso vital para cualquier organización dado que garantiza una estructura de control y supervisión al evitar imprecisiones por parte de los miembros en lo que ha sus tares se refiere, además de establecer una asignación directa que permite hacer seguimiento a los avances de lo proyectado o en casos de auditoria por eventos adversos.

6.3.1.1 Identificación de los responsables

La garantía de éxito de la organización está íntimamente ligada con los miembros de la organización y su capacidad de ejecutar las tareas para las cuales fueron contratados, tareas que requieren de una asignación específica que permita enfocar los esfuerzos y ser objeto de supervisión frente a los avances logrados.

6.3.1.2 Equipos de gestión

La dependencia de sistemas con el apoyo de la alta dirección será el encargado de planear, implementar y realizar seguimiento a todas las políticas y estándares de seguridad que conforma el sistema de gestión y seguridad de la información, es decir será el responsable de la administración y sostenibilidad del este.

6.3.1.3 Perfiles y responsabilidades

La alta dirección debe establecer un grupo interdisciplinario que apoye la dependencia de sistemas en la tarea de implementación del SGSI, se recomienda contar con al menos los siguientes perfiles:

Responsable de seguridad de la información para la entidad: En el escenario de no contar con profesionales o técnicos de competencias sólidas en la implementación de las políticas y estándares establecidos, se recomienda centralizar la gerencia del proyecto

en una única persona siendo esta la que mejor perfil demuestre, si es posible y se considera conveniente se puede realizar la contratación de personal calificado.

Responsabilidades Responsable de Seguridad de la información:

El profesional seleccionado previamente como responsable del proyecto debe estar en la capacidad de ejecutar las siguientes actividades:

- Guiar a los miembros de la organización en la aplicación de los mecanismos de control de seguridad establecidos en las políticas y estándares.
- Identificar las vulnerabilidades y amenazas no cubiertas durante la ejecución del análisis de riesgos.
- Generar el cronograma de tareas con sus respectivos responsables, tiempos y resultados.
- Realizar seguimiento a la ejecución del cronograma definido.
- Apoyar a todos las dependencias y miembros de la organización en el cumplimento de las tareas asignadas.
- Realizar los ajustes requeridos para garantizar el éxito de la implementación, estos deben ser consultados con la alta dirección para su respectiva aprobación.
- Monitorear la calidad de la implementación de los controles y mecanismo de seguridad garantizando que se cumplen los tiempos y recursos asignados.
- Supervisar el proceso de documentación del proyecto en su totalidad.
- Coordinar las reuniones de seguimiento y la actualización de los indicadores de gestión del proyecto.

A continuación de referencian los dominios y responsabilidades recomendados por el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia en guía numero 4 titulada Seguridad y privacidad de la información, los cuales se han ajustado de forma mínima con el objetivo de garantizar su aplicación en QWERTY S.A.:

Tabla 16. Responsabilidades

DOMINIO	RESPONSABILIDADES
SERVICIOS TECNOLÓGICOS	• Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la organización. • Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. • Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. • Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. • Trabajar con la dirección y dependencias de la organización en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. • Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
ESTRATEGIA TI	• Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la organización. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.

Tabla 16. (Continuación)

GOBIERNO TI	• Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
SISTEMAS DE INFORMACIÓN	• Establecer los requerimientos mínimos de seguridad que deben cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la organización. • Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información de la organización. • Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. • Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. • Trabajar con la alta dirección y dependencias de la organización en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.

Tabla 16. (Continuación)

SISTEMAS DE INFORMACIÓN	• Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. • Verificar el cumplimiento de las obligaciones legales y regulatorias de la organización relacionadas con la seguridad de la información.
USO Y APROPIACIÓN	• Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. • Supervisar los resultados del plan de formación y sensibilización establecido para la organización, con el fin de identificar oportunidades de mejora. • Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

Fuente: Guía Numero 4 – Seguridad y privacidad de la información – MINTIC, https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

Equipo del proyecto: La alta dirección debe conformar un grupo interdisciplinario que apoye el proceso de implementación mediante la facilitación de la información requerida:

- Personal de seguridad de la información.
- Un representante del área de Tecnología.
- Un representante del área Jurídica.
- Miembros, proveedores, y usuarios.

Responsabilidades del equipo del proyecto:

- Apoyar al profesional designado como responsable del proyecto.
- Dar a conocer las dudas presentes en la aplicación de la tarea asignada.
- Ayudar al profesional designado con los proveedores TI.
- Asistir a las convocatorias en general que se realicen durante y después de implementación del proyecto.
- Cualquier otra responsabilidad que el profesional designado como responsable del proyecto o la alta gerencia consideren.

Finalmente se recomienda integrar activamente la dependencia jurídica en aras de garantizar la correcta y total implementación de la normativa vigente a nivel país sobre todo en lo referente al tratamiento de datos personales.

6.3.2 Política

6.3.2.1 Responsabilidad

Es responsabilidad de la dependencia de sistemas utilizar la Política de Seguridad de la Información, como parte de sus procesos de administración, definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento

6.3.2.2 Cumplimiento

Las políticas de seguridad establecidas son de obligatorio cumplimiento por parte todos los miembros de la organización sin importar su tipo de vinculación, su incumplimiento será motivo valido para la generación de medidas disciplinarias y/o legales.

6.3.2.3 Excepciones

Las políticas que no establecen excepciones explicitas en su contenido requieren de la autorización de la alta dirección de QWERTY S.A para llevarlas a cabo, previa justificación y documentación.

6.3.2.4 Administración de las políticas

El mantenimiento de las políticas debe ser acompañado y autorizado por la alta dirección de QWERTY S.A y acompañada por la dependencia de sistemas, sí que este no es quien presenta el ajuste u actualización, el proceso requiere ser presentado con sus respectiva justificación y documentación.

6.3.3 Políticas y estándares

Generalidades: El principal objetivo de las políticas y estándares es garantizar el estado de los activos en general, con un énfasis en el aseguramiento de la información activo que resulta de gran valor estratégico y operación para la organización, razón por cual esta debe ser salvaguardada de acuerdo con los principios de confidencialidad, integridad y disponibilidad.

Esta política está orientada a mitigar las amenazas encontradas durante la implementación de la metodología de análisis y gestión de riesgos MAGERIT la cual aporta el insumo necesario para la instruir una serie de controles que permiten aplicar un plan de tratamiento de riesgo que garantice la continuidad de las operaciones de la organización.

6.3.4 Organización de seguridad

Política de la organización de seguridad: La dependencia de sistemas con el apoyo de la alta dirección de QWERTY S.A son los responsables de establecer las medidas necesarias para garantizar que los riesgos encontrados en la fase de análisis sean mitigados en forma eficiente de acuerdo con los controles establecidos por la norma.

Estándares de la Política de la organización de seguridad

- Responsabilidades para la seguridad de la información: En términos generales QWERTY S.A es el principal responsable de su información incluida aquella de terceros que hacen parte de la lógica de negocio, información que es delegada para su administración a todos los miembros de la organización partiendo desde la alta dirección hasta los cargos operativos, a los cuales se les debe instruir con dedicación la importancia de su protección frente a los diferentes riesgos.

- Contacto con autoridades y grupos de interés: La dependencia de sistemas de QWERTY S.A debe establecer canales de contacto con las autoridades y organizaciones especializadas en seguridad a fin de establecer si requieren procesos de actualización sobre las políticas y controles ya establecidos.

- Revisión independiente en seguridad de la información: QWERTY S.A debe ejecutar auditorías internas orientadas a identificar las nuevas amenazas y fortalecer las medidas ya existentes aplicando el Ciclo de Deming que permite establecer los procesos de mejora continua, todos estos procesos requieren ser informados y documentados.

- Seguridad en los Accesos por Terceros: La dependencia de sistemas de llevar a cabo el proceso de evaluación de riesgos presentes en lo referente al acceso de información confidencial por parte de terceros, este proceso requiere ser apoyado por cada una de las dependencias de la organización y el resultado de la evaluación debe quedar documentado en común acuerdo con él o los terceros.

6.3.5 Clasificación y control de activos de información

Política para la clasificación y control de activos de información: La información como el activo más importante de la organización debe ser objeto de los procesos de identificación y clasificación a fin de establecer su nivel confidencialidad, el cual requiere quedar documentado para ser incluido en los acuerdos de no divulgación, asignación de roles, permisos, etc.

Estándares de la Política de clasificación y control de activos de información.

- Responsabilidad sobre los activos: Todos los miembros QWERTY S.A contarán con los medios requeridos para la ejecución de sus labores y serán responsables de estos hasta la finalización su proceso contractual, tiempo durante el cual deben ajustarse a la política de uso aceptable.

- Metodología de clasificación de activos: El proceso se ejecutará aplicando los parámetros establecidos por la metodología de análisis y gestión de riesgos MAGERIT en su apartado de clasificación de activos.

6.3.6 Uso aceptable de los activos

Política de Uso Aceptable de los Activos y Recursos de información: Todos los miembros de QWERTY S.A incluidos los terceros con acceso a activos de la organización deben ajustarse a la política de uso aceptable con objetivo de cumplir con los controles establecidos en pro de mitigar el riesgo y optimizar sus labores diarias.

Estándares para el uso aceptable de los activos de información:

- Uso de los sistemas y equipos de cómputo: QWERTY S.A expresa de forma clara que los activos informáticos asignados a sus miembros o terceros habilitados para ello, que el uso inadecuado de los estos será penalizado mediante acciones disciplinarias y/o legales, entiéndase como inadecuado todo uso no relacionado con su labor u operaciones en beneficio de la lógica de negocio.

- Correo electrónico: QWERTY S.A mediante la dependencia de sistemas debe suministrar a cada uno de los miembros de la organización que lo requiera, una cuenta de correo corporativo para la ejecución de las tareas propias del cargo, la solicitud de creación debe presentarse con anticipación y de forma escrita por el líder de la dependencia.

  La cuenta asignada puede ser inactivada en los casos que se incumplan con las políticas establecidas, por la terminación de la vinculación laboral u otros casos excepcionales que requieren de aprobación por parte de la alta dirección, cual sea la causal de la inactivación esta debe ser justificada y documentada.

