ETAPA DE PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL AREA DE TECNOLOGÍA DE LA IPS GARPER MÉDICA SAS BASADO EN LA NORMA ISO/IEC 27001:2013

IRMAENA CRIOLLO BETANCOURT

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

ETAPA DE PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL AREA DE TECNOLOGÍA DE LA IPS GARPER MÉDICA SAS BASADO EN LA NORMA ISO/IEC 27001:2013

IRMAENA CRIOLLO BETANCOURT

Proyecto de Grado – Aplicado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

MSC. KATERINE MARCELES
Directora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico este trabajo a mis padres, quienes fueron un gran apoyo, brindándome su motivación en cada una de las actividades permitiéndome ver los progresos que tenía día a día.

A toda mi familia por confiar en que sería capaz de superar todos los obstáculos y darme nuevas expectativas, recordándome todos los anhelos para alcanzar el sueño de culminar este proyecto.

Finalmente, a Dios por bendecirme en cada momento dándome la fuerza necesaria para no desfallecer en la realización de este proyecto.

AGRADECIMIENTOS

A la Universidad Nacional Abierta y a Distancia UNAD por permitirme ser parte de esta gran institución, así como también a cada uno de los profesores y asesores que me acompañaron en este proceso.

Agradezco infinitamente a Dios, padres y familiares, los cuales, con su apoyo incondicional, ayuda y esmero han permitido crecer como gran persona, profesional y ser de bien útiles en la sociedad.

Igualmente, el más profundo agradecimiento a la asesora de Tesis, Katerine Márceles, por haberme brindado la oportunidad de recurrir a su gran capacidad y conocimiento, donde por medio de su paciencia, esmero y dedicación me pudo guiar durante todo el desarrollo de la Tesis.

Al Gerente de la IPS Garper Médica SAS, el Dr. Pablo Emilio Gutiérrez Méndez, por haberme permitido realizar el proyecto de grado aplicado: Etapa de planificación de un sistema de gestión de seguridad de la información para el área de tecnología de la IPS Garper Médica SAS basado en la norma ISO/IEC 27001:2013

Finalmente, agradezco a todos los que fueron mis compañeros de clase, ya que gracias al compañerismo y apoyo han aportado un alto porcentaje en mis ganas de seguir adelante como especialista en Seguridad informática.

CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

Pág.

LISTA DE CUADROS

Pág.

GLOSARIO

ACCIÓN CORRECTIVA: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del Sistema de Gestión de la Seguridad de la Información (SGSI) con el fin de prevenir su reproducción[1].

ACCIÓN PREVENTIVA: Encaminada a prevenir latentemente las no conformidades agrupadas a la culminación y acción del Sistema de Gestión de la Seguridad de la Información (SGSI).

ACTIVO DE INFORMACIÓN: Cualquier elemento que tenga valor para la organización.

AMENAZA: Acción que se produce por una vulnerabilidad para infringir contra la seguridad de un sistema de información. De esta forma podría tener un gran efecto negativo sobre algún elemento. Las amenazas proceden de ataques como fraude, robo, virus, sucesos físicos (incendios, inundaciones) o negligencia y fallos institucionales (inadecuado majeo de contraseñas, no usar cifrado)[2].

DIAGRAMA GANTT: Herramienta gráfica cuyo objetivo es exponer el tiempo de dedicación previsto para diferentes tareas o actividades a lo largo de un tiempo total determinado[3].

DATOS: Elementos de la información que crean almacenan, tratan, transmiten y

---

[1] ESCUELA EUROPEA DE EXCELENCIA. 10.2. No conformidad y acción correctiva. [Sitio web]. https://www.nueva-iso-9001-2015.com/10-2-no-conformidad-y-accion-correctiva/.

[2] INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? 2021, de Gobierno de España [Sitio web]. https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

[3] LAUDON, Kenneth C. y LAUDON, Jane P., Sistemas de Información Gerencial, trad. por Vidal Romero Elizondo, 12ª Edición pp.56-64.

destruyen.

ISO: Organización Internacional de Normalización", es el organismo encargado de promover el desarrollo de normas internacionales[4].

IPS: Institución Prestadora de servicios de Salud.

INCIDENTE DE SEGURIDAD: Se presenta cuando una amenaza o un conjunto de amenazas suceden y aprovecha una vulnerabilidad.

MAGERIT: Define los procedimientos que sirven de guía para el establecimiento de la protección necesaria de los sistemas de información de una institución [5].

PERSONAL: Todo el personal de Garper Médica S.A.S, subcontratado, los usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información.

POLÍTICAS DE SEGURIDAD: Es la declaración de las reglas que se deben respetar para acceder a la información y a los recursos.

RIESGOS: Probabilidad de sufrir daños o pérdidas.

SISTEMA DE GESTIÓN DE SEGURIDAD EN LA INFORMACIÓN SGSI: Conjunto de políticas, instrucciones, directrices que son dirigidos conjuntamente por una entidad, en la exploración de salvaguardar sus activos de información.

---

[4] PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA. Software ISO Calidad. 2021, de ISOTools Sitio web: https://www.isotools.org/normas/calidad/iso-9001/.

[5] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. (2017). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España: © Ministerio de Hacienda y Administraciones Públicas.

SEGURIDAD INFORMÁTICA: Hace un énfasis en la protección de los sistemas de información, computadoras, las redes e infraestructura tecnológica, también se relaciona con temas en un contexto como: ataques informáticos, virus, Spam, estudio de vulnerabilidad, Firewall, contraseñas[6].

SEGURIDAD DE LA INFORMACIÓN: Su objetivo es salvaguardar la información teniendo en cuentas los tres pilares de confidencialidad, integridad y disponibilidad de la información. También se relación con temas como la definición de políticas y normas, el control escaso de cambios, los riesgos operacionales, el plan de continuidad de negocio, categorización de la información y matrices de riesgo.

TECNOLOGÍA: Son todos los equipos utilizados para gestionar la información y las comunicaciones.

TIC: Tecnología de la información y comunicaciones.

VULNERABILIDAD: Corresponde a una debilidad en un sistema que pone en peligro la seguridad de la información, permitiendo que un atacante pueda complicar la integridad, disponibilidad o confidencialidad, por lo que es necesario encontrarlas y eliminarlas lo antes posible, estas vulnerabilidades también se pueden orientar en fallos de diseño, errores de configuración o faltas de procedimientos [7].

[6] ROMERO de Castro, Martha Irene. La seguridad en términos generales. En INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. *2020* pp.13- 22. Manabí: Innovación y Desarrollo,S.L.

[7] CASTRO Gil, Manuel A. Gestión de Proyectos con Microsoft Project 2013. España: Editorial RA-MA.

RESUMEN

Este proyecto aplicado para la etapa de planificación de un sistema de Gestión de seguridad de la información a través de un proceso integral para el área de Tecnología de la IPS Garper Médica SAS, como Institución prestadora de servicios de salud privada, se realiza con el fin de planificar un SGSI, establecer las políticas y lineamientos de seguridad de la información, en beneficio de proteger la información teniendo en cuenta los pilares fundamentales como son la confidencialidad, integridad y disponibilidad, lo anterior, efectuando con el compromiso constitucional de salvaguardar la información de la entidad y así garantizar la continuidad en su prestación de servicios.

Para el desarrollo del SGSI (Sistema de gestión de seguridad de la información) se enmarca la norma ISO/IEC 27001:2013, donde se establecen los requisitos para la planeación, implementación, mantenimiento y mejora continua de un sistema de gestión, definiendo el alcance del SGSI, se someterá a evaluación o auditoría los sistemas de seguridad informática e infraestructura TI de la entidad, este diagnóstico indicará en qué estado se encuentran estos sistemas y las medidas correctivas para el mejoramiento, a su vez, se reunirá toda la documentación deseada que alimentará una base de conocimiento, agrupando por tareas lógicas y actividades que será ajustable según el tamaño de la empresa. Igualmente, se organizará dicha documentación por fases de ejecución y organización del proyecto mediante el uso del diagrama Gantt.

Se definirá un tratamiento de los riesgos detectados y decidiendo la aplicación o controles a implementar, se presentará los resultados de la medición de la eficacia de los controles, dando un panorama completo de los alcances de la norma. Por último, se hace el despliegue y puesta marcha del proyecto.

Palabras clave: Riesgos de seguridad, ISO 27001, controles, Políticas de Seguridad de la información.

ABSTRACT

This project applied to the planning stage of an information security management system through an integral process for the Technology area of the IPS Garper Médica SAS, as an Institution that provides private health services, is carried out in order to to plan an ISMS, establish information security policies and guidelines, in order to protect the information taking into account the fundamental pillars such as confidentiality, integrity and availability, the above, carrying out the constitutional commitment to safeguard the information of the entity and thus guarantee continuity in its provision of services.

For the development of the ISMS (Information Security Management System) the ISO / IEC 27001: 2013 standard is framed, where the requirements for the planning, implementation, maintenance and continuous improvement of a management system were achieved, defining the scope of the ISMS, the entity's computer security and IT infrastructure systems will be evaluated or audited, this diagnosis will indicate in what state these systems are and the corrective measures for improvement, in turn, all the desired documentation that It will feed a knowledge base, grouping by logical tasks and activities that will be adjustable according to the size of the company. Likewise, said documentation will be organized by phases of execution and organization of the project through the use of the Gantt chart.

A treatment of the risks detected will be defined and, after deciding the application or controls to be implemented, the results of the measurement of the effectiveness of the controls will be presented, giving a complete overview of the scope of the standard. Finally, the deployment and start-up of the project is carried out.

Keywords: Security risks, ISO 27001, controls, Information Security Policies.

INTRODUCCIÓN

Hoy en día cualquier entidad que posea un sistema de información, sin importar el tamaño de la información, debe preocuparse por la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que garantice integridad y control sobre los datos que se almacenan.

Una buena implementación de un SGSI en las clínicas privadas es muy básica, con lo cual su infraestructura, sistemas informáticos y de información son vulnerables a riesgos de seguridad y ataques cibernéticos. Al indagar directamente en la IPS Garper Médica S.A.S, se encontró que esta institución ha tenido problemas al no tener un SGSI implementado, lo cual hace que esta IPS tenga varios factores negativos en su operatividad, seguridad informática y mantenimiento de sistemas críticos.

Este proyecto de grado pretende Planificar un sistema de gestión de seguridad de la información para el área de Tecnología de la IPS Garper Médica S.A basado en el estándar ISO/IEC 27001:2013, por medio de este tipo de soluciones se pretende minimizar el riesgo de fallas, incidencias, fraudes, manipulación y pérdida de información sensible en los sistemas informáticos en la clínica Garper Médica SAS, a su vez, se quiere que con esta implementación se preserve la confidencialidad, integridad y disponibilidad de la información en sus procesos y sistemas.

Para el desarrollo de este proyecto de grado, se definirá un tratamiento de los riesgos detectados y decidiendo la aplicación o controles a implementar, se presentará los resultados de la medición de la eficacia de los mismo, dando un panorama completo de los alcances de la norma.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Actualmente en las IPS Privadas, la aplicabilidad de los SGSI respecto a la ISO/IEC 27001:2013, es muy básica o nulo, lo cual hace que su sistema sea vulnerable a riesgos y ataques cibernéticos, provocando problemas en su funcionamiento empresarial, infraestructura y de seguridad de la información, no se cuenta con políticas establecidas respecto a la confidencialidad, integridad y disponibilidad de la información de la IPS. Igualmente, la IPS ha tenido muchos problemas al no tener un SGSI implementado, como, por ejemplo:

- Pérdida de información.
- Manipulación inapropiada de información.
- Falta de soporte en procesos críticos.
- Pérdidas de competitividad y oportunidades en procesos comerciales.
- Falta de integración en los sistemas de información.
- Ausencia de confidencialidad en la información manejada.
- Falta de proceso y políticas en manejo de la información.
- Pérdida de trazabilidad en el reporte de incidentes presentados.
- La falta de concienciación, apropiación y conocimiento en temas de seguridad por parte de todos los funcionarios.

Lo cual hace que la IPS presente varios factores negativos en su operatividad, seguridad informática y mantenimiento de sistemas críticos.