  La dependencia de sistemas de instruir de forma clara y regular a los miembros de la organización sobre los riesgos de abrir correo de cuentas desconocidas o con asuntos sospechosos que inviten a abrir enlaces, descargar archivos o ejecutar programas de puedan contener virus o malware, generando afectación al equipo e información.

La cuenta de correo electrónico es personal e intransferible y es responsabilidad del miembro de la organización proteger sus credenciales de acceso y sesiones. Por lo anterior este se debe comprometer a:

- La suplantación u acceso no autorizado a cuentas de otros miembros de la organización será causal de acciones disciplinarias y/o legales.

- El envío de correos masivos debe ser autorizado previamente por la alta dirección y su solicitud y respectiva justificación requiere ser presentada por el escrito y con anticipación.

- La cuenta de correo electrónico está destinada exclusivamente para el intercambio de información propia de la lógica de negocio de la organización, el contenido de los mensajes debe ser apropiado y acentuado en marco de respeto y cordialidad.

- Se recomienda evitar el envío de mensajes que contengan información protegido por derechos de autor como libros, música, películas, programas, etc., omitir esta recomendación podría acarrear acciones disciplinarias y/o legales.
- Informar a la dependencia de sistemas cualquier eventualidad que afecte el correcto funcionamiento de la herramienta o genere algún tipo de sospecha.

- Navegación en Internet: El uso de Internet por parte de los miembros de la organización debe ser exclusivo para las tareas propias del cargo u otras que aporten directamente a lógica de negocio sin que estas presenten algún incumplimiento de las políticas establecidas o norma vigente, a continuación, se detallan reglas específicas de uso:

- El miembro de la organización está en la obligación evitar la visualización y descarga de contenido inapropiado como pornografía, música, películas, programas, etc.
- El ancho de banda de la organización no puede ser usado para fines personales o de terceros bajo ningún escenario que no haya sido autorizado previamente por la alta dirección de forma explícita y por escrito.
- El uso de herramientas o mecanismos que faciliten la violación de reglas de navegación como Proxy está prohibida.
- La conexión de dispositivos personales como teléfonos móviles, tabletas, equipos de cómputo portátiles, etc., está prohibida.

- Uso de herramientas que comprometen la seguridad: La manipulación de cualquiera de las herramientas de control enfocadas en garantizar el correcto funcionamiento de los siguientes procesos será causal de acciones disciplinarias y/o legales.:

  - Acceder el sistema o red.
  - Monitorear datos o tráfico.
  - Sondear, copiar, probar firewalls o herramientas de hacking.
  - Atentar contra la vulnerabilidad del sistema o redes.
  - Violar las medidas de seguridad de autenticación del sistema o red.

- Recursos compartidos: La implementación de esta práctica debe ser ejecutada exclusivamente por el personal de la dependencia de sistemas dado el nivel de riesgo que esto con lleva para garantizar la confidencialidad, integridad y disponibilidad de la información, lineamientos para su uso seguro:

  - La información para compartir debe ser identificada y clasificada.
  - Definir acciones permitidas (lectura, escritura, modificación y borrado).
  - Implementar sistemas de identificación y autenticación.

- El control de acceso debe estar ligado a nivel de confidencialidad de la información e implementar un sistema de roles y permisos.
- Centralizar en servidor de archivos el almacenamiento y gestión de los archivos compartidos.
- Solo la dependencia de sistemas con previa autorización de la alta dirección o líder de la dependencia puede ejecutar el proceso, siendo quien autoriza el responsable de la información.
- Implementar herramientas para la generación de copias de seguridad.

- Computación en nube: El almacenamiento de información corporativa en servidores o equipos externos debe ser autorizado específicamente por la alta dirección, previo concepto de la dependencia de sistemas.

- Uso equipos portátiles y dispositivos móviles: Los miembros de la organización que tengan a su cargo equipos móviles corporativos deben ceñirse a las recomendaciones establecidas que se mencionan a continuación:

    - El dispositivo debe resguardarse en lugar seguro.
    - Implementar mecanismos de autenticación seguro como contraseña, patrón huella dactilar, patrones, entre otras.
    - Uso de aplicación de antivirus y sistema de cifrado.
    - Configuración de red que evite la conexión automática a redes no seguras.

- Acceso de equipos distintos a los asignados.
    - Desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.
    - No dejar claves en ningún sistema de almacenamiento de información web.
    - Creación de contraseñas seguras, no incluir información personal como nombres, fechas de nacimiento, otros.
    - Bloqueo de sesión automática no inferior a 30 segundos frente a inactividad.

La dependencia de sistemas debe incluir a todos los dispositivos de la organización en la herramienta de control de acceso a la red (Firewall) para garantizar que solo los dispositivos autorizados pueden acceder a ella, el proceso de solicitud de registro de cada uno ellos requieren presentarse por escrito por parte del líder de la dependencia el cual será el responsable del activo y todas las tareas que se ejecuten él.

6.3.7 Tratamiento y gestión del riesgo en seguridad de la información

Política del Tratamiento y Gestión del Riesgo en Seguridad de la Información: Todos los procesos relacionados con la toma de decisiones para la implementación del plan tratamiento de riesgos deben ser consensuados entre la alta dirección y la dependencia de sistemas quien postula el mejor control, el cual requiere estar alineado con la lógica de negocio y la política de seguridad de la Información de la organización.

La priorización de los riegos estará a cargo de la alta dirección con el apoyo técnico de la dependencia de sistemas.

Estándares de la Política del Tratamiento y Gestión del Riesgo en Seguridad de la Información: Dando cumplimiento a la norma se recomienda ejecutar de forma periódica la revisión general de los controles implementación haciendo uso de la estrategia el Ciclo de Deming que permite auditar los procesos de mejora continúa encaminados a establecer los nuevos controles que se den a lugar y el fortalecimiento de los ya implementados.

Los posibles tratamientos a los riesgos identificados incluyen:

- Evitar el riesgo.
- Disminuir la probabilidad de ocurrencia.
- Disminuir el impacto.
- Transferir los riesgos.
- Retener los riesgos

6.3.8 Seguridad del personal

Política de Responsabilidad del Personal: Todas las dependencias de la organización deben reportar las novedades presentadas con relación a su personal a la dependencia de sistemas, esto con el objetivo de conservar la coordinación en los procesos, sobre todo en aquellos que tiene que ver con ingresos, traslados, delegaciones, retiros y vacaciones del personal.

Estándares de la Política de Seguridad del Personal.

- Seguridad previa a la contratación del personal: Como aspecto fundamental del proceso precontractual el aspirante a cualquier cargo de la organización debe conocer las responsabilidades sobre seguridad de la información, incluidas todas políticas y estándares aplicados para el cargo en específico.

- Seguridad durante el contrato: Todos los miembros de la organización están obligados a asistir al proceso de inducción y reinducción en cual entre otras cosas contempla la socialización de las políticas de seguridad de información por parte de la dependencia de sistemas, proceso que se va desde la generalidad hasta lo específico del cargo, el proceso requiere ser certificado.

- Finalización o cambio de puesto: Todos los miembros de QWERTY S.A están obligados a firmar un acuerdo de confidencialidad especifico según la dependencia y cargo que estará vigente por el tiempo que considere necesario.

  El retiro de personal debe estar acompañado y certificado por el líder de la dependencia con el objetivo de garantizar que cumple con la devolución de los activos asignados.

6.3.9 Seguridad física y del entorno

Política de Seguridad Física y del Entorno: El centro de procesamiento de datos y cuarto de equipos de TIC, requieren estar en áreas protegidas físicamente contra el acceso no autorizado, daño o interferencia y deben cumplir con las políticas de seguridad física.

Estándares de la Política de Seguridad Física y del Entorno.

- Controles de acceso físico: El acceso a áreas TIC restringidas sólo se debe permitir para:
    - Desarrollo de operaciones tecnológicas.
    - Tareas de aseo (monitoreado por personal de la dependencia de sistemas).
    - Pruebas de equipos.
    - Almacenamiento de equipos.
    - Implementación o mantenimiento de los controles ambientales.

- Escritorio limpio: Se recomienda a los miembros de la organización no exponer información confidencial en espacios de fácil acceso físico o visual, esto tanto para escenarios físicos como virtuales, por cual las archivos físicos confidenciales deben estar bajo llave en archiveros o similares, en escenarios virtuales se recomienda no tener archivos en el escritorio o abierto cuando no se encuentran en la estación de trabajo, se recomienda bloquear el equipo informático ya se forma manual o automática mediante el temporizador de actividad.

- Seguridad de los equipos: QWERTY S.A debe implementar un sistema de regulación de energía que como mínimo garantiza la regulación de voltaje para los equipos de las diferencias dependencias y un sistema de alimentación interrumpida para el centro de datos.

- Retiro de equipos: Cualquier retiro de un equipo informático ya sea entre dependencias o fuera de la organización está obligado a ser documentado y autorizado por el responsable del activo, además de un visto bueno de la alta dirección y la dependencia de sistemas cuando este retiro es extramural y por varios días, el documento debe contener como mínimo el serial del equipo, el responsable, el origen, el destino, el motivo de retiro y el tiempo.

6.3.10 Control de acceso a la información

Política de Control de Acceso a la Información: La dependencia de sistemas debe establecer las medidas de seguridad aplicables a cada uno de los activos según previa identificación y clasificación, el objetivo es instruir controles de acceso de acuerdo con el perfil del activo y así evitar pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento, etc.

El control de acceso de datos e información sensible se debe basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido.

Estándares de Política de Control de Acceso a la Información.

- Gestión de acceso a usuarios: La dependencia de sistemas con base a la identificación y clasificación previa de la información debe establecer los roles y permisos de los miembros de la organización, el proceso requiere acompañamiento las diferentes dependencias y el aval de la alta dirección.
- Registro de usuarios: Todas las dependencias de la organización están obligadas a solicitar en forma escrita a la dependencia de sistemas la creación de los nuevos miembros, incluyendo los datos básicos para su creación:

    - Tipo y Número de Identificación
    - Nombre completo
    - Cargo y Dependencia
    - Rol y Permisos.