Respecto a la pérdida de información, manipulación, se ve afectada la IPS ya que, por terminaciones de contratos a nivel del talento humano, las personas se llevan la

información o la eliminan. En el cuadro 1 se presentan otros factores asociados a las problemáticas en materia de seguridad que se presentan en la organización.

Cuadro 1.Factores asociados a los antecedentes del problema

Antecedentes	Factor
No existe una cultura de seguridad de la información	• Falta de apropiación, capacitación, concientización, en temas de seguridad por parte de los funcionarios de Garper Médica. • No existe una cultura para la mejora continua de la seguridad de la información. • Falta de interés por parte de los funcionarios en temas de seguridad. • No existe una participación de toda la organización con relación a la definición de procedimientos adecuados para la identificación de controles de seguridad basados en una evaluación de riesgos.
Existen procesos definidos y documentados, pero no se socializan	• Falta de liderazgo y acompañamiento en los procesos definidos • Falta de compromiso por parte de los funcionarios y líderes.
No existen políticas de seguridad en la información definidas	• No se cuenta con conocimientos del modelo que se debe desarrollar.

Fuente: Elaboración Propia

1.2 FORMULACIÓN DEL PROBLEMA

Teniendo en cuenta lo anterior, surge el siguiente interrogante: ¿Cómo la fase de planificación de un SGSI mejoría el entorno digital y la seguridad informática en los procesos internos de la IPS Garper Médica SAS?

2 JUSTIFICACIÓN

El diseño de las políticas de seguridad en la información para la IPS Garper Médica SAS permitirá asignar un valor significativo a los activos de la información, de acuerdo con lo analizado se realiza la definición de los controles, metodologías y mecanismos de protección que permitan el mejoramiento continuo y la minimización de riesgos para la entidad, lo anterior basado en la norma ISO/IEC 27001:2013.

Se logrará establecer una metodología clara la cual permita gestionar el sistema de seguridad de la información de manera segura, precisa y oportuna, realizando una evaluación de los controles que comprende la ISO/IEC 27001:2013 a la IPS Garper Médica SAS, la implementación de este tipo de soluciones minimiza el riesgo en fraudes, manipulación y pérdida de información sensible en los sistemas informáticos en la clínica Garper Médica SAS.

La realización del análisis de riesgos y con la Identificación de fallas e incidencias, se logrará la mejora continua de la organización, preservando la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorgando a las partes interesadas confianza sobre la adecuada gestión.

La implementación de un SGSI es un elemento favorable para la empresa frente a la competencia, elevando su imagen a la ejecución de más contratos, la definición de la política y los objetivos de seguridad de la información, así mismo lograr su aplicabilidad, previniendo y reduciendo efectos indeseados por pérdida de información.

Teniendo identificadas las opciones adecuadas de tratamiento del riesgo de la seguridad de la información, será mucho más eficiente la toma de decisiones y concientización a todos los colaboradores de Garper Médica, sobre los beneficios

de una mejora continua y los inconvenientes de no cumplir con los requisitos del sistema de gestión de la información, manteniendo una información documentada y actualizada de acuerdo con los lineamientos establecidos para la aplicabilidad de la norma.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar la etapa de planeación de un sistema de gestión de seguridad de la información para el área de tecnología a través de un proceso integral para la IPS Garper Médica SAS basado en el estándar ISO/IEC 27001:2013 con el fin de proporcionar mayor seguridad, confiabilidad, disponibilidad e integridad sobre los activos de información.

3.2 OBJETIVOS ESPECÍFICOS

- Determinar el estado real de los lineamientos de seguridad que están implementados en la IPS Garper Médica en el estándar ISO/IEC 27001:20013, para identificar el nivel de madurez tecnológica y lograr el punto de referencia para una buena implementación del SGSI.

- Analizar los riesgos asociados a los activos que pertenecen al proceso de mejora en la IPS Garper Médica, mediante la metodología magerit, para la identificación del impacto que tendrían los posibles riesgos y de esta forma tomar las medidas oportunas para su mitigación.

- Elaborar políticas de seguridad de la información que permitan gestionar los riesgos y amenazas, con el fin de prevenir algún evento cibernético y de esta forma se pueda tener tranquilidad en el manejo y seguridad de los sistemas críticos de información de la IPS Garper Médica SAS.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Importancia de un Sistema de gestión de seguridad de información en Garper Médica. Teniendo en cuenta que Garper Médica no cuenta con un SGSI, por tanto hace que su sistema sea vulnerable a riesgos y ataques cibernéticos, generando varias dificultades en sus procesos, la IPS ha tenido muchos problemas como pérdida de información, manipulación inapropiada, falta de integración sobre algunos sistemas, llevando a que el personal no tenga un control, centralización y trazabilidad de sus procesos, no cuenta con políticas en manejo de la información, adicionalmente no cuenta con una trazabilidad sobre el reporte de incidentes presentados, todo lo anterior hace que la IPS Garper Médica presente factores negativos a nivel de seguridad informática e infraestructuras críticas.

La aplicabilidad del SGSI se tendrá que fortalecer y apoyar el área de TIC – Tecnología de la información y comunicación, con el fin de controlar prever y asegurar sus sistemas y su información todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad del dato, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital [8].[YN1]

Uno de los valores más importantes de los activos de información, se encuentran asociados a riesgos y amenazas que detonan una amplia tipología de

[8] NEIRA LOPEZ, Agustín. ISO 27000. 2021, de Lead Tutor ISO 27001 [Sitio web]: [Consulta: 20 de diciembre]. Disponle en: https://www.iso27000.es/sgsi.html.

vulnerabilidades. La seguridad de estos activos de información está en función de la correcta gestión de una serie de mecanismos como: la capacidad, la elaboración de un plan de contingencia frente a las eventualidades, el análisis de riesgos, las capacidades, el grado en que se involucra la Dirección, las trasformaciones en seguridad y el grado de implementación de controles.

Un SGSI (Sistema de Gestión de Seguridad de la información), son un conjunto de políticas, directrices, procedimientos, recursos y acciones que son dirigidos colectivamente por una organización, en la exploración de salvaguardar sus activos de información principales y críticos[9].

Un SGSI basado en la Norma internacional ISO/IEC 27001:2013, se puede definir como una guía sistémica para implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos a nivel productivos, comerciales o de servicio[10].

Cada organización puede ampliar e integrar en un SGSI las tres características básicas iniciales de definición de la seguridad a otras adicionales como suelen ser la autenticidad, trazabilidad, no repudio, adaptabilidad, entre otras, según se considere oportuno para cumplir con los requerimientos internos y/o externos aplicables en cada actividad y organización.

La importancia de implementar un SGSI en una organización radica en que toda empresa precisa cuidar y proteger los activos de información y la mejor forma de hacerlo es implementando un SGSI ya que este trae varios beneficios como es:

- Disminución del riesgo de pérdida, hurto o corrupción de información con la

[9] NORMAS-ISO.COM. ISO 27001 SEGURIDAD DE LA INFORMACIÓN. [Sitio web]. [Consulta: 15 de abril de 2020]. Disponible en: https://www.normas-iso.com/
[10] NORMAS-ISO.COM. ISO 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN [Sitio web]. [Consulta: 15 de abril de 2021]. Disponible en: https://www.normas-iso.com/iso-27001/

posibilidad de continuar la acción después de un incidente grave.

- Gestionar los activos de información de manera organizada que proporcione la mejora continua y el ajuste a los objetivos organizacionales en cada momento sin una compra sistemática de productos y tecnologías.
- Establecimiento de una metodología de gestión de la seguridad clara y estructurada cumpliendo con los reglamentos, la legislación y las exigencias de la industria.
- Confianza y satisfacción de las exigencias de seguridad de la información por los clientes y otras partes interesadas[11].

Los aspectos claves de un SGSI basado en la norma ISO/IEC 27001:2013, corresponde a una solución de mejora continua en la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización. Permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros. La norma ISO 27001 es un sistema basado en el enfoque del ciclo de mejora continua. Dicho ciclo consiste, en Planear, Hacer, Verificar y Actuar[12].

Los riesgos de seguridad informática de una organización realmente es un componente y una preocupación fundamental para toda empresa, es importante que las organizaciones fortalezcan sus mecanismos y protocolos de seguridad, ya que los ataques cibernéticos e informáticos están en alza día tras día, las incidencias de ciberseguridad se deben a errores humanos, siendo el foco de atención tanto ciberdelincuentes como trabajadores de la empresa.

---

[11] NORMAS-ISO.COM. ISO 27001, seguridad de la información .ISO 27001 gestión de la seguridad de la información. [Sitio web]. [Consulta: 15 de abril de 2021]. Disponible en: https://www.normas-iso.com/iso-27001/

[12] MINTIC. Guía para la implementación de seguridad de la información en una MIPYME. [Sitio web]. [Consulta: 15 de abril de 2021]. Disponible en:https://www.mintic.gov.co/gestionti/615/articles-482_Guia_Seguridad_informacion_Mypimes.pdf.

Estos riesgos y ataques de ciberseguridad representan millones en pérdidas, haciendo que la implementación de estrategias de seguridad informática sea algo prioritario y poco implementado en muchas empresas y organizaciones a nivel mundial[13].

Algunos comportamientos que provocan riesgos de ciberseguridad en las empresas son:

- Uso de Dispositivos externos en equipos corporativos: Si se va a utilizar dispositivos USB externos, lo ideal es que sean analizados o formateados para evitar que un Malware infecte los equipos corporativos.
- Uso de redes sociales en equipos corporativos: Acceder a perfiles en redes sociales, leer mensajes o descargar archivos posee una amenaza alta para la seguridad de los equipos empresariales.
- Uso inadecuado de dispositivos móviles de la empresa: Acceder a correos corporativos desde el móvil o conectarse a una red wi-fi pública significa un riesgo latente para datos tanto de clientes como de la empresa.
- Dejar equipos sin bloquear o sin cerrar sesión: Esto constituye un riesgo grave para la seguridad informática de la empresa, donde lo ideal es utilizar sistemas de bloqueo automático en los equipos, lo cual evitará que cualquier persona pueda usarlos.
- Descargar archivos desde correos personales o corporativos: Si se va a descargar archivos, lo ideal es que estos archivos sean analizados por el antivirus.
- Subir archivos a la nube sin cifrar: Lo mejor en estos casos así sean servicios cloud gratuitos o de pago es que los documentos siempre estén protegidos o cifrados.

[13] ESCUELA EUROPEA DE EXCELENCIA. Gestión de Riesgos: Identificación y Análisis de Riesgos. [Sitio web]. [consulta: 15 de abril de 2021]. Disponible en:https://www.escuelaeuropeaexcelencia.com/2016/07/gestion-de-riesgos-identificacion-analisis/

- Mala gestión de contraseñas y de permisos: Es importante que los permisos de acceso a determinada información no estén al alcance de todos.
- Falta de copias de seguridad: Esta práctica debería ser habitual en las empresas, lo cual evitará pérdida total de información en caso de un incidente informático.
- Envío de correos masivos a clientes: Lo ideal es utilizar la copia oculta para no exponer la información de la lista de destinatarios.
- No informar los incidentes o problemas ocurridos en la empresa con los dispositivos o sistemas corporativos: Es deber de todo trabajador informar de este tipo de hechos, con lo cual se evitarán brechas de seguridad empresarial[14].

4.1.2 Principales amenazas en organizaciones del sector salud. Las principales amenazas en organizaciones del sector salud se derivan por la ausencia de mecanismos de seguridad definidos para la conservación de integridad de la información, la existencia de Software en cualquier organización hace necesario llevar un control, una aplicabilidad de medidas que prohíban el acceso no autorizado o la deliberada edición de información y más cuando esta información corresponde a datos sensibles como es la Historia Clínica.

Existen varias amenazas al interior de las organizaciones del sector salud, correspondientes al robo de identidad médica, comercialización de información en mercado negro, acceso no autorizado a la información del paciente y divulgación, teniendo en cuenta que muchas organizaciones del sector salud ya se encuentran en la automatización de procesos para generar ambientes más productivos,

[14] SANTIAGO, Enrique Javier, SANCHEZ Jesús. Riesgos de ciberseguridad en las empresas. Universidad Alfonso X el Sabio, Escuela Politécnica Superior. Villanueva de la Cañada Madrid. [Consulta: 10 de septiembre del 2021]. Disponible en http://www.uax.es/publicacion/riesgos-de-ciberseguridad-en-las-empresas

interoperabilidad a nivel de historias clínicas, manejo de tecnología de punta en equipos biomédicos y a su vez el desarrollo de interfaces para el manejo centralizado de información, surge la necesidad de la aplicabilidad de controles basado en la ISO 27001.

Por otra parte, estas amenazas también se identifican en procesos administrativos como por ejemplo: la filtración de información como es tarifas, procesos, protocolos, guías, historia clínica, datos personales, costos asociados a los activos o inclusive divulgación de honorarios médicos, venta de datos a ciberdelincuentes, mal uso de los datos que generan un riesgos alto a nivel de seguridad del paciente, todo lo anterior puede generar un impacto alto en procesos financieros y de la vida del paciente.

La pérdida de información es un riesgo latente en muchas organizaciones incluidas las del sector salud, estarán totalmente expuestas sino se implementan las estrategias para prevenir, controlar y mitigar los ataques que se puedan producir.

Los ataques de tipo ransomware pueden generar un efecto catastrófico para cualquier entidad de salud, ya que generaría una irrupción del historial clínico y administrativos, el costo para la restauración de los sistemas y recuperación de los datos será un proceso que generará traumatismos sobre los procesos asistenciales, administrativos y sobre todo en la privacidad y seguridad del paciente.

La formación, educación y concienciación en procesos de seguridad informática, son siempre una apuesta segura, el conocer como es el manejo y los posibles riesgos que se derivan del desconocimiento en la gestión de las buenas prácticas, será clave para la no afectación en incidentes de seguridad de la información, algunos escenarios que el sector salud y cualquier otra organización debe hacer frente para la mitigación de los riesgos y amenazas, son la fuga de información,

ataque por ingeniería social e infección por ransomware, como se expresaba en el texto anterior[15].

Analizando los diferentes escenarios de posibles amenazas se identifican tres formas en que pueden producirse estos incidentes de seguridad que afectan los datos de la organización los cuales se definen como: Accidental, intencionado o por medio de un ataque externo, de esta forma se denota que estas formas de incidentes se pueden generar acusa de debilidad en controles o inexistencia de estos[16].

4.1.3 Gestión de riesgos como mecanismo de disminución y prevención de amenazas en organizaciones del sector salud: La Gestión y análisis del riesgo cumplen un papel vital para la planeación e implementación de un SGSI, ya que con la valoración de los activos de información y análisis de cada posible riesgo y amenaza, se logra la toma de decisiones, implementación de controles y herramientas que permitan la mitigación o eliminación de posibles amenazas y riesgos, a través de metodologías permite la identificación, tratamiento bajo unos controles y salvaguardas, así mismo con la oportuna gestión de estas amenazas, se logra generar un método adecuado ante un impacto crítico que vulnere la integridad de los datos.

La gestión del riesgo aporta grandes beneficios y contempla objetivos importantes para el mejoramiento continuo de cualquier organización, sin nos centramos en entidades de salud, podemos analizar que el manejo y la concientización al personal es un problema que se encuentra expuesta las organizaciones, el personal es uno de los factores que genera más eventos de riesgos, ya que tienen acceso a los

[15] MINTIC.GOV. Guía de Gestión de Riesgos. Gestión y Privacidad de la Información. [Sitio web]. [Consulta: 15 de abril de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles5482_G7_Gestion_Riesgos.pdf

[16] INSTITUTO NACIONAL DE CIBERSEGURIDAD - INCIBE. Ciberseguridad para tu sector salud. SECtoriza2, [Sitio web]. [Consulta: el 12 de noviembre del 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sectoriza2-ciberseguridad-especifica-el-sector-salud

sistemas y pueden observan todo lo concerniente a la salud del paciente, será fundamental la implementación y socializaciones en los riesgos que puede llegar a generar el inadecuado uso de los datos, lo anterior ya que varias personas tienen acceso a información sensible, de esta forma las IPS deben implementar las políticas, aplicar los controles necesarios y generar una cultura organizacional que prohíba la divulgación de información, manejo y reserva del tratamiento o diagnósticos del paciente, la filtración de información o la pérdida de información son eventos que generan un impacto critico en organizaciones de salud.

Para el análisis de estos riesgos y lograr el desarrollo de este proyecto aplicado se emplea la metodología Magerit.

4.2 MARCO CONCEPTUAL

- Seguridad de la información: Corresponde a las medidas y técnicas para lograr salvaguardar los activos de información de cualquier organización, dando un valor significativo a cada uno, asegurando la integridad, confidencialidad y máxima protección, de esta forma se logra una mayor confiabilidad[17].

- Riesgo: El riesgo se puede definir como la probabilidad de sufrir daños o pérdidas, en el contexto de los SGSI, los riesgos de seguridad de la información se pueden expresar como la incertidumbre o la posibilidad de que las amenazas aprovechen las vulnerabilidades de un activo de información y de esta forma pueden causar daños a la organización[18].

- Amenaza: La amenaza corresponde a la causa potencial de un incidente no

[17] NECTEC.COM. ¿Qué es seguridad informática? [Sitio web]. [Consulta: el 15 de abril de 2021]. Disponible en: https://www.netec.com/que-es-seguridad-informatica.
[18] ESCUELA EUROPEA DE EXCELENCIA. Gestión de Riesgos: Identificación y Análisis de Riesgos. [Sitio web]. [Consulta: el 15 de abril de 2021]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2016/07/gestion-de-riesgos-identificacion-analisis/

deseado que puede causar daños a un sistema o a una organización. Una amenaza es algo puede o no ocurrir, pero tiene el potencial de causar daños graves[19].

- Vulnerabilidad: Una vulnerabilidad es la debilidad de un sistema de la información que pone en riesgo la seguridad del sistema, permitiendo a un atacante comprometer la integridad, disponibilidad o confidencialidad del sistema informático[19]**.**

- SGSI: El sistema de gestión de seguridad en la información (SGSI) es el elemento más importante de la norma ISO 27001 que consta de una serie de políticas, de procedimientos y directrices con el fin de gestionar, implementar, operar, monitorear, revisar y mejorar, los activos de la información, controlando y evaluando los riesgos de seguridad de la información[20].

- Metodología de análisis de riesgo: Corresponde a las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Sobre el proceso de gestión del riesgo se aplican las políticas de gestión de procedimientos y practicas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgos[21].

- Planificación SGSI: Teniendo en cuenta la norma ISO 27001 en la cláusula 4 se indica la importancia de conocer la organización y su contexto, de manera que

[19] ISOTOOLS EXCELLENCE. ISO 27001 y la gestión de los riesgos de la seguridad de la información en PYMEs. 2021, de PMG SSI [Sitio web]. Disponible e: https://www.pmg-ssi.com/2014/08/iso-27001-gestion-riesgos-seguridad-informacion-pymes/

[20] ISO27000.ES. Temas relacionados con los SGSI y la seguridad de la información. [Sitio web]. [Consulta: el 15 de abril de 2021]. Disponible en: http://www.iso27000.es/

[21] DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: © Ministerio de Hacienda y Administraciones Públicas.

la definición del sistema de gestión tenga en cuenta los propios objetivos de la organización, con los que deberá alinearse la gestión de la seguridad de la información, por este motivo se realiza un reconocimiento de la organización[22].

- Norma ISO/IEC 27001: Es una norma desarrollada por la organización internación de normalización, con el objetivo de apoyar en la gestión de seguridad de la información, esta norma contiene detalles correspondientes a los principales requisitos que debe contener un Sistema de gestión de seguridad de la información[23].

4.3 MARCO CONTEXTUAL

La seguridad siempre ha sido una preocupación por parte de los directivos y gerentes de una organización, la trascendencia de esto se ha venido identificando por el crecimiento de las entidades y así mismo el volumen de la información crece. La información es un elemento bastante apreciable e interesante para cualquier recurso al interior o exterior de la organización; sin embargo, la frecuencia de los ataques es cada vez mayor, si se aplicara una cultura que permita asegurar la información y se mantuvieran las buenas prácticas para la gestión de la seguridad de la información, se podría contemplar un gran porcentaje en minimización de riesgos informáticos.

A fines del año 2020 el ciberataque a una Clínica en Alemania, que, según la fiscalía, el ministerio de justicia, la policía y los técnicos informáticos concluyen que la causa de falla fue un ciberataque, afectando a 30 servidores del centro médico, manteniendo cerrada su atención por 13 días, sin lograr acceder a la información

[22] NORMAS-ISO.COM. ISO 27001 seguridad de la información .ISO 27001 gestión de la seguridad de la información. [Sitio web]. [Consulta: el 15 de abril de 2021] Disponible en: https://www.normas-iso.com/iso-27001/

[23] ISO27000.ES. Temas relacionados con los SGSI y la seguridad de la información. [Sitio web]. [Consulta: el 15 de abril de 2021] Disponible en: http://www.iso27000.es/

almacenada, generando pérdidas grandes, fueron atacadas con variantes de ransomware (secuestro de datos)[24].

Los hospitales o clínicas son objetivo de los criminales del ransomware porque sus datos son esenciales y su ciberseguridad no está bien trabajada, algunas IPS no disponen de presupuesto para ciberseguridad y la tratan de manera tradicional, como por ejemplo, carpetas compartidas sin ningún tipo de restricción, manejo de historias clínicas de forma manual, no cuenta con un Sistema de gestión de calidad que permita almacenar todos los manuales, formatos, procedimientos que son importante ante auditorias por parte de las secretarías de salud, de esta forma están muy expuestas y poco preparadas para contener un ataque.

Conocimiento de la organización y de su contexto

Nombre de la empresa: Garper Médica Sas

Razón Social: García Pérez Médica y Compañía SAS.

Es una Institución Prestadora de Servicios de Salud de alta complejidad, su actividad principal es el manejo de pacientes con cualquier tipo de patología del aparato cardiovascular y circulatorio, incluyendo el intervencionismo periférico, neuro intervencionismo y manejo endovascular.

Actualmente Garper Médica SAS trabaja en la implementación de un sistema de gestión de la seguridad en la información que cumpla con los requisitos la norma ISO/IEC 27001:2013 con el objetivo de aumentar la confianza de sus clientes y construir medidas de control para la reducción los riesgos[25].

[24] CARBAJOSA Ana, Ciberataque a un hospital alemán en tiempos de pandemia. [Sitio web]. [Consulta: el 15 de abril de 2021] Disponible en: https://elpais.com/internacional/2020-10-03/ciberataque-a-un-hospital-aleman-en-tiempos-de-pandemia.html.
[25] GARPER MÉDICA SAS. Reseña histórica. [Sitio web]. [Consulta: 02 de Mayo del 2021], Disponible en: https://www.garperMédica.com/nosotros_resena_historica.html

Objetivos de negocio:

- Mejorar el sistema de gestión de calidad y cumplimiento de los requisitos aplicables, para garantizar la prestación de servicios médicos cardiovasculares en beneficio de los usuarios, colaboradores, socios, proveedores y la comunidad en general; basados en un talento humano competente y comprometido con la optimización de los recursos.
- Instituir una cultura de seguridad del paciente: cultura justa, educativa y no punitiva pero que no fomente la irresponsabilidad.
- Educar, capacitar, entrenar y motivar al personal para la seguridad del paciente.
- Protección de activos.
- Mantener los criterios de disponibilidad integridad y confidencialidad de la información.
- Concientización a la necesidad de la seguridad de la información.

El crecimiento de la organización ha llevado a que Garper Médica SAS implemente un SGSI, con el fin de mejorar sus procesos, garantizando ante todo la confidencialidad de la información, mantenimiento un sistema centralizado, unificado, desarrollando una política clara para la organización y así evitar una manipulación inapropiada de información y tal vez pérdidas significativas de la misma.

4.4 MARCO HISTÓRICO

4.4.1 Reseña histórica: Garper Médica es una institución prestadora de servicios de salud (IPS) de alta complejidad, constituida en el año 1994, cuya actividad principal es el manejo del diagnóstico y tratamiento de los pacientes con cualquier tipo de patología del aparato cardiovascular y circulatorio. En el año 2014 Garper Médica S.A.S. inaugura en Tunja (Boyacá), el programa de cardiología integral más moderno del Departamento, instalando el tercer Angiógrafo. En el año 2020 se inicia operación en sede calle 93 Bogotá para atención prioritaria y vacunación de Covid-19, así mismo en Tunja se inaugura una nueva sede para atención prioritaria y primer nivel de atención, para este año 2021 se tiene proyectado a corto plazo la instalación de un TAC en clínica de la calle 27[26].