- Responsabilidades del usuario: Todos los miembros de la organización están obligados a aplicar las medidas de seguridad socializadas durante los procesos de inducción y reinducción, se recomienda la revisión periódica de roles y permisos mediante procesos de auditoria con el propósito de verificar su correcta asignación.

- Control de acceso a la red: La dependencia de sistemas debe implementar mecanismos de control y autenticación con el fin de garantizar el acceso a la red corporativa, además de establecer perfiles generales según la dependencia y cargo.

- Control de acceso a las aplicaciones.

    - Solo el personal de la dependencia de sistemas puede instalar software en los equipos informáticos.
    - Todas las aplicaciones utilizadas por la organización en la ejecución de las tareas propias de la lógica de negocio deben implementar la autodestrucción de las sesiones después de un tiempo de inactividad.
    - Ninguna aplicación o dispositivo informático adquirido por la organización debe funcionar en producción con datos de acceso de fabrica o preestablecidos por terceros.

6.3.11 Gestión de incidentes de seguridad de la información

Política de Gestión de incidentes de Seguridad de la Información: Los miembros de la organización están en la obligación de reportar los eventos en donde se evidencian errores o fallas en la seguridad, sobre todo en aquellos casos en donde estas falencias pueden afectar gravemente las operaciones.

Estándares de la Política de Gestión de Incidentes de Seguridad de la Información.

- Notificación de eventos y debilidades de seguridad de la información: La dependencia de sistemas debe implementar mecanismos que faciliten el reporte de vulnerabilidades por parte de demás miembros de la organización, además de garantizar la generación de log de eventos de todos los sistemas.

    El mecanismo de permitir el registro, seguimiento y respuesta del evento reportado, de tal manera que sea posible documentar la incidencia.

- Gestión de incidentes de seguridad de la información: QWERTY S.A mediante la dependencia de sistemas debe establecer de forma clara las responsabilidades y procedimientos a ejecutar cuando se presente un evento adverso de este tipo, dado que este puede escalar al punto de requerir la recopilación de pruebas en un caso que implique medidas legales, estas pruebas están obligadas a cumplir a cabalidad con lo establecido en la norma en lo referente a levantamiento, preservación, cadena custodia, etc.

6.3.12 Gestión de seguridad para telecomunicaciones e infraestructura de TIC

Política de Gestión de Telecomunicaciones e Infraestructura de TIC: La dependencia de sistemas de QWERTY S.A debe garantizar la disponibilidad y calidad del servicio para el correcto funcionamiento de las operaciones, además de implementar mecanismos de control de seguridad como la implementación de algoritmos de cifrado para el tráfico de los datos tanto a nivel interno como externo.

Estándares de la Política de la Política de Gestión de Telecomunicaciones e Infraestructura de TIC.

- Procedimientos y responsabilidades de operación: La organización requiere establecer en forma clara los procesos y procedimientos a aplicar en la administración de la infraestructura tecnológica, apoyada en las recomendaciones de los fabricantes de los equipos, se debe establecer como mínimo los siguientes procesos y procedimientos:

    - Copias de seguridad y Verificación de las copias.
    - Administración de consolas de antivirus.
    - Administración de usuarios, roles y contraseñas.
    - Administración de acceso a los recursos y entornos de ejecución.
    - Productividad y Gestión de los recursos de TI.
    - Auditorias y gestión de logs.
    - Protección del software en general.

- Gestión del Cambio: La dependencia de sistemas está en la obligación de implementar los mecanismos de control e identificación sobre los activos TI y sus responsables, los cuales se deben documentar con al menos estos datos:

    - Responsable actual del activo.
    - Nuevo responsable del activo (si aplica).
    - Responsable de autorizar el cambio.
    - Motivo del cambio.
    - Análisis de riesgo del activo.
    - Nivel de impacto frente a amenazas.
    - Certificación del estado antes y después del cambio.

- Segregación de funciones: QWERTY S.A debe implementar un sistema de roles y permisos que además de identificar y clasificar al personal, segregue las responsabilidades con el objetivo de evitar super usuarios que acceden sin control a los diferentes procesos.

- Separación de Ambientes: El control de los entornos de ejecución es un aspecto vital para las organizaciones que integran procesos de mejora continua en sus productos de software o su administración a distancia, dado que existen riesgos asociados en los dos escenarios que pueden afectar las operaciones, por esto se sugiere separar los entornos a fin de identificar cuáles corresponde a desarrollo, pruebas o producción, siendo este último es más importante debido a que ya almacena información real.

- Planificación y Aceptación: La alta dirección de la organización con apoyo de la dependencia de sistemas y las diferentes dependencias deben proyectar los recursos encaminados al sostenimiento de la infraestructura tecnológica que permita garantizar el crecimiento de las operaciones y la organización en general.

- Protección contra el código malicioso: La dependencia de sistemas está en la obligación de garantizar la adquisición, implementación y mantenimiento de las soluciones de seguridad tipo antivirus y malware, además de llevar a cabo en forma periódica la socialización de las amenazas actuales y futuras a los miembros de toda la organización.

- Copias de seguridad: La alta dirección debe facilitar los recursos económicos y logísticos para que la dependencia de sistemas pueda establecer una estrategia de copias seguridad que integre al menos una programación local y externa de los servidores de la organización, esto su respectivo proceso de verificación y validación de copias.

- Gestión de seguridad en las redes: El responsable de la administración de la red de datos de la organización es la dependencia de sistemas el cual debe implementar las medidas de seguridad estándar como aseguramiento de puertos, cifrado de datos, configuración de controles de acceso, etc., al igual que instruir al personal sobre el correcto uso servicio, sin dejar de lado la responsabilidad que tiene el ISP mediante los acuerdos de niveles de servicio y requisitos de gestión.

- Servicios de Comercio Electrónico: La implementación de este tipo de servicios mediante los cuales se almacena información corporativa en servidores externos requiere de procesos previos de identificación y clasificación de esta, además de la revisión exhaustiva de los términos y condiciones de uso del servicio entre el proveedor y la organización.

- Monitoreo de uso del sistema: La dependencia de sistemas está obligado a implementar mecanismos de monitoreo a nivel de red y sistema de información en general los cuales se deben priorizar según los hallazgos del análisis de riesgo.

- Registros de Auditoría: Estos registros se deben crear y almacenar alienados con la norma dado el caso estos sean requeridos en algún proceso legal.

- Protección de la información de registro: La custodia de los registros de auditoria debe alinearse de igual manera con la norma dado el caso estos sean requeridos en algún proceso legal.

- Tratamiento de medios con información: La dependencia de sistemas con el apoyo de la alta dirección debe implementar e instruir mecanismos de control para los medios de almacenamiento, incluidos los medios extraíbles en los cuales se requiere aplicar métodos de cifrado certificados y procesos estándar de borrado que garanticen la no recuperación de lo allí almacenado.

- Sincronización de relojes: Todos los equipos informáticos de la organización con énfasis en los servidores deben estar correctamente configurados para obtener un fecha y hora de un servicio acreditado.

6.3.13 Gestión de seguridad para la adquisición, desarrollo y mantenimiento de sistemas

Política de Adquisición, Desarrollo y Mantenimiento de sistemas: Como se mencionó con anterioridad la dependencia de sistemas con el apoyo de las diferentes dependencias de organización está en la obligación de proyectar todos mecanismos e insumos requeridos para garantizar la seguridad en todos los activos que integran la infraestructura tecnológica.

Estándares de la Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.

- Requerimientos de seguridad de los sistemas: El estándar define que la dependencia de sistemas debe justificar y documentar las diferentes actividades que permitan aplicar las medidas de seguridad proyectadas, esto incluye los recursos y herramientas.

- Seguridad de las aplicaciones del sistema: La dependencia de sistemas haciendo uso de los lineamientos establecidos en la norma ISO/IEC 27001:2013 y su respectivo análisis de riesgos debe implementar los controles que permitan transferir, aceptar, mitigar o eliminar las amenazas detectadas sobre este tipo de activo.

- Seguridad de los sistemas de archivos: Todos los procesos de administración de los equipos informáticos incluida la administración del sistema operativo se debe centralizar en el personal de la dependencia de sistemas.

- Seguridad de los procesos de desarrollo y soporte: La asignación de acceso para el personal encargado de ejecutar este tipo de actividades debe realizarse previa identificación y clasificación de los procesos a intervenir, esto con el objetivo de garantizar que no se afecten las operaciones y que estos pueden efectuar algún cambio que comprometa la seguridad en su favor y contra de la organización.

6.3.14 Cumplimiento y normatividad legal

Política para el Cumplimiento y Normatividad Legal: QWERTY S.A esta en la obligación de ajustarse a normatividad vigente de Colombia en todo lo relacionado a la protección de datos personales y demás regímenes legales a los que la organización por su tipificación debe cumplir.

Estándares de la Política para el Cumplimiento y Normatividad Legal.

- Cumplimiento legal: La alta dirección con el apoyo de la dependencia jurídica debe garantizar que el aspecto contractual aplicado a las diferentes políticas y estándares de seguridad ajustados a la normatividad vigente del país protegiendo los intereses de la organización frente a eventos de índole legal.

- Propiedad intelectual: La alta dirección con el apoyo de la dependencia jurídica está en la obligación de garantizar que se protegen los intereses de la organización en lo que a propiedad intelectual se refiere, aplicando las cláusulas correspondientes los modelos contractuales.

- Protección de datos: Todos los miembros de la organización están obligados a aplicar las políticas y estándares encaminados a protección de los datos durante todo su ciclo de vida, bajo esta perspectiva se debe contemplar:

    - Definir los escenarios y ámbitos de gestión del activo.
    - Definición de roles, permisos y responsabilidades de los miembros de la organización con datos asignados a su cargo.
    - Establecer los mecanismos propicios para el reporte de fallas, su seguimiento y respectiva solución.
    - Implementación de la estrategia de copias de seguridad.
    - Seguimientos periódicos a la implementación de las medidas de seguridad a fin de garantizar el cumplimiento de los objetivos.

- Cumplimiento de políticas y normas de seguridad: La alta dirección debe exigir a todos las dependencias de la organización la implementación de cada una de las políticas y estándares de seguridad, al igual que su seguimiento en aras de generar una realimentación que permita establecer una mejora continua, estos seguimientos requieren ser documentados.