Hoy día Garper Médica cuenta con dos salas de procedimientos en Bogotá, equipos de última generación para Ecocardiografía, Holter, Prueba de Esfuerzo, Electrocardiografía, Rehabilitación Cardiaca y Recuperación.

Misión: Garper Médica S.A.S. es una institución prestadora de servicios de salud, especializada en el área cardiovascular no invasiva, intervencionista y quirúrgica de alta complejidad[27].

Visión: Ser una institución reconocida por su excelencia y liderazgo en la prestación de servicios médicos especializados en el área cardiovascular.

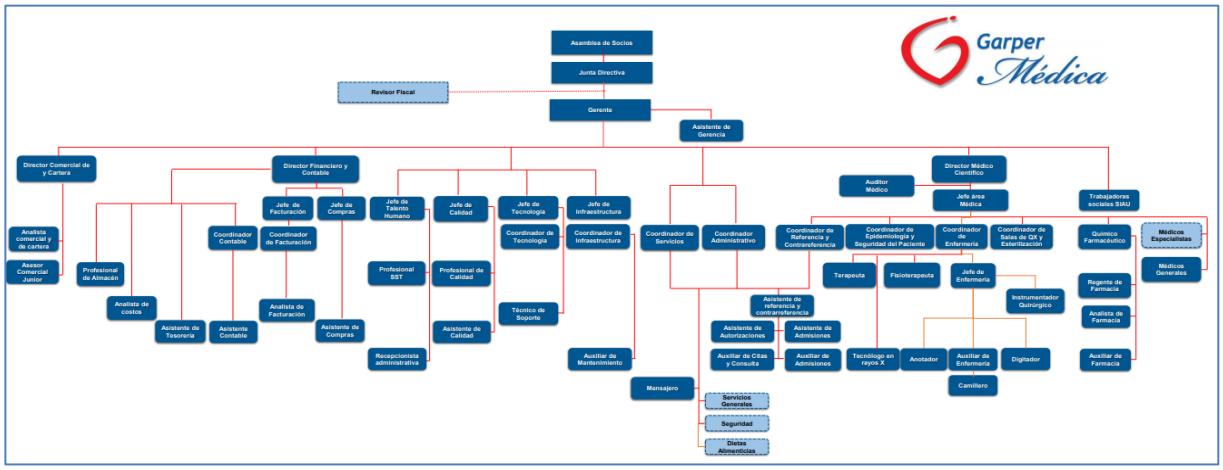
4.4.2 Estructura organizacional: En la ilustración 1 se muestra cada una de las áreas que confirman garper médica y su dependencia.

---

[26] GARPER MÉDICA SAS. Reseña histórica. [Sitio web]. [Consulta: 02 de Mayo del 2021], Disponible en: https://www.garperMédica.com/nosotros_resena_historica.html

[27] GARPER MÉDICA SAS. Reseña histórica. [Sitio web]. [Consulta: 02 de Mayo del 2021], Disponible en: https://www.garperMédica.com/nosotros_quienes_somos.html

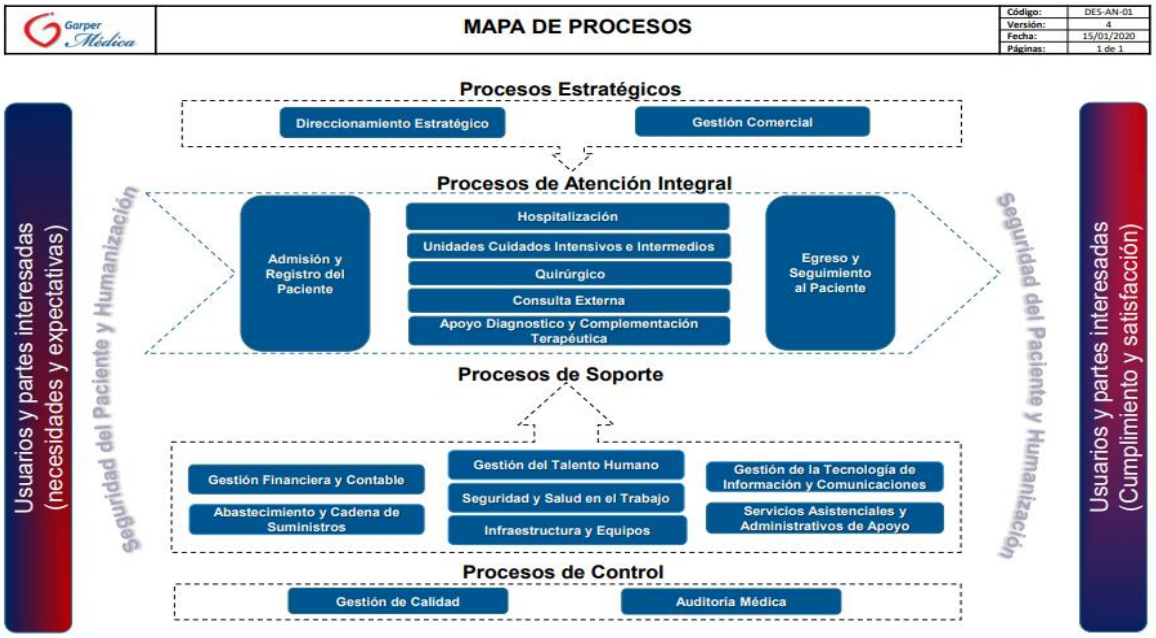
Ilustración 1. Estructura Organizacional Garper Médica SAS



Fuente: Garper Médica SAS. Información en línea - Privado (Fecha de registro 2020-02-17) Disponible en https://www.garperMédica.com/intranet/gestion_sistema_calidad/gestion_sistema_calidad.php?pagina=1&id=null&folder=c3RvcmFnZS8zUDc1LXZfOFNKQktPbEVGUzNkQy9mV1NqSExjUVp5ci1hUWd1dEJTci8=

4.4.3 Mapa de proceso: En la ilustración 2 corresponde al mapa de procesos de Garper Médica se indican los tipos de procesos, como es el estratégico, proceso de soporte y el proceso de control, de esta forma el área de tecnología se en cuenta en el proceso de soporte.

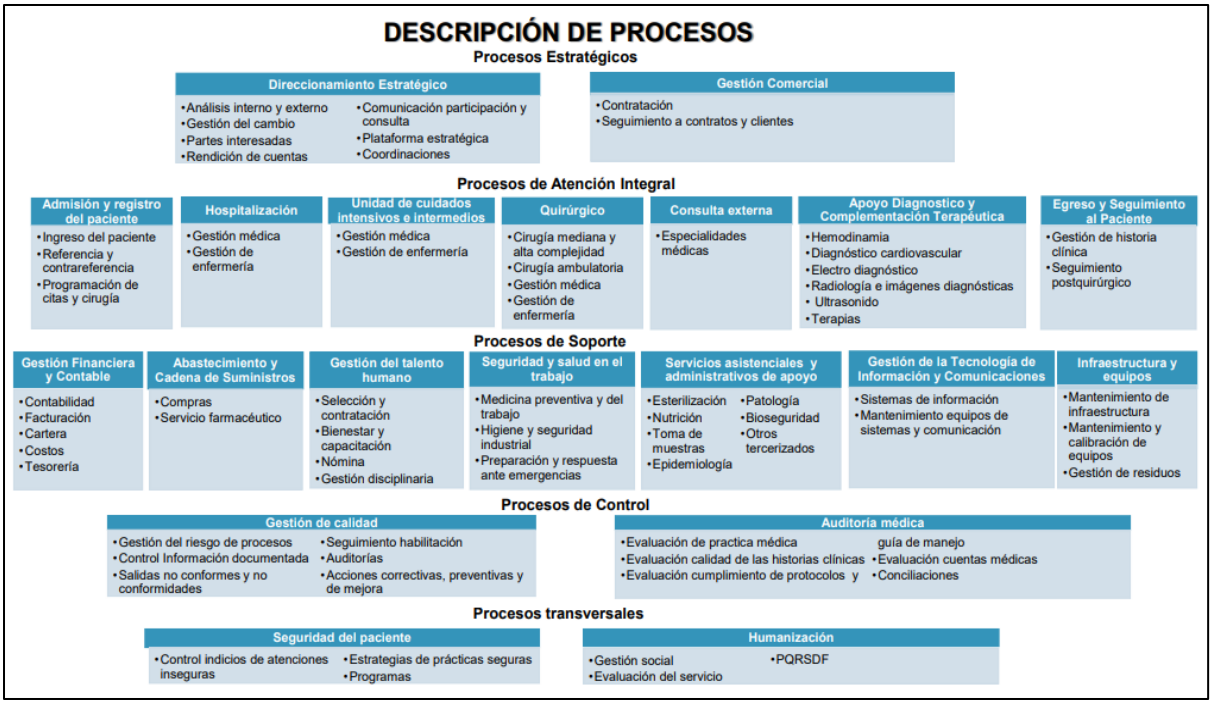
Ilustración 2. Mapa de procesos Garper Médica



Fuente: Garper Médica SAS. Información en línea - Privado (Fecha de registro 2020-02-17) Disponible en https://www.garperMédica.com/intranet/gestion_sistema_calidad/gestion_sistema_calidad.php?pagina=1&id=null&folder=c3RvcmFnZS8zUDc1LXZfOFNKQktPbEVGUzNkQy9mV1NgSExjUVp5ci1hUWd1dEJTci8=

4.4.4 Descripción de proceso: En la ilustración 3 se describe por cada proceso algunas de sus funciones más relevantes.

Ilustración 3. Descripción de procesos Garper Médica



Fuente: Garper Médica SAS. Información en línea - Privado (Fecha de registro 2020-02-17) Disponible en https://www.garperMédica.com/intranet/gestion_sistema_calidad/gestion_sistema_calidad.php?pagina=1&id=null&folder=c3RvcmFnZS8zUDc1LXZfOFNKQktPbEVGUzNkQy9mV1NqSExjUVp5ci1hUWd1dEJTci8=

4.5 ANTECEDENTES

Para el desarrollo de este proyecto se tomaron algunos trabajos que tenían similitud con los objetivos propuestos como ayuda en el diseño de la etapa de planeación del sistema de gestión de seguridad en la información, de esta forma se describen algunos proyectos.

Proyecto ‘Diseño de políticas de seguridad de la información para la unidad de tecnología de la cámara de comercio de Cúcuta’ trabajo de grado realizado por María Carolina Duarte Martínez, a la UNAD, presentado como requisito para optar al título de Especialista en Seguridad Informática en el año 2019 , en este proyecto se explica la metodología de análisis de riesgo utilizada para dicho proyecto Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), donde hace énfasis en que esta metodología plantea dentro del análisis de riegos la identificación de los activos de información, las salvaguarda, las amenazas y vulnerabilidades de un sistema de información, el método utilizado sirve como guía donde se detalla la metodología de análisis de riesgos incluyendo listado de elementos tales como activos, dimensiones de seguridad, criterios de valoración de los activos, amenazas típicas y salvaguardas, contiene algunas técnicas útiles para el análisis de riesgos, tales como tablas, análisis costo-beneficio, histogramas, gráficas en barras, entre otras, esta metodología y análisis será de gran valor para el proyecto[27].

Proyecto ‘Implementación de un sistema de gestión en seguridad de la información para el hospital agua de dios’, trabajo de grado presentado Andrés Cárdenas Hernández, Daniel Hernán Castañeda Montes, a la Universidad Piloto De Colombia en el Año 2018 para obtener el título de Especialista en Gerencia de Proyectos. Este proyecto al ser aplicado para una IPS ayuda a tener una orden y una idea de los activos que serán importantes evaluar así mismo se implementa el diagrama de Gantt, donde se ve la representación del proyecto y evidencia de su ruta crítica[28].

Proyecto ‘Plan de implementación del SGSI basado en la norma ISO 27001:2013

[27] DUARTE, María Carolina. Diseño de políticas de seguridad de la información para la unidad de tecnología de la cámara de comercio de Cúcuta. Trabajo de grado. Cúcuta: UNAD, Facultad de Ingenierías, Departamento de Seguridad informática, 2019.
[28] CASTAÑEDA, Daniel Hernán, CÁRDENAS Andrés, Implementación de un sistema de gestión en seguridad de la información para el hospital agua de dios, Universidad Piloto De Colombia en el Año 2018.

Proponen' Paula Andrea Maya Arango. Universidad Oberta de Catalunya. "Este trabajo describe los objetivos, alcance, expectativa del SGSI y metodología asociada a la definición, planificación, identificación y creación del modelo de seguridad de la información para la organización Textilera SA, con base en la ISO 27001: 2013; partiendo de la comprensión de la organización desde la perspectiva de los procesos críticos, ejecución de diagnóstico de seguridad de la información, identificación de vulnerabilidades y amenazas clave, aplicación de una metodología de gestión de riesgos seguridad de la información, planificación de planes de tratamiento de riesgos y generación del marco documental del sistema de gestión de seguridad de la información para Textiles SA El objetivo principal es sentar las bases del proceso de mejora continua y proponer medidas para minimizar el impacto de las acciones de riesgos potenciales. El proyecto propone el establecimiento de las bases para la implementación de un SGSI", este proyecto nos aporta una base o guía clara, ya que básicamente nos muestra cómo desarrollar e implementar un SGSI para la organización Textilera SA[29].

Proyecto, 'Informe de auditoría sobre el sistema de gestión de seguridad de la información del fondo rotatorio de la policía'. Presentado por Oscar Diaz. Fondo Rotatorio de la policía. "Este trabajo es un ejemplo claro de auditoria sobre el sistema de la información del fondo rotatorio de la policía. Nos muestra paso a paso como se realizó esta misma" Aportes: El trabajo aportó una base o guía clara, ya que básicamente nos muestra cómo desarrollar e implementar una auditoría interna para el Fondo Rotatorio de la policía[30].

[29] MAYA ARANGO, Paula Andrea, Plan de implementación del SGSI basado en la norma ISO 27001:2013. Universidad Oberta de Catalunya 2016.
[30] DIAZ, Oscar, Informe de auditoría sobre el sistema de gestión de seguridad de la información del fondo rotatorio de la policía'. Fondo Rotatorio de la policía Año de Publicación 2015.

4.6 MARCO LEGAL

En relación con la seguridad en la información aplicabilidad de las siguientes leyes serán de gran importancia:

4.6.1 Ley 1273 de 2009. Ley de delitos informáticos en Colombia, donde se modifica el código penal y se crea un bien jurídico tutelado, denominado protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, teniendo en cuenta los pilares fundamentales confidencialidad, integridad y la disponibilidad de los datos y de los sistemas informáticos[31].

4.6.2 Norma ISO/IEC 27001: Donde se adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI, consistente en medidas orientadas a proteger la información, contra cualquier amenaza, de forma que se garantice en todo momento la continuidad de las actividades de la empresa El riesgo se evalúa mediante la identificación de amenazas y vulnerabilidades y luego se establece la probabilidad y el impacto de cada riesgo, la aplicabilidad de la norma será fundamental para logra analizar de forma detalladas todos los aspectos que se deben tener en cuenta para la gestión de la seguridad de la información en Garper Médica, detallando los términos y definiciones para que la planeación se haga de una forma enfocada y alineada a los objetivos propuestos[32].

[31] COLOMBIA. CONGRESO DE LA REPUBLICA. ley 1273 de 2009. [Consulta: el 05 de enero del 2021] Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado. Diario Oficial. Bogotá: El Congreso, 2009. 2 p

[32] ISO 27000.ES. El portal de ISO 27001 en español. [Sitio web]. [Consulta: el 16 de mayo del 2021]. Disponible en: http://www.iso27000.es/iso27000.html

4.6.3 La Ley 1581 de 2012: Por la cual se dictan disposiciones generales y la prohibición de transferencia de datos personales velando por la protección de los mismos, esta ley tiene por objeto “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales, Garper Médica tiene definido el reglamento respecto a las de políticas y procedimientos de protección de datos personales, antes de proceder con el envío de la información se debe diligenciar la respectiva autorización de transferencia de datos[33].

4.6.4 Norma ISO/IEC 27002: Se estable la descripción de controles correspondientes a seguridad de la información esta norma fue publicada en Julio 01 de 2007, el objetivo principal es establecer, implantar, mantener y mejorar de forma continua la seguridad de la información, compuesta por 11 dominios, 39 objetivos y 113 controles[34].

Esta norma se centrada en las buenas prácticas para la gestión de la seguridad de la información, genera beneficios como es concientización sobre la seguridad de la información, un mayor control de los activos sensibles, brindar un enfoque para la implementación de políticas de control, genera una oportunidad para identificar y corregir puntos débiles, se logra una mejor organización en los procesos.

4.6.5 Norma ISO/IEC 27005: Se adoptan actualizaciones respecto a requisitos de la norma ISO/IEC 27001:2013, diseñada para ayudar a la aplicación satisfactoria de la seguridad con enfoque en gestión de riesgo[35].

---

[33] COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1377 (23, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá D.C. El Ministerio. 2013.

[34] ISO27000.ES. Serie "27000". Guías de referencia útiles para la implantación, mantenimiento, auditoría y certificación de los Sistemas de Gestión de la Seguridad de la Información. [Sitio web]. [Consulta: el 11 de noviembre de 2021]. Disponible en: http://www.iso27000.es/iso27000.html

En el numeral 6 se observa una visión general de los procesos de gestión del riesgo en la seguridad de información, esta gestión debe contribuir en la identificación y valoración de los riesgos en términos de consecuencias y probabilidad de ocurrencia, lo logra definir la priorización de las acciones para reducir la ocurrencias de los riesgos, define una eficacia del tratamiento de los riesgos, ya que se establece un monitoreo y revisión de los procesos de gestión, adicionalmente se contribuye en la educación a los directores y a todo el personal respecto de los riesgos y acciones que se toman para su mitigación.[35]

[35] NORMAS-ISO.COM. ISO 27001 SEGURIDAD DE LA INFORMACIÓN. [Sitio web]. [Consulta: el 15 de abril de 2020]. Disponible en: https://www.normas-iso.com/

5 DISEÑO METODOLÓGICO

La metodología para lograr alcanzar los objetivos del proyecto para la IPS Garper Médica, es la metodología aplicada, la cual consiste en planificar los objetivos propuestos sobre el proyecto, logrando analizar al detalle todas aquellas vulnerabilidades, amenazas, seleccionando controles para lograr diseñar la etapa de planificación de un SGSI, para el manejo eficiente y confidencial de los procesos internos de la IPS **Garper Médica SAS,** esta metodología tendrá en cuenta el marco de referencia de la norma ISO/IEC 27001:2013, que especifica los requerimientos y actividades que se deben desarrollar para la planificación del SGSI[36].

Durante el desarrollo del proyecto, la metodología de investigación aplicada permite un análisis de la problemática y puesta en marcha de los beneficios al aplicar un SGSI.

Se inició realizando la evaluación de los controles teniendo en cuenta la Norma ISO/IEC 27001:2013, se analizó los resultados de estos controles de acuerdo a las técnicas de recolección de información, se realizó el inventario de los activos teniendo en cuenta la clasificación e identificación de cada uno con base en la metodología seleccionada Magerit, se aplica la valoración de las cinco dimensiones de la seguridad para cada activo (confidencialidad, integridad, disponibilidad, autenticidad y Trazabilidad).

Con la identificación de los activos y analizando los riesgos asociados a los activos de la información, verificando al detalle todas aquellas vulnerabilidades y riesgos asociados a la integridad de la información, se desarrolla una cuadro con la valoración de estos activos y evaluación de controles, de esta forma se confirma si cumple o no con las condiciones generales en que se encuentra la información,

[36] NORMAS-ISO.COM. ISO 27001 SEGURIDAD DE LA INFORMACIÓN. [Sitio web]. [Consulta: el 15 de abril de 2020]. Disponible en: https://www.normas-iso.com/

luego se determina el estado real en cuanto a lineamientos de seguridad que se tiene implementado, con el fin de definir un plan de tratamiento del riesgo aplicando una guía de buenas prácticas.

Se propuso una política de seguridad de la información que permita gestionar los riesgos, cumpliendo con el deber de custodiar la información y dando como beneficio la confidencialidad, integridad y disponibilidad para el mejoramiento continuo de los procesos al interior de Garper Médica.

5.1 FASES METODOLÓGICAS

Según los requerimientos de la norma ISO/IEC 27001:2013 para la planificación del SGSI se establecen las fases necesarias para el desarrollo del proyecto, las cuales se representan en el cuadro 2.

Cuadro 2. Fases iniciales para la implantación del SGSI

Diagnóstico del SGSI	Preparación del SGSI	Planificación del SGSI
Identificación del nivel de madurez de la entidad, Conocer los activos y recursos a proteger, evaluar la viabilidad y efectividad de los controles, Identificar el nivel de riesgo.	Conocer el contexto de la organización y definición de alcance y la política del SGSI.	Valorar el riesgo, definir planes de tratamiento, establecer el marco de la norma o leyes de SI y lineamientos para su gestión.

Fuente: Elaboración Propia

5.2 POBLACION Y MUESTRA

Se define la población que confirma el área de Tecnología de Garper Médica con un total de 4 personas, de las diferentes sedes de la Entidad:

- Cargo: Jefe de Tecnología. Cantidad personas: 1
- Cargo: Coordinador de Tecnología. Cantidad: 1
- Cargo: Técnico en Sitio. Cantidad: 1
- Cargo: Técnico en Sitio. Cantidad: 1

5.3 TÉCNICAS PARA RECOLECCIÓN DE INFORMACIÓN:

- Inspección
- Observación
- Entrevistas
- Documentación existente respecto al SGSI.

Estas herramientas que son esenciales para lograr la identificación de lo que se desarrolló de esta forma se maneja la técnica de inspección, la cual consiste en visitar a la entidad, observar los procesos, entrevista al Gerente y a la Jefe de Tecnología con el fin de dimensionar el proyecto y tener una visual más completa y personalizada de la estructura informática, conductas de los funcionarios que hacen parte del área de Tecnología.

6 ESTADO REAL DE LOS LINEAMIENTOS DE SEGURIDAD QUE ESTÁN IMPLEMENTADOS EN LA IPS GARPER MÉDICA EN EL ESTÁNDAR ISO/IEC 27001:2013, PARA IDENTIFICAR EL NIVEL DE MADUREZ TECNOLÓGICA Y LOGRAR EL PUNTO DE REFERENCIA PARA UNA BUENA IMPLEMENTACIÓN DEL SGSI

A continuación, se presentan los objetivos que se desarrollaron de acuerdo con unas actividades en función de lograr el cumplimiento a la etapa de planeación de un sistema de Gestión de seguridad de la información a través de un proceso integral para el área de Tecnología de la IPS Garper Médica SAS basados en el estándar ISO/IEC 27001: 2013.

6.1 DETERMINAR EL ESTADO REAL DE LOS LINEAMIENTOS DE SEGURIDAD QUE ESTÁN IMPLEMENTADOS EN LA IPS GARPER MÉDICA EN EL ESTÁNDAR ISO/IEC 27001:2013, PARA IDENTIFICAR EL NIVEL DE MADUREZ TECNOLÓGICA Y LOGRAR EL PUNTO DE REFERENCIA PARA UNA BUENA IMPLEMENTACIÓN DEL SGSI.

La identificación de los dominios y evaluación de controles, llevan a un alcance de medición en la madurez tecnológica de la IPS Garper Médica, ya que, por medido de esta evaluación, permite en análisis de efectividad, ineficiencia o inexistencia de controles, sirviendo como punto de referencia para lograr la aplicabilidad de lineamientos de seguridad efectivos para la IPS, se desarrollan las actividades para su proceso de evaluación de la siguiente forma.

Actividad 1: Realizar la evaluación de los controles teniendo en cuenta la Norma ISO/IEC 27001:2013, se toma como guía algunos elementos que son importantes del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, con el fin de fortalecer el desarrollo del proyecto propuesto.