- Cumplimiento técnico: La dependencia de sistemas con el apoyo de la alta dirección está obligado a ejecutar auditorías periódicas que permitan identificar el estado de los mecanismos de control de seguridad aplicados para mitigar las amenazas encontradas y a su vez detectar nuevas. Estas auditorías se deben apoyar de herramientas tecnológicas que automaticen y optimicen su ejecución.

6.3.15 Política de seguridad para proveedores

6.3.15.1 Servicios asociados al tratamiento de información

Todos los proveedores de servicios que almacenen información de uso corporativo de QWERTY S.A. están en la obligación de certificar que cuenta con los mecanismos de control de seguridad que permiten garantizar la protección de los datos, los controles deben como mínimo igualar los implementados en la organización.

6.3.15.2 Autorización y entrega de información

Todos los proveedores están obligados a realizar los requerimientos de información en forma escrita con su respectiva justificación, requerimiento que los miembros de QWERTY S.A. pueden rechazar si considera que este incumple alguna de las políticas y estándares de la seguridad de la información.

6.3.15.3 Acceso físico a los activos de información y los equipos tecnológicos

El acceso físico por parte de terceros vinculados con un proveedor está sujeto a previo aviso por escrito y aprobación de alta dirección o dependencia objeto de la visita, este personal debe estar siempre acompañado de algún miembro de la organización aún más cuando se trata de áreas protegidas.

El documento escrito requiere de como mínimo los datos personales del funcionario que realiza la vista:

- Número de identificaron
- Nombre completo
- Cargo y área que visita.
- Fecha y hora
- Razón u objeto de la visita.
- Tarjeta de vinculación con el proveedor (carnet).

6.3.15.4 Acceso remoto a través de herramientas informáticas

Cualquier conexión externa a la red datos requiere de la aprobación de la alta dirección y la dependencia de sistemas a fin de garantizar que no se comprometen recursos vitales o información confidencial durante el proceso de manipulación por parte del personal externo. Todas las operaciones ejecutadas durante el proceso de conexión deberán quedar registradas de forma escrita y soportadas el log del sistema de información y/o sistema operativo.

6.3.15.5 Contratación permanente de servicios tecnológicos

Todos los proveedores de servicios que gestionen información de uso corporativo de QWERTY S.A. están obligados someterse a cláusulas de seguridad que permitan garantizar la confidencialidad, integridad y disponibilidad de esta, al igual que brindar toda la información requerida en caso de ocurrencia de un evento adverso.

6.3.15.6 Seguridad en la instalación y configuración de activos tecnológicos

Todos los proveedores que cumplan objetos relacionados con la instalación y configuración de equipos informáticos deben ceñirse a las políticas y estándares de seguridad de la organización, el proceso requiere acompañamiento de la dependencia de sistemas y su respectiva certificación de cumplimiento.

6.3.15.7 Posibilidad de inspeccionar y auditar las condiciones del servicio

Como medidas adicionales de protección QWERTY S.A. se reserva el derecho de solicitar la ejecución de auditorías independientes y visitas físicas programadas a las instalaciones del proveedor servicios con el objetivo de corroborar lo afirmado por este en cuanto al cumplimiento de las medidas de seguridad de la información.

6.3.15.8 Seguridad en el intercambio de información con proveedores

Todos los medios de intercambio de información entre la organización y los diferentes proveedores deben estar asegurados mediante la implementación de estándares y procedimientos de cifrado, validación de integridad e identidad del receptor, estos medios deben ser certificados por la dependencia de sistemas y aprobados por la alta gerencia.

6.3.15.9 Manejo de incidentes de seguridad asociados a los servicios

Todos los servicios TI asociados a proveedores deben establecer en forma clara y documentada los procedimientos a ejecutar frente a incidentes de seguridad, así como los responsables de atender el incidente.

Si el activo se encuentra en las instalaciones de la organización el proceso de revisión requiere del acompañamiento de la dependencia de sistemas, si por lo contrario el activo se encuentra fuera de las instalaciones de la organización el proveedor debe entregar un informe del incidente y las afectaciones a alta gerencia y la dependencia de sistemas el cual podrá según criterio solicitar más información.

6.3.15.10 Acuerdos de niveles de servicios y los planes de recuperación

El proveedor está obligado a indicar de forma explícita que cuenta con la capacidad de cumplir con los niveles mínimos de servicio requeridos por la organización y los tiempos de respuesta frente a fallas, adicionalmente debe indicar los planes de continuidad del servicio para los casos de las fallas prolongadas.

6.3.15.11 Monitoreo sobre los servicios tecnológicos externalizados

La dependencia de sistemas es la responsable del seguimiento y monitoreo de los servicios brindados por los diferentes proveedores, esto incluye garantizar que se mantienen los niveles de servicio requeridos, de no ser así está en la obligación informar a la alta gerencia para el respectivo proceso de notificación al proveedor.

6.3.15.12 Entrega y difusión de las políticas de seguridad a proveedores

La dependencia de sistemas está en la obligación de socializar las políticas acordadas con todos los miembros de la organización, al igual que el proveedor debe realizarlo con su personal o al menos con el asignado para ejecutar tareas en QWERTY S.A.

6.3.16 Procedimientos

6.3.16.1 Procedimientos de operación para gestión de TI

Objetivo: Instruir los mecanismos de operación de los diferentes componentes tecnológicos de la organización, aplicando las políticas y estándares seguridad definimos.

Alcance: Desde la adquisición del componente TI hasta su baja del servicio por obsolescencia o falla.

Líder del procedimiento: Dependencia de sistemas.

Condiciones generales:

- Todos los procesos relacionados con la administración y el mantenimiento de los componentes tecnológicos se deben ejecutar con base a la ficha técnica del producto y manuales del proveedor.
- La dependencia de sistemas debe diseñar, aprobar, socializar y ejecutar el cronograma de mantenimientos de cada uno de los componentes.
- La dependencia de sistemas debe generar el concepto técnico que permita establecer si el componente ha cumplido si ciclo de vida.

Actividades

Tabla 17. Actividades procedimientos

Ítem	Actividad	Descripción	Responsable
1	Instalación y configuración.	Se dispone el activo en servicio destino, se asocia responsable, se habilita el acceso según el tipo de activo con sus respectivos niveles de seguridad.	Dependencia de sistemas.
2	Capacitación de uso.	Se socializa al responsable del activo sobre el uso del este, si aplica.	Dependencia de sistemas.

Tabla 17. (Continuación)

3	Entrega.	Se realiza entrega a satisfacción al nuevo responsable del activo.	Dependencia de sistemas.
4	Seguimiento.	Ejecución del proceso de mantenimiento según cronograma, el proceso puede ser ejecutado por el proveedor o dependencia de sistema según especificaciones contractuales o tiempo trascurrido.	Dependencia de sistemas. Proveedor.
5	Certificación mantenimiento.	Verificar y certificar que el activo funciona correctamente finalizado el proceso de mantenimiento.	Responsable del activo.
6	Baja.	Se realiza la documentación y socialización respectiva en donde se justifica el final de ciclo de vida del activo.	Dependencia de sistemas.

Fuente: Elaboración propia.

6.3.16.2 Puntos de control

Tabla 18. Puntos de control procedimientos

Ítem	Actividad	Método	Frecuencia	Responsable
4	Seguimiento.	Revisión programada o solicitud del responsable del activo.	Ajustada al cronograma de mantenimientos.	Dependencia de sistemas. Proveedor.
5	Certificación mantenimiento.	Verificar y certificar que el activo funciona correctamente finalizado el proceso de mantenimiento.	con cada mantenimiento.	Responsable del activo.

Fuente: Elaboración propia.

6.3.16.3 Control de cambios

Tabla 19. Control de cambios procedimientos

Ítem cambiado	Detalle cambios.	Fecha	Versión
No Aplica	Elaboración del documento primera versión	DD/MM/AAAA	001

Fuente: Elaboración propia.

6.3.17 Procedimientos para gestión de incidentes

6.3.17.1 Objetivo

Establecer los mecanismos de atención que permitan a los usuarios reportar y realizar seguimiento de los incidentes ocurridos hasta su solución.

6.3.17.2 Alcance

Recepción de la solicitud, solución y validación del incidente.

6.3.17.3 Líder del procedimiento

Dependencia de sistemas.

6.3.17.4 Condiciones Generales

- El soporte frente a los incidentes debe integrar a todos los miembros de la organización tanto internos como externos.
- La dependencia de sistemas debe brindar el soporte ajustado a las políticas y estándar de seguridad de la información de la organización.
- Se recomienda aplicar estándares internacionales de buenas prácticas a fin de mejorar la calidad del servicio.
- El horario de solicitudes y respuesta se debe ajustar a los horarios laborales de la organización.
- La organización mediante la alta gerencia debe suministrar las herramientas necesarias a la dependencia de sistemas para ejecución de las tareas.

6.3.17.5 Actividades

Tabla 20. Actividades gestión de incidentes

Ítem	Actividad	Descripción	Responsable
1	recibir solicitud.	Confirmar la recepción de la solicitud del incidente.	Dependencia de sistemas.
2	Análisis de la solicitud.	Clasificar el nivel del incidente a fin de determinar el proceder y el responsable de resolverlo.	Dependencia de sistemas.
3	Asignar responsable.	Notificar al responsable asignado para brindar solución al incidente.	Dependencia de sistemas.
4	Atención del incidente.	Según el nivel del incidente se procede a brindar solución por el medio adecuado o a escalar con el proveedor si se requiere.	Dependencia de sistemas. Proveedor
5	Plan de trabajo	Si en el primer acercamiento no es posible solucionar el incidente se define nuevo plan de acción, tiempos, recursos y responsables.	Responsable del activo.
6	Certificar servicio	Verificación y aprobación por parte del usuario final.	Dependencia de sistemas.
7	Cerrar solicitud.	Finalizar el proceso de soporte.	El usuario.
8	Evaluación del soporte.	Se deben ejecutar auditorías periódicas a fin de evaluar la calidad del servicio.	Dependencia de sistemas.

Fuente: Elaboración propia.