Se utilizó el “Instrumento de Evaluación MSPI” que fue desarrollado por el MinTIC con el objetivo de que las Entidades estatales puedan identificar el nivel de madurez

de la implementación de un Modelo de Seguridad y Privacidad de la Información[37]. Esta evaluación de controles se realizó en conjunto con la gerencia, el área de calidad, Jefe de Talento Humano y Jede de sistemas de Garper Médica, permitiendo establecer un análisis efectivo de los controles a nivel interno.

Una vez aplicado el instrumento de Evaluación MSPI donde se observa el nivel alcanzado en la evaluación de efectividad teniendo en cuenta cada dominio de la norma ISO 27001:2013, definidos en el cuadro 3 y representados de forma gráfica en la ilustración 4.

Cuadro 3. Evaluación de efectividad de controles

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	15	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	10	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	20	100	INICIAL
A.9	CONTROL DE ACCESO	10	100	INICIAL
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	35	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	15	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	15	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	15	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	25	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**17**	**100**	INICIAL

Fuente: Elaboración propia

[37] MINTIC.GOV. Guía de Gestión de Riesgos. Gestión y Privacidad de la Información. [Sitio web]. [Consulta: el 15 de abril de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles5482_G7_Gestion_Riesgos.pdf

Ilustración 4. Brecha anexos según la ISO 27001:2013

Fuente: Elaboración propia

Análisis de los resultados:

Teniendo en cuenta los resultados obtenidos se puede observar que Garper Médica se encuentra en una fase inicial ya que no cuenta con los controles suficientes, puede que se tengan establecidas algunas políticas de seguridad, pero no se establece realmente un documento que permita la socialización de estos, los procesos y controles no se aplican oportunamente, no existen procesos estandarizados ni una ruta claro del proceso que se debe realizar con cada procedimiento que se desee realizar.

A continuación, se detallan algunos aspectos que son relevantes y que se detectó sobre la evaluación de controles y que no permitió obtener un resultado mayor de evaluación:

- Políticas de seguridad de la información: No se cuenta con políticas claras,

debidamente establecidas, no se encuentran socializadas, tampoco se encuentra definida una asignación de responsabilidad, adicionalmente no se encuentran actualizadas estas políticas teniendo en cuenta el crecimiento de la organización, no se realiza la respectiva verificación de cumplimiento y aplicabilidad.

- No existen los documentos necesarios como el procedimiento en materia de protección de información.
- Organización de la seguridad de la información: No se cuenta con la definición de responsabilidades, existe un comité de Tecnología, sin embargo, este no se enfoca en procedimientos correspondientes a seguridad, control y protección de los activos de la información.
- No se cuenta con un Sistema de gestión de seguridad de la información.
- No existe un procedimiento para reporte de casos, eventos o incidentes de seguridad de la información.
- Seguridad de los recursos humanos: No existe un documento que defina las responsabilidades ante cualquier incidente de seguridad en la información provocada por un empleado,
- No existe un proceso disciplinario cuando se incurre en la violación a la seguridad de la información.
- Se cuenta con un documento que permite el registro de la firma que cumple con las normas de autenticidad de acuerdo con el decreto 2364 del 22 de noviembre del 2012, mediante el cual se reglamenta el artículo 7 de la ley 527 de 1999 sobre la firma electrónica, este punto es muy importante ya que todas las historias clínicas deben contener la firma del especialista que realiza dicha atención.
- Control de Accesos: Garper Médica a pesar de que cuenta con el protocolo establecido para la asignación de credenciales de ingreso a las diferentes plataformas, estos no se solicitan oportunamente, tampoco los permisos a las carpetas en red, adicionalmente no se informa oportunamente sobre la inactivación de usuarios para retirar los permisos, se cuenta con un Paz y salvo

para firma de las diferentes áreas y así mismo para que el departamento de tecnología firme y realice inmediatamente la inactivación, algunos usuarios no se presentan para la misma del mismo, de esta forma existe una base de usuarios activos en las diferentes plataformas que ya no laboran en la IPS.

- No se cuenta con la carnetización para todo el personal y de esta forma no se logra la identificación del funcionario para acceso a las instalaciones de la IPS.
- En la sede Tunja, se cuenta con un directorio activo que permite mantener el control de acceso a los documentos en red, sin embargo, no se cuenta con una política establecida ni protocolo de uso de este, este servidor de DA (Directorio activo), no se encuentra implementado en todas las sedes.
- En cuanto al acceso a la red, no se cuentan con los controles necesarios para denegación o acceso a las navegaciones o instalación de programas.
- Por otra parte, no se está realizando una revisión periódica respecto a los permisos sobre roles a los diferentes sistemas.
- Gestión de activos: No existe un inventario de activos de información, tampoco se encueta con un documento establecido para el manejo de estos, no se asegurará el manejo apropiado del activo cuando es eliminado o destruido.
- Solo se encuentra con el inventario debidamente registrado y rotulado de los activos físicos.
- Considerándose que los activos también corresponden al personal, no se tiene un archivo actualizado con el personal de directo por Garper, los que cuentan con contratos por OPS, y los que se encuentran con contratación por la temporal.
- La información no se cuenta debidamente clasificada, teniendo en cuenta los requisitos legales, de valor, criticidad y susceptibilidad para evitar la divulgación o modificación no autorizada.
- Criptografía: Dentro de las políticas existentes no existe una que corresponda al control criptográfico que permita la protección de la información, este es un riesgo sobre las transferencias de archivos y de esta forma sea ilegible evitando corrupción o perdida de información por algún ataque a nivel informático.

- Seguridad de las operaciones: No se cuenta con un documento donde se lleve un control de los cambios sobre los procedimientos nuevos establecidos o modificados.
- Seguridad de las comunicaciones: A pesar de que existen unos acuerdos de niveles de servicios con proveedores de Software no se cumplen y tampoco se realizan acciones para que se efectúen cambios y mejoras en un tiempo establecido según estos acuerdos contractuales.
- La Entidad no cuenta con procedimientos definidos para exigir los requisitos y responsabilidades de seguridad de la información.
- Gestión de incidentes de seguridad de la información: Garper Médica maneja una gestión de incidentes por medio del área de tecnología, sin embargo estos no se reportan oportunamente, se reportan por los medios incorrectos y los incidentes reportados no tienen los soportes necesarios y la claridad para gestionar oportunamente el incidente, tampoco se cuenta con un protocolo para aclarar los medios, metodologías para poder realizar esta gestión de incidentes y ser oportunos en la solución de estos.
- Dominio Aspectos de Seguridad de la Información de la Gestión de la Continuidad del negocio: Garper Médica cuenta con un plan de contingencia establecido, el cual cuenta con el procedimiento si se presenta algún evento en caso de fallo de la infraestructura informática, sin embargo, no se encuentra socializado.
- Es necesario incluir dentro del plan para la continuidad de las operaciones, el procedimiento necesario para la recuperación de la información, metodología aplicada y definir los procesos coherentes de acuerdo con los objetivos de continuidad.
- No se cuentan con planes de respuesta a incidentes y recuperación.
- Adquisición, desarrollo y mantenimiento de sistemas: Garper no cuenta con procedimiento para el cumplimiento de los requisitos de seguridad cuando se trata de nuevos desarrollos, ni con los parámetros necesarios para el cumplimiento de los controles de registros o de accesos.

- Relaciones con los proveedores: Garper Médica no cuenta con una política correspondiente a la seguridad de la información para las relaciones con los proveedores.

Por otra parte, se detallan los dominios más fuertes que tiene la IPS Garper Médica, dentro del análisis realizado, como son los, seguridad física y del entorno y cumplimiento.

- Seguridad física y del entorno: Garper Médica cuenta con el formato de bitácora para el ingreso a centros de Cableado y data center, cuenta con una cerradura, alarma, circuito cerrado de televisión y acceso exclusivo a personal autorizado.
- Existe un cronograma de mantenimientos de equipos informáticos físicos, así mismo se cuenta con el instructivo.
- Cumplimiento: Se lleva un control de los activos que no cuenta con licenciamiento, de esta forma verifica y adquiere licencia requeridas, se cuenta con el proceso documentado, se debe mejorar en la política publicada sobre el cumplimiento de la propiedad intelectual.

Por lo anterior se puede evidenciar que durante el proceso de diagnóstico de la IPS Garper Médica basado en la ISO 27001:2013 y utilizando el instrumento de Evaluación MSPI, se logró evidenciar aquellos dominios que tienen poco cumplimiento, debido a las diferentes falencias que se comentaron en el texto anterior; así mismo, se relacionó los que tienen mayor complimiento, logrando identificar que se debe seguir trabajando en la aplicabilidad de controles y buenas prácticas para el cumplimiento de la norma.

6.2 ANALIZAR LOS RIESGOS ASOCIADOS A LOS ACTIVOS QUE PERTENECEN AL PROCESO DE MEJORA EN LA IPS GARPER MÉDICA, MEDIANTE LA METODOLOGÍA MAGERIT, PARA LA IDENTIFICACIÓN DEL IMPACTO QUE TENDRÍAN LOS POSIBLES RIESGOS Y DE ESTA FORMA TOMAR LAS MEDIDAS OPORTUNAS PARA SU MITIGACIÓN.

Para lograr un análisis de riesgos asociados a los activos, fue necesario investigar sobre las diferentes metodologías existentes para articular la necesidad de la IPS, se continua con el inventario de activos de acuerdo a la metodología adoptada, se valora las dimensiones de seguridad sobre cada activo, se identifica las amenazas a las que se encuentran expuestos los activos, se realiza una valoración de las amenazas y riesgos, se analizan los resultados y de esta forma lograr alcanzar una identificación de riesgos de los activos de la IPS Garper Médica.

Actividad 1: Selección de metodología para que se adapte a las necesidades de la IPS.

Metodologías analizadas

OCTAVE: (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - evaluación operativa crítica, de amenazas, de activos y de vulnerabilidad, esta metodología se centra en los aspectos de riesgos operativos y prácticas de seguridad, Octave está compuesta por tres fases correspondientes a: la identificación de los perfiles de amenazas basados en activos, a la tipificación de la infraestructura de vulnerabilidades y al desarrollo de planes buenas prácticas y mitigación de riesgos a nivel de seguridad sobre los activos de información, enfocándose en los principios de integridad, confidencialidad y disponibilidad[38].

[38] CHRISTOPHER J. Alberts; OCTAVE catalogue of practices, *version 2.0, 2021,* Carnegie Mellon, Software Engineering Institute, pp.56-64

Como muchas metodologías Octave también ha brindado una evolución con el fin de enfrentar los retos de seguridad, basándose en la aplicación de la ley de transferencia y responsabilidad de seguro médico por sus siglas HIPAA.

Los elementos principales que maneja Octave son, las medidas de probabilidad, teniendo en cuenta un rango de frecuencias y un análisis de límite entre niveles de probabilidad, adicionalmente comprende procesos para la Identificación la perspectiva que tienen los directivos, se analiza la visión de la organización reconocimiento de activos, perfil de las amenazas, basado en un cuestionario de estrategias de protección, catálogo de buenas prácticas, técnicas, datos como es el organigrama, las políticas, las leyes y regulaciones que se deben adoptar de forma obligatoria y lista definiendo las prioridades de los activos con sus valores relativos, la identificación el conocimiento del área operativa, teniendo en cuenta la identificación de los riesgos, y definiendo programas de concientización, generación de aplicabilidad de políticas y procedimientos para la protección de los activos[39].

MEHARI: Method for Harmonized Analysis of Risk (Método para el análisis armonizado del riesgo) esta metodología fue desarrollada para apoyar a las personas que son responsables de la seguridad informática, por medio de un análisis de los factores principales de riesgos[40].