6.3.17.6 Puntos de control

Tabla 21. Puntos de control gestión de incidentes

Ítem	Actividad	Método	Frecuencia	Responsable
4	Atención del incidente.	Identificar y clasificar los incidentes reportados según su tipo y nivel.	Por cada solicitud realizada.	Dependencia de sistemas.

Fuente: Elaboración propia.

6.3.17.7 Control de cambios

Tabla 22. Control de cambios gestión de incidentes

Ítem cambiado	Detalle cambios.	Fecha	Versión
No Aplica	Elaboración del documento primera versión	DD/MM/AAAA	001

Fuente: Elaboración propia.

6.3.18 Procedimientos de continuidad de negocio

6.3.18.1 Objetivo

Establecer los mecanismos mínimos de funcionamiento para garantizar las operaciones de la organización frente a contingencias.

6.3.18.2 Alcance

Definir los roles y responsabilidades a ejecutar frente a una contingencia, su desarrollo y finalización.

6.3.18.3 Líder del procedimiento

Dependencia de sistemas.

6.3.18.4 Condiciones generales

- La alta gerencia de la organización debe instruir en forma clara a la dependencia de sistemas sobre el actuar frente a contingencias de afecten las operaciones desde punto de vista tecnológico.
- La alta gerencia de la organización debe suministrar las herramientas necesarias a la dependencia de sistemas para estructurar e implementar el plan de continuidad de negocio.
- La dependencia de sistemas debe contemplar como mínimo la ejecución de un análisis de riegos.

- El plan de continua a utilizar durante la contingencia debe como mínimo establecer lo siguiente:

    - Roles
    - Responsabilidades
    - Medios de comunicación
    - Espacios
    - Lista de prioridades
    - Procedimientos.

- El principal componente para proteger de ser el corazón de las operaciones de la organización, es decir el centro de datos donde se almacenan los servidores y dispositivos de red.
- La dependencia de sistemas debe justificar la estructuración e implementación del plan de continuidad en cifras.
- La dependencia de sistemas con el apoyo de alta gerencia está en la potestad de integrar a las demás dependencias que se requieran en la estructuración y posterior implementación del plan de continuidad.
- Finalmente, el plan de continuidad debe ser socializado a todos los miembros de organización para su conocimiento, revisión y actualización periódica.

6.3.18.5 Actividades

Tabla 23. Actividades continuidad de negocio

Ítem	Actividad	Descripción	Responsable
1	Asignar roles y responsabilidades	La dependencia de sistemas debe coordinar la asignación de roles y responsabilidades durante la estructuración e implementación del plan de continuidad. La alta gerencia debe garantizar la disponibilidad del personal, el espacio y los recursos.	Alta gerencia. Dependencia de sistemas y otras vinculadas.

Tabla 23. (Continuación)

2	Análisis de impacto y evaluación de riesgos.	Los responsables de estructurar el plan de continuidad deben identificar, clasificar y priorizar los servicios críticos para las operaciones, así como los servicios brindados por terceros y los tiempos de recuperación.	Alta gerencia. Dependencia de sistemas y otras vinculadas.
3	Recursos requeridos	Definir los recursos humanos, físicos y económicos requeridos para mantener las operaciones, se sugiere al menos contar con: Personal, Espacios, Información, Hardware, Software, Proveedores, Socios, Comunicaciones y redes,	Alta gerencia. Dependencia de sistemas y otras vinculadas. Proveedores y asociados.
4	Administración	Establecer el mecanismo de implementación del plan según el tipo de incidente que ocasiona la contingencia para disminuir el impacto. Instruir y coordinar claramente al personal de como ejecutar las actividades de recuperación en cada servicio. Estas son las fases contempladas: **Fase I:** Aspectos previos: Define las actividades a realizar antes de la estructuración, realización e implementación del plan de continuidad. **Fase II:** Estado de la organización: Comprende la recolección de información que permite identificar, clasificar y priorizar las actividades. **Fase III:** Prevención: Su propósito es evitar activar el plan de continuidad mediante la aplicación de medidas preventivas que reduzcan el impacto del incidente. **Fase IV:** Recuperación: Define las prioridades de recuperación con base en el impacto que estas producen en las operaciones de la organización. **Fase V:** Estructuración eimplementación del plan de continuidad: Establece en detalle las tareas y procedimientos a ejecutar para	Alta gerencia. Dependencia de sistemas y otras vinculadas.

		reactivar los servicios críticos que garanticen la continuidad de las operaciones. **Fase VI:** Mantenimiento: Todas las actividades encaminadas a su sostenimiento y actualización.	
5	Capacitación y Socialización	Conviene ejecutar procesos de capacitación al personal que tendrá a cargo responsabilidades asociadas a la implementación del plan, a fin de garantizar que tienen completamente claro su rol. Por otra parte, es importante que todos los miembros de la organización estén enterados del preceder frente a las contingencias.	Alta gerencia. Dependencia de sistemas y otras vinculadas.
6	Pruebas de funcionalidad	Ejecutar pruebas de funcionalidad resulta la mejor estrategia para garantizar que el plan estructurado funciona, al igual que para detectar posibles fallas u omisiones.	Alta gerencia. Dependencia de sistemas y otras vinculadas.
7	Seguimiento	Las revisiones posteriores a implementación permiten medir la efectividad de las medidas aplicas.	

Fuente: Elaboración propia.

6.3.18.6 Puntos de control

Tabla 24. Puntos de control continuidad de negocio

Ítem	Actividad	Método	Frecuencia	Responsable
6	Pruebas de funcionalidad	La ejecución del plan en un ambiente controlado es vital para medir su efectividad y puntos débiles.	Con cada prueba del plan.	

Fuente: Elaboración propia.

6.3.18.7 Control de cambios

Tabla 25. Control de cambios continuidad de negocio

Ítem cambiado	Detalle cambios.	Fecha	Versión
No Aplica	Elaboración del documento primera versión	DD/MM/AAAA	001

Fuente: Elaboración propia.

7 RESULTADOS

Estos se reflejan en el cumplimiento de los objetivos establecidos para el proyecto, los cuales se evidencia en su totalidad en este documento.

- Realizar un análisis de la infraestructura tecnológica para identificar y clasificar los activos de compañía.

- Realizar un análisis evaluativo de las amenazas, vulnerabilidades y riesgos presentes en los activos de compañía.

- Definir las políticas de seguridad de la información de acuerdo con lo establecido la Norma ISO 27001:2013.

- Establecer una propuesta que contenga los controles que permitan la mitigación de los riesgos.

8 CONCLUSIONES

- QWERTY S.A como cualquier empresa u organización deben contar como mínimo con políticas de seguridad de la información que se integren a todos los procesos y procedimientos propios de la lógica de negocio, esto con el fin de establecer e instruir unas reglas claras frente al tratamiento de los datos por parte de los miembros de la organización, los clientes y los terceros con acceso a estos.

  Ahora el diseño, implementación, socialización y mantenimiento de esas políticas de seguridad representan un enorme esfuerzo a nivel de recurso humano, económico, material, tiempo, etc., esfuerzo que la gran mayoría no realiza sobre todo aquellas de menor tamaño como QWERTY S.A al considerar que este tipo de procesos no son prioritarios dado que desconocen su importancia. Es precisamente ese desconocimiento el que no permite establecer la relevancia del tema y el impacto que este puede llegar a casuar en los activos y por ende operaciones.

  La falta de ese interés sustentado en el desconocimiento del valor que aporta a QWERTY S.A. la implementación de las políticas de seguridad de información impide la ampliación del espectro relegando aún más la posibilidad de contemplar un ecosistema más robusto que aporte de forma integral a la protección de los datos y por ende a la calidad de las operaciones en general, lo que común mente se conoce como un sistema de gestión de seguridad de la información (SGSI).

  La ausencia de una estrategia de seguridad más allá de políticas dispersas abre la puerta a una serie de vulnerabilidades que amenazan la productividad y crecimiento de la empresa, las cuales aparecen entre otras cosas debido a la falta de organización y gestión de los activos, puesto que no se cuenta con información estructurada y actualizada de cada uno de ellos, datos que resultan vitales para los procesos de identificación, clasificación y priorización.

Son varios los aspectos a cubrir al momento de optar por implementar un sistema de gestión de seguridad de la información (SGSI) lo puede resultar abrumador y en algunos casos frustrante impidiendo lograr el objetivo de aseguramiento del activo más importante de todos, la información.

- La falta de organización dificulta la gestión de cada uno de los componentes que integran las operaciones en QWERTY S.A. por lo cual no es posible detectar las vulnerabilidades y amenazas presentes en cada uno de ellos.

- La falta de iniciativa y compromiso por parte la alta gerencia ha permitido la nulidad o flexibilización en las medidas encaminadas al aseguramiento de la información en cada uno de los procesos de QWERTY S.A. obteniendo como resultado medidas insuficientes que dificultad la identificación de las vulnerabilidades y por ende la mitigación de las amenazas.

- Durante la fase inicial en la declaración de aplicabilidad se evidencio la deficiencia en la creación de los controles, su implementación, documentación y alineamiento con los estándares.

- No se identificó ninguna metodología o proceso similar encaminado al análisis de los posibles riesgos presentes en los diferentes activos tangibles e intangibles.

- No se evidencia ningún documento que soporte la implementación de medidas que permitan mitigar el impacto de las vulnerabilidades presentes, lo que confirma la ausencia del proceso de análisis de riegos.

- No existen planes de mejora continua establecidos, a su vez que documentación alguna que integre estándares, políticas, procesos y procedimientos de referencia acordes a la normatividad vigente.

9 RECOMENDACIONES

- Construir e instruir un enfoque de seguridad centralizado en la protección de la información que integre a cada una de la áreas y miembros de QWERTY S.A encabeza de la alta gerencia y demás directivos, estableciendo así una hoja de ruta que permita encaminar los esfuerzos en construir una política de seguridad clara tanto en el papel como en la práctica.

  Como se mencionó anteriormente estos procesos requieren de un compromiso firme de la alta gerencia y demás directivos a fin consolidar con los recursos para tal fin, por lo cual se recomienda ejecutar una proyección previa del talento humano, los tiempos, espacios físicos y recursos económicos en general requeridos para el éxito del proyecto.

  Es imperativo definir una estructura jerárquica del personal que hará parte del proyecto con el objetivo de establecer los roles y responsabilidades de cada uno de ellos, esto sin duda aportará a la ejecución de las tareas y su respectivo seguimiento aun después de finalizada, puesto que estas deben contemplar planes de actualización y mejora continua.

  Por otra parte, es altamente recomendado apoyarse de estándares, normas metodologías, etc., que llevan años de mejora continua y que han sido utilizados durante mucho tiempo por un gran número de empresas u organizaciones de prestigio a nivel mundial para establecer procesos y procedimientos en permitan mitigar las vulnerabilidades que ponen el riesgo el activo más importante, la información.

- A fin de brindar una orientación especifica en la selección de norma que aporte de manera significativa a la implementación de un sistema de gestión de seguridad de la información que integre los procesos y procedimientos propios de la lógica de negocio de empresa, se deja a consideración de QWERTY S.A este documento que busca establecer las bases de un SGSI basado en el catálogo de documentos,

metodologías y requisitos de la Norma ISO 27001:2013 la cual tiene por objetivo principal la protección de la información mediante el fortalecimiento de la confidencialidad, integridad y disponibilidad de la información.

- Integrar en la estructura jerárquica del proyecto al menos un profesional idóneo con experiencia en el diseño, implementación y mejora continua de sistemas de gestión de seguridad de la información que cumpla el rol de líder, facilitando así la estructuración de la base del proyecto como el alcance, los objetivos, roles, responsables, tiempos, tareas, etc., componentes requeridos para el éxito del proyecto.

- Disponer de una base de datos actualizada y veraz de todos los activos de QWERTY S.A. con al menos sus características generales, serial, ubicación, responsable y disposición, a fin de contar con el insumo base para la implementación de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) integrada en la Norma ISO 27001:2013.

- Socializar en forma clara y periódica a todos los miembros de la empresa incluidos terceros la política de seguridad de la información con sus respectivos procesos, procedimientos y demás mecanismos de seguridad, enfatizando y dando a conocer su importancia para el éxito de las operaciones de QWERTY S.A.

- Finalmente se recomienda implementar el enfoque metodológico del Ciclo de Deming: Planificar – Hacer – Verificar – Actuar (PHVA), como herramienta de apoyo para la ejecución de las tareas de mejora continua sobre el sistema de gestión de seguridad de la información, integrando procesos de análisis de riesgos y auditorías externas e internas, enfoque que se encuentra integrado en la Norma ISO 27001:2013 y que ya se ha detallo anteriormente en este documento.

BIBLIOGRAFÍA Y REFERENCIAS BIBLIOGRÁFICAS

[1] WIKIPEDIA, Sistema de gestión de la seguridad de la información, 2019. [En línea]. Disponible en: https://bit.ly/36gfNm2

[2] CONGRESO, República de Colombia, Ley 1266 de 2008. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[3] CONGRESO, República de Colombia, Ley 1581 de 2012. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[4] CONGRESO, República de Colombia, Ley 1273 de 2009. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[5] CONGRESO, República de Colombia, Ley 0527 1999. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

[6] CONGRESO, República de Colombia, Ley 1581 2012. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[7] CENTRO, Memoria Histórica, Plan de continuidad tecnológica, versión 001. [En línea]. Disponible en: https://bit.ly/2TnR3mP

[8] CELSIA, Política seguridad de la información, 2014. [En línea]. Disponible en: https://bit.ly/3bQ3XQO

[9] ACUÑA MONTES, Rubén Darío. (julio de 2017). Realizar un sistema de gestión de seguridad informática para Centro Educativo de Sistemas UPARSISTEM de acuerdo con la Normativa ISO/IEC 27001. Disponible en https://repository.unad.edu.co/handle/10596/12586

[10] ÁLVAREZ RIAÑO, Gerson Harley, (abril de 2017). Diseño de un sistema de gestión de seguridad de la información - SGSI basado en la norma ISO27001 incluye: asesoría, planeación. Disponible en https://repository.unad.edu.co/handle/10596/11950.

[11] ARDILA NAVARRETE, Julián Andrés. (octubre de 2016). Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para Positiva Compañía de Seguros S.A en la ciudad de Bogotá. Disponible en https://repository.unad.edu.co/handle/10596/11980

[12] BARRERA CONTRERAS, C. A. (2005). Guía para el Diseño de Sistema de Control Interno en Seguridad de la Información. Disponible en http://biblioteca.uniandes.edu.co/acepto52.php?id=00005056

[13] BAUTISTA SARRIA, S. (2018). Diseño de un sistema de gestión de seguridad informática - SGSI para la Fundación Sabemos Cuidarte en la ciudad de Popayán. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/21306

[14] BERNAL LÓPEZ, W. (2015). Diagnosticar y asesorar la implantación de un sistema SGSI que permita controlar y gestionar todos los procesos relacionados con la información. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/3509

[15] BLOG DE CIENCIAS DE LA INFORMACIÓN. (enero de 2016). La Importancia de la Información en la vida diaria. Disponible en http://blog.pucp.edu.pe/blog/ccii/2010/01/26/la-importancia-de-la-informacion-en-la-vida-diaria/

[16] BOJACÁ GARAVITO, Edgar Alonso. (noviembre de 2016). Diseño de un Sistema de Gestión de Seguridad Informática basado en la norma ISO/IEC 27001- 27002 para el Hospital de Gachetá. Disponible en https://repository.unad.edu.co/handle/10596/12685

[17] BOTERO VEGA, David Humberto. (agosto de 2017). Diseño del Sistema de Gestión de Seguridad Informática y de la Información (SGSI) para la Empresa Belisario Ltda. de la ciudad de Bogotá D.C. Disponible en https://repository.unad.edu.co/handle/10596/12925

[18] BRIÑEZ BAUTISTA, Martha Lucia. (diciembre de 2017). Diseño de un sistema de gestión de seguridad informática para la alcaldía de la Jagua de Ibirico – Cesar basado en la Norma ISO 27001:2013. Disponible en https://repository.unad.edu.co/handle/10596/18453

[19] BUITRAGO ROJAS, D. S. (26 de abril de 2018). Sistema de Gestión de Seguridad de la Información (SGSI) Aplicada al Área de Operaciones de una Empresa de Telecomunicaciones. Disponible en http://hdl.handle.net/11349/13418

[20] CADENA SIERRA, M. A. (23 de febrero de 2017). Modelo de un sistema de Gestión de la Seguridad de la Información aplicada a Entidades Bancarias. Disponible en http://hdl.handle.net/11349/8325

[21] CALERO RODRÍGUEZ, A. X. (27 de mayo de 2017). Propuesta de Modelo de un Sistema de Gestión de la Seguridad de la Información Aplicada a Instituciones Educativas. Disponible en http://hdl.handle.net/11349/6139

[22] CALDERÓN SÁNCHEZ, A. (2015). Implementación del SGSI en el área de redes de COMPUSERVER basado en la norma ISO/IEC 27001:2013. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/3676

[23] CAMARGO RAMÍREZ, Juan David, (abril de 2017). Diseño de un sistema de Gestión de la Seguridad de la Información (SGSI) en el área tecnológica de la Comisión Nacional del Servicio Civil - CNSC basado en la norma ISO27000 e iso27001. Disponible en https://repository.unad.edu.co/handle/10596/11992.

[24] CARDONA TOVAR, L. P., & Ardila García, A. J. (19 de mayo de 2016). Desarrollo de un Marco de Trabajo para la Gestión del SGSI en PYMES Desarrolladoras de Software en Bogotá Basado en la Metodología MGSM-PYME. Disponible en http://repository.udistrital.edu.co/bitstream/11349/2807/1/CardonaTovarLorenaPatricia2016.pdf

[25] CASTAÑEDA MURCIA, A. R. (4 de septiembre de 2018). Diseño de un Sistema de Seguridad de la Información para la Empresa VPS Software. Disponible en http://hdl.handle.net/11349/14194

[26] CASTILLO SARMIENTO, José Darling, Rueda León, Alix. (diciembre de 2017). Diseñar SGSI para el Colegio Agroindustrial de Puerto Nuevo. Disponible en https://repository.unad.edu.co/handle/10596/17415.

[27] CAZARAN BUITRAGO, Olger Yonatan. (marzo de 2018). Diseño de un sistema de gestión de seguridad de la Información en el área de recursos informáticos de la Contraloría Departamental del Meta, según la norma ISO 27001. Disponible en https://repository.unad.edu.co/handle/10596/17423

[28] CELIS MÉNDEZ, Carlos Alberto. Franco GÓEZ, Oralia. (noviembre de 2016). Implementación del Sistema de Gestión de Seguridad de la Información – SGSI, en el proceso de apoyo “Gestión Tecnológica y de la Información” del Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON. Disponible en https://repository.unad.edu.co/handle/10596/11482

[29] CELY ESPITIA, Ronald Mauricio. (agosto de 2017). Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) con base al modelo de seguridad y privacidad de la información según lineamentos del Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia gel (gobierno en línea) y en cumplimiento del Decreto 1078 de 2015 y 2573 de 2014. Disponible en https://repository.unad.edu.co/handle/10596/17379

[30] CONTRERAS ESGUERRA, Lidia Constanza. (diciembre de 2016). Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la dirección de sistemas de la gobernación de Boyacá. Disponible en https://repository.unad.edu.co/handle/10596/11895

[31] CORAL OJEDA, Jesús Armando. (abril de 2017). Diseño de un sistema de gestión de seguridad para la red datos bajo la norma ISO 27001:2013 en el Centro de Estudios Emssanar CETEM de la ciudad de Pasto. Disponible en https://repository.unad.edu.co/handle/10596/11875

[32] DORIA CORCHO, A. (2015). Diseño de un sistema de gestión de la seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas y telecomunicaciones de la Universidad de Córdoba. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/3624

[33] DURÁN FLÓREZ, Á. N., & LUMBAQUE Figueroa, I. C. (20 de septiembre de 2017). Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa HECC CURRIER basado en ISO 27001. Disponible en http://repository.udistrital.edu.co/bitstream/11349/13421/13/LumbaqueFigueroaIvanCamilo2018.pdf

[34] ELECTRÓNICA, A. (octubre de 2012). MAGERIT – versión 3.0 Libro II - Catálogo de Elementos. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