Los apartados de Mehari corresponden inicialmente al análisis de la seguridad, buscando las principales debilidades de la entidad, esta metodología también se centra en el diagnóstico para lograr asegurar la mitigación de los riesgos, utilizando planes basados en seguridad y en análisis de vulnerabilidad, contiene unos dominios, síntesis sobre los módulos y emplea el análisis de interés de seguridad,

[39] HURTADO, Martha. Gestión del riesgo Metodologías OCTAVE Y MAGERIT. Universidad Piloto de Colombia, *2020* 1, pp. 1-11.
[40] ESCUELA EUROPEA DE EXCELENCIA. Metodología Mehari para el análisis de Riesgos en SGSI. [Sitio web]. [Consulta: 11 de diciembre del 2021], Disponible en: https://www.pmg-ssi.com/2021/09/metodologia-mehari-para-el-analisis-de-riesgos-en-sgsi/

MAGERIT: Esta metodología fue desarrollada por el Ministerio de Hacienda y Administraciones Públicas de España, y corresponde a la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, contiene tres libros correspondientes a Métodos, catálogos y guías de técnicas, magerit maneja un marco de trabajo según la ISO 31000 correspondiente a: Principios, mandatos y compromiso, diseño del marco de trabajo, implementación de la gestión de riesgos, seguimientos y revisión del marco y mejora continua sobre el marco, lo cual genera un ciclo de mejoras y que los órganos de gobierno consideren y tomen disposiciones teniendo en cuenta los riesgos procedentes del uso de las tecnologías de la información.

Teniendo en cuenta las diferentes características de las metodologías expuestas en el anterior texto y sobre una previa investigación que permiten analizar y comparar la adopción de una de estas metodologías se realiza una evaluación cuantitativa de estas metodologías de análisis de riesgos, como se observa en el cuadro 4.

Evaluación de 1 a 3 donde 1 es la calificación menor y 3 la mayor calificación.

Cuadro 4. Evaluación de metodologías de análisis de riesgos

Características	Octave	Mehari	Magerit
Aplicación	2	3	3
Costo	2	3	3
Sencillez en la documentación	1	2	3
Disposición de profesionales entrenados	1	2	3
Recomendaciones a nivel de controles	3	1	3
Permite análisis tanto cualitativo como cuantitativo	3	3	3
Total	12	14	18

Fuente: Elaboración propia.

Acorde a la evaluación generada en el cuadro anterior el valor más alto corresponde a la metodología Magerit, de esta forma se seleccionó dicha metodología para realizar el análisis de los riesgos para la IPS Garper Médica SAS.

Actividad 2: Realizar el inventario de los activos teniendo en cuenta la clasificación e identificación de cada uno con base en la metodología seleccionada Magerit, esta actividad se realiza en conjunto con el técnico en Sitio y el jefe de tecnología, definiéndolos.

A continuación, basados en la metodología Magerit se realiza un inventario de activos al área de tecnología, donde se puede evidenciar cada activo definidos según el nombre, clasificación, cantidad y responsables, como se muestra en el cuadro 5.

Cuadro 5. Identificación y clasificación de los activos

Nombre del Activo	**Cantidad**	**Responsables**
Tipo: [D] Datos		
Base de datos Página Web	1	Jefe de Tecnología
Base de datos Intranet	1	Jefe de Tecnología
Base de datos E-learning	1	Técnico en Sitio
Backups de bases de datos	1	Jefe de Tecnología - Técnico en Sitio
Manuales de contingencias	NA	Jefe de Tecnología
Manuales de los Sistemas	NA	Jefe de Tecnología
Carpetas de archivos de Sistema Gestion de Calidad	NA	Técnico en Sitio
Carpetas de archivos de Facturacion	NA	Técnico en Sitio
Carpetas de archivos de Cartera	NA	Técnico en Sitio
Carpeta de archivos Financiera - costos	NA	Técnico en Sitio
Carpeta de Archivos gerencia	NA	Técnico en Sitio
Carpeta de Archivos Compras	NA	Técnico en Sitio
Backups Correos	1	Técnico en Sitio
Datos de gestión interna	NA	Jefe de Tecnología - Técnico en Sitio
Tipo: [K] Claves criptográficas		
Código QR de Activos Fisicos	1	Técnico en Sitio
Tipo: [SW] Servicios		

Cuadro 5 :(Continuación)

Directorio Activo - Autenticación	1	Coordinador de Tecnología
Telefonía IP	2	Técnico en Sitio
Página web	1	Desarrollador
Mesa de ayuda	1	Técnico en Sitio
Intranet	1	Jefe de Tecnología - Técnico en Sitio
Correo electrónico	1	Jefe de Tecnología - Técnico en Sitio
Proxy	2	Técnico en Sitio
Sistema de Gestión Documental	1	Jefe de Tecnología - Coordinador de Tecnología
Dropbox	1	Técnico en Sitio
ERP- Sistema Clínico iMédicalCloud	1	Jefe de Tecnología - Coordinador de Tecnología- Técnico en Sitio
Anydesk - Remoto a equipos	1	Técnico en Sitio
OneDrive	10	Técnico en Sitio
Tipo: [SW] Software		
Sistemas operativos	225	Técnico en Sitio
Antivirus	25	Técnico en Sitio
Plataforma OFFICE 365	111	Técnico en Sitio
Firewall Seguridad perimetral	2	Técnico en Sitio
Monitoreo de Red	2	Técnico en Sitio
Isabel- Telefonia IP	2	Técnico en Sitio
sql- Server.	1	Jefe de Tecnología
Helisa - Sistema contable	1	Jefe de Tecnología - Técnico en Sitio
Sistema para Back up	1	Técnico en Sitio
Tipo: [HW] Hardware		
Servidores	4	Técnico en Sitio
Almacenamientos	3	Técnico en Sitio
Computadores	214	Técnico en Sitio
Portatiles	14	Técnico en Sitio
Tablet	1	Técnico en Sitio
Impresoras	57	Técnico en Sitio
Switches	9	Técnico en Sitio
Access Point	7	Técnico en Sitio
Equipo para Back up	1	Técnico en Sitio
Escaner	3	Técnico en Sitio
Modems	1	Técnico en Sitio
DVR	6	Técnico en Sitio
Router	6	Técnico en Sitio
Biométricos	6	Técnico en Sitio
Teléfono IP	102	Técnico en Sitio
Tipo: [COM] Redes de comunicaciones		
Red LAN	1	Técnico en Sitio
Red Wifi	6	Jefe de Tecnología - Técnico en Sitio
Canal SIP Telefonía IP	4	Jefe de Tecnología - Técnico en Sitio

Cuadro 5 :(Continuación)

Telefonía móvil	2	Técnico en Sitio
Internet	7	Jefe de Tecnología - Técnico en Sitio
Tipo: [Media] Soportes de información		
Memorias USB	5	Jefe de Tecnología - Técnico en Sitio
Discos Duros Externos	5	Jefe de Tecnología - Técnico en Sitio
[AUX] Equipamiento auxiliar		
UPS en Centros datos	7	Jefe de infraestructura
Cableado estructurado	6	Técnico en Sitio - Auxiliar de Mantenimiento
Tipo: [L] Instalaciones físicas		
Centros de Datos	6	Financiera- Jefe de Tecnología
Oficinas	6	Gerente - Financiera
Tipo: [P] Personal		
Jefe de Tecnología	1	Gerente
Coordinador de Tecnología	1	Jefe de Tecnología
Técnicos en Sitio	2	Jefe de Tecnología
Programador	1	Jefe de Tecnología

Fuente: Elaboración propia

Actividad 3: Valorar las cinco dimensiones de la seguridad para cada activo (confidencialidad, integridad, disponibilidad, autenticidad y Trazabilidad).

Se analizaron los riesgos de los diferentes activos que posee Garper médica SAS, por medio de la metodología magerit, la cual, mediante el análisis de riegos e identificación de los activos de información, se hace una valoración de dichos activos y riesgos, logrando así tener una identificación clara del impacto que puede tener para la empresa ante una violación o evento correspondientes a seguridad de la información y las diferentes medidas que se pueden tomar.

Teniendo en cuenta el objetivo de margerit pretende analizar la gestión de los riesgos, y de esta forma los riesgos son cuantificables y medibles además de que se debe hacer seguimiento de su comportamiento y que cuando surjan se debe estar preparado para lograr mitigarlos y que afecten en lo menor posible el SGSI, a continuación, se caracterizan los activos de la organización y de esta forma se logra un cálculo e identificación de los riesgos, con el fin de lograr tomar las medidas para evitar cualquier riesgo.

La metodología magerit valora las siguientes dimensiones:

[D] Disponibilidad de los datos: Característica de los activos sólida en que las entidades autorizadas tienen acceso a estos cuando lo requieren. [UNE 71504:2008].

[I] Integridad de los datos: Característica sólida en que el activo de información no ha sido alterado de forma no autorizada. [ISO/IEC 13335-1:2004].

[C] Confidencialidad de los datos: Característica sólida en que la información ni se pone a disposición, ni se revela a individuos, entidades no autorizadas. [UNE-ISO/IEC 27001:2007].

[A] Autenticidad del origen de los datos: Característica en que una garantiza la fuente de la que provienen los datos. [UNE 71504:2008].

[T] Trazabilidad: Característica en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

También se centra en tres objetivos:

- Concientizar sobre la existencia de los riesgos y de la necesidad de mitigarlos.
- Brindar un procedimiento ordenado para examinar estos riesgos.
- Descubrir y proyectar las medidas oportunas para conservar los riesgos bajo control.

Análisis de riesgos**:** Para el desarrollo y complemento del análisis de los riesgos existentes para los activos identificados en la entidad, se utilizó la metodología magerit 3.0 distribuido de la siguiente forma[41].

- **Identificación y clasificación de los activos de Garper Médica SAS**, teniendo en cuenta la criticidad de cada activo como se representa en el cuadro 6.

Cuadro 6. Criticidad de los activos

Valor cuantitativo	Valor cualitativo	Descripción
1	Nivel de riesgo Bajo	Daño donde su impacto es no aplicable para la entidad
2	Nivel de riesgo Medio	Daño importante o medianamente alto para la entidad, La pérdida de seguridad en la dimensión no impediría la actividad normal de la organización
3	Nivel de riesgo Alto	Daño muy grave y de alto impacto para la entidad, La pérdida de seguridad en la dimensión originaría trastornos leves en la actividad normal de la organización.

Fuente: Elaboración propia

- **Valoración de activos,** se hace una valoración de activos, mediante una calificación de 1 a 3 se valora la seguridad que impediría la actividad normal de la organización, en cuanto a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de cada uno de los activos, relacionado en el cuadro 7.

[41] DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. 20 p

Cuadro 7. Valoración de dimensiones de los activos de información

Nombre del Activo	Valoración de Dimensiones [D] Disponibilidad	[I] Integridad de los datos	[C] Confidencialidad de la información	[A] Autenticidad	[T] Trazabilidad	Valor Cualitativo (Criticidad)	Valor Cuantitativo (Criticidad)
Tipo: [D] Datos							
Base de datos Página Web	2	3	3	3	3	14	Critico
Base de datos Intranet	2	3	3	3	3	14	Critico
Base de datos E-learning	1	2	2	2	2	9	Alto
Backups de bases de datos	3	3	3	3	3	15	Critico
Manuales de contingencias	1	2	2	2	2	9	Alto
Manuales de los Sistemas	1	1	1	2	1	6	Medio
Carpetas de archivos de Sistema Gestión de Calidad	1	2	2	2	1	8	Medio
Carpetas de archivos de Facturación	1	2	2	2	2	9	Alto
Carpetas de archivos de Cartera	1	2	2	2	2	9	Alto
Carpeta de archivos Financiera - costos	1	2	2	2	2	9	Alto
Carpeta de Archivos gerencia	1	2	2	2	2	9	Alto
Carpeta de Archivos Compras	1	2	2	2	2	9	Alto
Backups Correos	1	2	2	2	2	9	Alto
Datos de gestión interna	2	2	3	3	3	13	Critico
Tipo: [K] Claves criptográficas							
Código QR de Activos Fisicos	3	3	3	3	3	15	Critico
Tipo: [SW] Servicios							
Directorio Activo - Autenticación	3	3	3	3	2	14	Critico
Telefonía IP	2	2	2	2	2	10	Alto
Página web	3	2	2	2	2	11	Alto
Mesa de ayuda	2	2	2	2	2	10	Alto
Intranet	2	2	2	2	2	10	Alto
Correo electrónico	2	3	2	2	2	11	Alto
Proxy	2	1	1	1	1	6	Medio
Sistema de Gestión Documental	1	1	1	1	1	5	Medio
Dropbox	1	1	1	1	1	5	Medio
ERP- Sistema Clínico iMédicalCloud	3	3	3	3	3	15	Critico
Anydesk - Remoto a equipos	1	1	1	1	1	5	Medio
OneDrive	1	1	1	1	1	5	Medio
Tipo: [SW] Software							
Sistemas operativos	3	1	2	2	1	9	Alto
Antivirus	2	2	1	2	2	9	Alto
Plataforma OFFICE 365	1	2	2	2	2	9	Alto
Firewall Seguridad perimetral	3	2	2	2	2	11	Alto
Monitoreo de Red	1	1	1	1	1	5	Medio
Isabel- Telefonia IP	2	2	2	2	2	10	Alto
sql- Server.	1	1	1	1	1	5	Medio
Helisa - Sistema contable	1	2	2	2	2	9	Alto
Sistema para Back up	1	2	2	1	1	7	Medio
Tipo: [HW] Hardware							
Servidores	2	2	2	1	1	8	Medio
Almacenamientos	2	2	2	2	2	10	Alto
Computadores	1	1	2	1	1	6	Medio
Portatiles	1	1	2	1	1	6	Medio
Tablet	1	1	2	1	1	6	Medio
Impresoras	1	1	2	1	1	6	Medio
Switches	1	1	2	1	1	6	Medio
Access Point	1	1	2	1	1	6	Medio
Equipo para Back UP	1	1	2	1	1	6	Medio