[35] ELECTRÓNICA, a. (octubre de 2012). MAGERIT – versión 3.0 Información Libro III - Guía de Técnicas. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

[36] ELECTRÓNICA, A. (octubre de 2012). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información libro l. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[37] ESCOBAR MORENO, D. R., & TOBARIA León, C. C. (25 de enero de 2017). Modelo De Medición Para El SGSI De Las Entidades Gubernamentales, Que Han Seguido Los Lineamientos Establecidos Por La Estrategia De Gobierno En Línea. Disponible en http://repository.udistrital.edu.co/bitstream/11349/6618/1/EscobarMorenoDanielRicardo2017.pdf

[38] FUENTES PEÑA, T. P. (15 de noviembre de 2017). Propuesta de viabilidad de la implementación del estándar ISO/IEC 27001:2013 en el proceso de investigación, diseño y desarrollo de la empresa TECNOFACTORY SAS. Disponible en http://hdl.handle.net/11349/13416

[39] GARCÍA HERNÁNDEZ, D. A., & Ruiz Murillo, J. H. (11 de septiembre de 2017). análisis y Gestión de Riesgos en el Marco del SGSI, Basado en la Metodología MAGERIT y Apoyado en un API Web para su Ejecución. Disponible en http://repository.udistrital.edu.co/bitstream/11349/6813/1/Documento%20Proyecto%20Grado.pdf

[40] GÓMEZ PACHÓN, E. L. (24 de mayo de 2017). Modelo de un Sistema de Gestión de la Seguridad de la Información (SGSI) Aplicada a Corredores de Seguros Bajo el Marco de Referencia de la Norma ISO/IEC 27001:2013. Disponible en http://hdl.handle.net/11349/14205

[41] GONZÁLEZ GARCÍA, Ronald Alejandro, (2016). Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para el área de tecnología de la empresa Baker Tilly Colombia Ltda. de la ciudad de Bogotá, bajo la norma ISO 27001:2013. Disponible en https://repository.unad.edu.co/handle/10596/12722

[42] GONZÁLEZ TABARES, E. (2018). plan de implementación de un sistema de gestión de seguridad de la información para la Unidad Administrativa Parques Nacionales Naturales de Colombia, según Norma ISO 27001: 2013. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/23186

[43] GUERRERO RODRÍGUEZ, P. A., & Peña Muñoz, J. C. (5 de septiembre de 2018). Guía de Sistema de Gestión de Seguridad de la Información SGSI para entidades de CONTACT center. Disponible en http://repository.udistrital.edu.co/bitstream/11349/14199/1/GuerreroRodriguezPedroAlejandro2018.pdf

[44] GUERRERO, D. M., & Martínez, J. C. (noviembre de 2016). Propuesta de un Sistema de Gestión de la Seguridad de la Información para Entidades Dedicadas al Servicio de Outsourcing de TI. Disponible en http://repository.udistrital.edu.co/bitstream/11349/8320/1/GuerreroDiana%20Marcela%202016.pdf

[45] GIRALDO CEPEDA, L. (2016). Análisis para la implementación de un sistema de gestión de seguridad de la información según la norma ISO 27001 en la empresa SERVIDOC S.A. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/6341

[46] HERRERA CHÁVEZ, L. F. (15 de febrero de 2019). Diagnóstico y gestión de riesgos de los activos de información dentro de la secretaría de seguridad operacional y de la aviación civil de la aeronáutica civil. Disponible en http://hdl.handle.net/11349/14836

[47] ISOTOOLS, (S.F). Sistemas de Gestión de Riesgos y Seguridad. Disponible en https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

[48] JARA PÉREZ, D. F. (15 de agosto de 2017). Valoración y Plan de Tratamiento de Riesgos de Seguridad de la Información para los Procesos Incluidos en el Alcance del SGSI del Cliente TGE de la Empresa ASSURANCE CONTROLTECH. Disponible en http://repository.udistrital.edu.co/bitstream/11349/6492/1/JaraPerezDianaFernanda2017.pdf

[49] JIMÉNEZ GÓMEZ, Alejandro. (diciembre de 2016). Diseño de un sistema de gestión de seguridad en la información (S.G.S.I) basado en la norma NTC ISO/IEC 27001, para la agencia de publicidad MCCANN de la ciudad de Bogotá. Disponible en https://repository.unad.edu.co/handle/10596/13442

[50] JOJOA PAZ, D. y Córdoba CUAYCAL, K. (2016). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO 27001: 2013 para la red inalámbrica de la empresa innovación global S.A, ubicada en el municipio de Sibundoy Putumayo. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/6146

[51] MIRANDA RODRÍGUEZ, F. L. (26 de abril de 2018). Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para las Empresas Dedicadas a la Logística en Mensajería. Disponible en http://repository.udistrital.edu.co/bitstream/11349/13420/1/AnaLuisaVillamilMartin2018.pdf

[52] MORENO PALOMEQUE, Letty Yaneth. Palacios. (febrero de 2018). Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO 27001:2013 para la empresa UNISANAR IPS de Quibdó. Disponible en https://repository.unad.edu.co/handle/10596/15028

[53] MOYANO ORJUELA, L. A., & Suárez Cárdenas, Y. E. (13 de septiembre de 2017). Plan de Implementación del SGSI Basado en la Norma ISO 27001:2013 para la Empresa Interfaces y Soluciones S.A.S. Disponible en http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

[54] NARANJO JIMÉNEZ, E. A. (3 de septiembre de 2018). Propuesta de un Sistema de Seguridad de la Información para la Institución Educativa CELCO San Lucas. Disponible en http://hdl.handle.net/11349/14207

[55] NÚÑEZ ÁLVAREZ, Y. (2015). Diseño de un SGSI para el área de automatización del proceso de báscula, de la empresa minera SANOHA LTDA ubicada en Nobsa –Boyacá. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/3649

[56] NÚÑEZ VERGARA, W. A. (11 de octubre de 2017). Diseño del Sistema de Gestión de Seguridad de la Información para la Empresa SEREXCEL Servicios Funerarios. Disponible en http://hdl.handle.net/11349/8323

[57] ORTIZ CÁRDENAS, G. A. (2 de abril de 2018). Propuesta de Implementación de un Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO 27001:2013 para la Empresa Lovato City Gas S.A.S. Disponible en http://hdl.handle.net/11349/13419

[58] ORTIZ MANRIQUE, Edwin Omar. (marzo de 2018). Análisis de causas de riesgos en la protección de la información de la Empresa SOLTEC-ING y recomendaciones de seguridad. Disponible en https://repository.unad.edu.co/handle/10596/17448

[59] PALACIOS, Y. y Moreno Palomeque, L. (2018). Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO 27001:2013 para la empresa UNISANAR IPS de Quibdó. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/15028

[60] PEÑUELA VÁSQUEZ, Dayan. (agosto de 2018). Análisis e identificación del estado actual de la seguridad informática, dirigido a las organizaciones en Colombia, que brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información. Disponible en https://repository.unad.edu.co/handle/10596/17260

[61] PERDOMO RAMÍREZ, M. A. (6 de septiembre de 2018). Diseño de un Sistema de Gestión de Seguridad (SGSI) para la Empresa Manufacturera Persianas y Enrollables SAFRA SAS Basado En Los Estándares de la Norma ISO 27001. Disponible en http://repository.udistrital.edu.co/bitstream/11349/14200/1/MateusAlfonsoFrankyeSteven2018.pdf

[62] PÉREZ PORTILLO, Maribel Jaqueline. Jurado Sánchez, Mario Fernando. (mayo de 2018). Diseño de un sistema de gestión de seguridad de la información para la ferretería argentina de la ciudad de Pasto. Disponible en https://repository.unad.edu.co/handle/10596/18306

[63] PINEDA VARGAS, L. Y. (24 de mayo de 2017). Diseño de un Sistema de Gestión de Seguridad de la Información para la Empresa DESIGNER Software LTDA. Disponible en http://hdl.handle.net/11349/6738

[64] PMG SSI, (abril de 2015). La importancia de la norma ISO 27001. Disponible en https://www.pmg-ssi.com/2015/04/la-importancia-de-la-norma-iso-27001/

[65] PRADA HERNÁNDEZ, N. M. (2010). Diseño de un sistema de gestión de seguridad de la información, alineado con la Norma ISO. Disponible en http://hdl.handle.net/10554/7515

[66] PRIETO MORENO, L. M. (16 de noviembre de 2016). Propuesta para Establecer un Sistema de Gestión de Seguridad de la Información para la Empresa SIE Software S.A.S. Disponible en http://hdl.handle.net/11349/7345

[67] PRIETO SARMIENTO, E. J. (17 de noviembre de 2016). Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Empresa Agility S.A.S. Disponible en http://repository.udistrital.edu.co/bitstream/11349/4709/1/Edward%20Jonathan%20Prieto%20Sarmiento%202016.pdf

[68] PÚBLICAS, M. d. (octubre de 2012). PAE Portal Administrativo Electrónica. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XJLGNyhKjIW

[69] PULIDO BARRETO, A. y Mantilla Rodríguez, J. (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. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/6327

[70] 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 Villa garzón Putumayo. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/3625

[71] RADA GONZÁLEZ, Eddie Luis. (diciembre de 2017). Determinar el nivel de seguridad y privacidad de la información del Instituto Museo Nacional (IMN). Disponible en https://repository.unad.edu.co/handle/10596/20450

[72] RODRÍGUEZ BARRERA, C. y Alemán Novoa, H. (2015). Metodologías para el análisis de riesgos en los SGSI. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/17000

[73] RODRÍGUEZ CORREA, Jorge Leonardo. (agosto de 2017). Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en ISO27001 para laboratorios servicios farmacéuticos de calidad SFC LTDA. Disponible en https://repository.unad.edu.co/handle/10596/12598.

[74] RODRÍGUEZ RUIZ, A. I. (junio de 2016). Modelo de un Sistema de Gestión de la Seguridad de la Información Aplicada a una Empresa de Software. Disponible en http://hdl.handle.net/11349/8318

[75] Ruiz Peña, J. (2018). Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001:2013, en la Cooperativa Multiactiva del personal del Sena, en Bogotá. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/17300

[76] SAMBONI, E. F. (9 de mayo de 2018). Propuesta de Modelo de un Sistema de Gestión de Seguridad de la Información para Pequeñas Empresas de Desarrollo de Software. Disponible en http://repository.udistrital.edu.co/bitstream/11349/13425/1/SamboniSamboniEduardFernando2018.pdf

[77] SAMPER IBÁÑEZ, P. (2015). Diseño de un sistema de gestión de seguridad de la información en el área de sistema de la empresa RYMCO S.A bajo la norma ISO

IEC/27001:2013. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/3987

[78] SGSI (s.f.). Disponible en http://www.iso27000.es/download/doc_sgsi_all.pdf

[79] SSI, P. (16 de marzo de 2015). SGSI. Disponible en https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

[80] SUAREZ ACUÑA, D. E. (4 de marzo de 2016). Diseño de una Arquitectura de Red Basado en un Modelo de Defensa en Profundidad Utilizando Estándares de las Normas ISO 27000 y COBIT 5.0. Disponible en http://hdl.handle.net/11349/2726

[81] SUÁREZ GONZÁLEZ, Rafael. (agosto de 2018). Análisis de activos de información para un sistema misional basados en la metodología MAGERIT v3 y la norma ISO 27001:2013. Disponible en https://repository.unad.edu.co/handle/10596/19571

[82] TABORDA BEDOYA, C. y Guzmán García, A. (2015). Diseño de un sistema de gestión de la seguridad informática – SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C., a través de la auditoría. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/3448

[83] TABARES RENDÓN, J. (2015). Implementación de un sistema de gestión de seguridad informática en la confederación de cámaras de comercio - CONFECÁMARAS. Colombia: Disponible en: https://repository.unad.edu.co/handle/10596/3653

[84] TORRES PÉREZ, Liliana Andrea. (marzo de 2018). Identificación del estado de madurez y diseño de controles para la implementación de un sistema de gestión de seguridad de la información en el proceso TIC de estrategias empresariales de Colombia S.A.S. Disponible en https://repository.unad.edu.co/handle/10596/17399

[85] VALERO DURAN, J. D. (14 de diciembre de 2015). Seguimiento y Evaluación para un Software de Administración para un Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO 27001:2013. Disponible en http://hdl.handle.net/11349/4786

[86] VARGAS RIVERA, Robinson. (noviembre de 2018). Diseño de un sistema de gestión de seguridad aplicada a la oficina de sistemas de información del Hospital Regional del Líbano ese. Disponible en https://repository.unad.edu.co/handle/10596/22964

[87] VÁSQUEZ, K. d. (octubre de 2013). Aplicación de la metodología MAGERIT para el Análisis y Gestión de Riesgos de la Seguridad de la Información Aplicado a la

Empresa Pesquera e Industrial Bravito S.A. Disponible en https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

[88] VILLAVISAN BUITRAGO, J. F. (20 de junio de 2018). Diseño Funcional de Módulo de Proyectos de Sistemas ERP Caso de Estudio en la Compañía Colombiana de Seguridad Electrónica MARNELL Security. Disponible en http://hdl.handle.net/11349/13585

[89] YEPES GONZÁLEZ, I. L. (octubre de 2018). Diseño de programa de inspecciones de seguridad para TGT GAMAS. Disponible en http://hdl.handle.net/11349/14601

[90] ZAQUE GONZÁLEZ, O. (2016). Proyección financiera y tecnológica requerida para la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), bajo la norma ISO/IEC 27001:2013 Disponible en: https://repository.unad.edu.co/handle/10596/8595

ANEXOS

Anexos a. Resumen analítico especializado.

Tema: Seguridad informática
Título: Diseño de un sistema de gestión de la seguridad de la información para la empresa QWERTY S.A.
Autor: GARCÍA GÓMEZ, Filanderson.
Fuer tes: [1] WIKIPEDIA, Sistema de gestión de la seguridad de la información, 2019. [En línea]. Disponible en: https://tinyurl.com/ybhmths4 [2] CONGRESO, República de Colombia, Ley 1266 de 2008. [En línea]. Disponible en: https://tinyurl.com/y927gc4p [3] CONGRESO, República de Colombia, Ley 1581 de 2012. [En línea]. Disponible en: https://tinyurl.com/yxh8glq9 [4] CONGRESO, República de Colombia, Ley 1273 de 2009. [En línea]. Disponible en: https://tinyurl.com/y7purzg5 [5] CONGRESO, República de Colombia, Ley 0527 1999. [En línea]. Disponible en: https://tinyurl.com/yy2t3qpf [6] CONGRESO, República de Colombia, Ley 1581 2012. [En línea]. Disponible en: https://tinyurl.com/yxh8glq9 [7] CENTRO, Memoria Histórica, Plan de continuidad tecnológica, versión 001. [En línea]. Disponible en: https://tinyurl.com/y8qz8sqe [8] CELSIA, Política seguridad de la información, 2014. [En línea]. Disponible en: https://tinyurl.com/y85ljtkq
Año: 2020
Resumen: La seguridad informática representa un gran reto para las compañías u organizaciones en general, y aún más para aquellas que hacen parte en forma directa del sector, como las compañías dedicadas a fomentar las tecnologías de información y comunicación, estas compañías llevan a cuesta una gran responsabilidad toda vez que cumplen la función de evangelizar su uso y por ende deben dar ejemplo en la aplicación de las normas, metodologías y estrategias que buscan fortalecer su avance. QWERTY S.A como una compañía del sector tecnológico debe asumir un rol ejemplificador en lo concerniente a la seguridad de la información, dado que resulta ser el activo más importante en la mayoría de las compañías u organizaciones, por este motivo se busca que mediante el diseño de un SGSI estandarizar los procesos inmersos en la administración de la información con el objetivo de garantizar su confidencialidad, integridad y disponibilidad, teniendo claro que no existe la seguridad absoluta.
Palabras Claves: DISEÑO**,** SGSI, ISO/IEC 27001:2013.

Contenido del documento:	
Definición del problema	• Antecedentes del problema • Formulación del problema
Justificación	
Objetivos	• Objetivo general • Objetivos específicos
Marco referencial	• Marco teórico • Marco conceptual • Marco legal
Diseño metodológico	• Metodología de desarrollo • Enfoque metodológico
Desarrollo de los objetivos	• Análisis de la infraestructura tecnológica para identificar y clasificar los activos de compañía. • Análisis evaluativo de las amenazas, vulnerabilidades y riesgos presentes en los activos de compañía. • Definir las políticas de seguridad de la información de acuerdo con lo establecido la norma ISO/IEC 27001:2013
Resultados	
Conclusiones	
Recomendaciones	

Descripción del problema de investigación: QWERTY S.A a pesar de pertenecer al sector tecnológico no cuenta con una política clara que le permita estandarizar los procesos inmersos en la administración de la información, lo cual representa una gran dificultad técnica y a su vez moral, si se toma en cuenta que su principal objetivo busca el desarrollo tecnológico en comunidades colombianas, este enfoque evangelizador no surtirá efecto si la compañía no refleje un compromiso real en aplicación de la norma que aporte al avance de la tecnología sirviendo como modelo para los demás.

Los problemas presentes en una compañía que no estandariza sus procesos inmersos en la administración de la información pueden ir desde lo más básico, como la falta de un sistema de control de acceso a sus instalaciones e infraestructura tecnológica a nivel hardware y software que no cumple con requisitos técnicos mínimos, hasta aspectos vitales como la no caracterización del personal y su nivel de acceso a la información.

Los riesgos presentes ante la omisión de esta política de estandarización se pueden ver reflejados en un sin número de eventos adversos que puede afectar el núcleo de la compañía, entiéndase como núcleo la información, lo cual resultaría devastador para su modelo de negocio en todos los niveles.

Objetivo general: Diseñar un SGSI bajo la norma ISO/IEC 27001:2013 para la compañía QWERTY S.A en busca de establecer un control sobre de los riesgos de seguridad de la información en sus procesos de administración.

Objetivos específicos:

- Realizar un análisis de la infraestructura tecnológica para identificar y clasificar los activos de compañía.
- Realizar un análisis evaluativo de las amenazas, vulnerabilidades y riesgos presentes en los activos de compañía.
- Definir las políticas de seguridad de la información de acuerdo con lo establecido la Norma ISO/IEC 27001:2013.
- Establecer una propuesta que contenga los controles que permitan la mitigación de los riesgos.

Metodología: Cuantitativa donde el objetivo es establecer el número de las vulnerabilidades, amenazas y riesgos, etc., que afectan o podrían llegar afectar la seguridad de la información y descriptiva porque integra todos procesos de la empresa QWERTY S.A.

Principales referentes teóricos y conceptuales:

- Norma ISO/IEC 27001:2013
- Norma ISO/IEC 27002:2013
- MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Resultados:

- Análisis de la infraestructura tecnológica para identificar y clasificar los activos de la compañía.
- Análisis evaluativo de las amenazas, vulnerabilidades y riesgos presentes en los activos de la compañía.
- Propuesta que contenga los controles que permitan la mitigación de los riesgos.
- Políticas de seguridad de la información.

Conclusiones:

- Cualquier empresa u organización deben contar como mínimo con políticas de seguridad de la información que se integren a los procesos y procedimientos propios de la lógica de negocio, esto con el fin de establecer e instruir unas reglas claras frente al tratamiento de los datos por parte de los miembros de la organización, los clientes y los terceros con acceso a estos.

- El diseño, implementación, socialización y mantenimiento de las políticas de seguridad representan un enorme esfuerzo a nivel de recurso humano, económico, material, tiempo, etc., esfuerzo que la gran mayoría de empresas u organizaciones no realiza sobre todo aquellas de menor tamaño al considerar que este tipo de procesos no son prioritarios dado que desconocen su importancia.

- La ausencia de los mecanismos de control denota la falta de organización y gestión de cada uno de los componentes que integran las operaciones de la empresa u organización, por lo cual no es posible detectar las vulnerabilidades y amenazas presentes en cada uno de ellos.

- No se invierten recursos en personal calificado o en mejorar las competencias del personal actual en busca de fortalecer las metodologías que permitan avanzar en securización de la información de la empresa u organización.