Cuadro 7. (Continuación)

Escaner	1	1	2	1	1	6	Medio
Modems	1	1	2	1	1	6	Medio
DVR	1	1	2	1	1	6	Medio
Router	1	1	2	1	1	6	Medio
Biometricos	1	1	2	1	1	6	Medio
teléfono IP	1	1	2	1	1	6	Medio
Tipo: [COM] Redes de comunicaciones							
Red LAN	3	3	2	2	2	12	Alto
Red Wifi	1	1	1	1	1	5	Medio
Canal SIP Telefonía IP	2	1	1	1	1	6	Medio
telefonía móvil	2	1	1	1	1	6	Medio
Internet	3	2	2	1	1	9	Alto
Tipo: [Media] Soportes de información							
memorias USB	0	1	1	0	0	2	Bajo
Discos Duros Externos	1	1	1	0	0	3	Bajo
[AUX] Equipamiento auxiliar							
UPS en Centros datos	2	2	2	2	1	9	Alto
Cableado estructurado	2	2	2	2	1	9	Alto
Tipo: [L] Instalaciones físicas							
Centros de Datos	3	2	3	2	1	11	Alto
Oficinas	2	2	2	2	0	8	Medio
Tipo: [P] Personal							
Jefe de Tecnologia	2	3	3	2	3	13	Critico
Coordinador de Tecnologia	2	3	3	2	3	13	Critico
Tecnicos en Sitio	2	3	3	2	3	13	Critico
Programador	2	3	3	2	3	13	Critico

Fuente: Elaboración propia

Análisis de Valoración de dimensiones de los activos de información.

La metodología Magerit propone la identificación de los activos, así mismo la dependencia de estos, de esta forma se logra la identificación de niveles de criticidad que estarán ligados al activo y al responsable, se logra la identificación que cualquier vulnerabilidad tendrá un impacto menor o mayor, definiendo el nivel de criticidad e impedimento la realización de las actividades de la Entidad.

Para Garper Médica tratándose de una Entidad de salud, su mayor impacto se valora sobre el Tipo [D] Datos, [SW] Servicios, [P] Personal, la información que se maneja teniendo en cuenta la parte administrativa y asistencial, para lograr la atención integral de los pacientes se lleva a través de los servicios en la Nube, como por ejemplo su sistema de información Clínico, si este no se encuentra disponible, integro, confidencial, se estaría repercutiendo en problemas graves con entes de

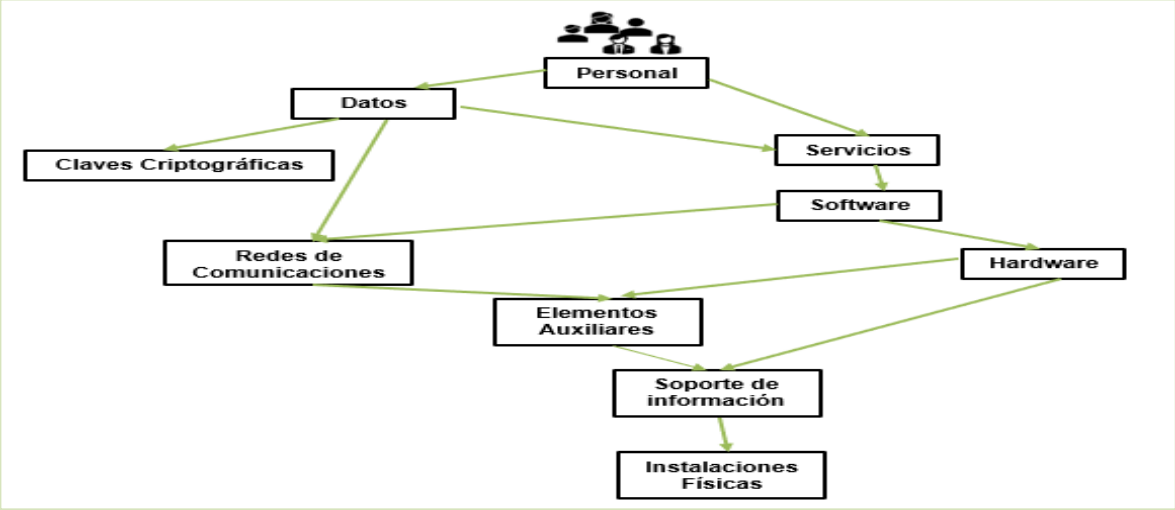
control (Ministerio de salud y secretarias de salud) ya que las Historias Clínica son documentos privados, obligatorio y sometido a reserva, se maneja de forma cronológica teniendo en cuenta la condición del paciente (Resolución 1995 de 1999 Ministerio de salud- Por la cual se establecen normas para el manejo de la Historia Clínica).

Esta información se debe salvaguardar y mantener en un servicio seguro, ya que puede tener incidencia en la vida del paciente.

Los tres tipos de activos se encuentran ligados y por este motivo se da un valor Critico él ya que el daño es extremadamente grave y crítico para Garper Médica, la perdida de seguridad causará trastornos graves tanto para el paciente como para la organización, de esta forma es indispensable los tipos de Activos [P], [D] y [SW].

En la ilustración 5 se diseña la jerarquía de los activos de información de la IPS Garper Médica.

Ilustración 5. Árbol de dependencia de activos



Fuente: Elaboración propia

Actividad 4. Identificar las amenazas y los riesgos a las que están expuestos los activos: La vulnerabilidad corresponde a toda debilidad que puede ser aprovechada por una amenaza, o más específicamente a la debilidad es de los activos o de sus medidas o políticas de defensa que proporcionan el éxito de una amenaza permisible.

Son vulnerabilidades todas las ineficacias o falta de las salvaguardas acertados para proteger el valor propio de un activo

La identificación de las amenazas es una de las actividades de mayor importancia y relevancia ya que se realiza la clasificación según las categorías expuestas en la metodología Magerit y así mismo realizar la dimensión y la descripción del activo.

Las categorías de amenazas relacionadas en la metodología Magerit son:

- [N] Origen de desastres Naturales: Hechos que pueden suceder sin intervención de los seres humanos como causa directa o indirecta, su origen se caracteriza como accidental (Terremotos, inundaciones, incendios, huracanes).
- [I] Origen de industrial: Acontecimientos de forma accidental, originarios de la actividad humana de tipo industrial. Estas amenazas se dan de forma accidental o deliberada (Fuga de agua, explosiones, sobrecarga eléctrica, condiciones inadecuadas de temperatura o humedad, entre otras).
- [E] Errores y fallos no intencionados: Fallos no premeditados originados por las personas. está formada con los ataques deliberados, difiriendo exclusivamente en el propósito del sujeto. El origen es Humano (accidental)
- [A] Ataques intencionados: Fallos premeditados originados por las personas. El origen corresponde al Humano (deliberado).

No todas las amenazas afectan a todos los activos de información, por este motivo se realiza la valoración de cada activo y sus respectivas amenazas.

El responsable del SGSI aportará los datos actualizados para las reuniones de análisis que efectuará la dirección. De dicho análisis se pueden desglosar acciones correctivas.

La valoración de los riesgos se realiza teniendo en cuenta los siguientes niveles relacionados en la Tabla 1:

Cuadro 8. Niveles de clasificación de valoración del riesgo.

Valoración del riesgo		
Valor	Categoría	Nomenclatura
1 a 4	Despreciable	MB
5 a 9	Bajo	B
10 a 15	Medio	M
16 a 20	Importante	A
21 a 25	Critico	MA

Fuente: Elaboración propia

De acuerdo con la valoración de las amenazas se definen dos dimensiones: El impacto y la probabilidad.

Probabilidad: Se estudia que tan posible es que la amenaza se pueda materializar, de acuerdo con la tabla 2.

Degradación o Impacto: Se estudia que tan perjudicial resulta el activo ante la amenaza, la medición de este se realiza de acuerdo con la tabla 2.

Cuadro 9. Tabla de valoración del impacto y probabilidad.

Impacto y probabilidad			
Nomenclatura	**Probabilidad**	**Valoración**	**Impacto**
MA	Muy frecuente (diariamente)	5	Muy Alto
A	Frecuente (Mensualmente)	4	Alta
M	Normal (Una vez al año)	3	Media
B	Poco Frecuente (varios años)	2	Baja
MB	Nunca ocurre	1	Sin degradación o impacto

Fuente: Elaboración propia

A continuación, se observa la matriz con la identificación de las amenazas sobre cada activo de la IPS Garper Médica, la valoración de los riesgos teniendo en cuentas las dimensiones, el impacto en cada dimensión, sobre esta matriz se valoran tres dimensiones (Disponibilidad, confidencialidad e integridad) las cuales son de mayor impacto teniendo en cuenta los activos seleccionados con más relevancia, se identifica el impacto y la probabilidad de ocurrencia en la Tabla 3.

Cuadro 10. Matriz de Valoración de riesgos.

Nombre del activo	**Amenazas**	**Impacto en cada dimension**			**Impacto**	**Probabilidad**	**Nivel de riesgo**
		[D]	**[I]**	**[C]**			
Tipo: [D] Datos							
Base de datos Página Web	[A.11] Acceso no autorizado	3	5	5	A	A	IMPORTANTE
	[E.2] Errores del administrador	3	4	3	MA	B	MEDIO
	[E.15] Alteración accidental de la información	3	5	2	MA	B	MEDIO
	[E.19] Fugas de información	-	5	4	A	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	-	5	-	A	M	BAJO

Cuadro 10: (Continuación)

	[A.3] Manipulación de los registros de actividad (log)	-	5	5	M	B	MEDIO
	[A.15] Modificación deliberada de la información	3	3	3	A	M	BAJO
	[A.19] Divulgación de información	-	3	3	A	M	BAJO
	[E.20] Vulnerabilidades de los programas (software)	3	3	5	M	B	MEDIO
	[A.24] Denegación de servicio	4	4	-	A	M	BAJO
	[A.6] Abuso de privilegios de acceso	-	-	4	A	M	BAJO
	[E.15] Alteración accidental de la información	-	5	3	A	M	BAJO
Base de datos Intranet	[E.20] Vulnerabilidades de los programas (software)	4	-	-	M	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	M	M	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	-	4	-	M	M	BAJO
	[A.15] Modificación deliberada de la información	3	5	5	A	A	IMPORTANTE
	[A18] Destrucción de información	4	4	-	M	B	MEDIO
	[A19] Divulgación de información	3	5	5	A	A	IMPORTANTE
	[E.8] Difusión de software dañino	-	-	4	M	M	BAJO
	[E.19] Fugas de información	-	-	5	M	B	MEDIO
	[A.11] Acceso no autorizado	-	3	5	M	M	BAJO
Base de datos E-learning	[A.11] Acceso no autorizado	3	3	5	B	B	MEDIO
	[E.19] Fugas de información	-	3	3	B	B	MEDIO
	[A.15] Modificación deliberada de la información	3	3	3	B	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	3	3	3	B	B	BAJO
Backups de bases de datos	[E.15] Alteración accidental de la información	-	5	5	MA	B	MEDIO
	[E.18] Destrucción de información	5	5	5	MA	M	CRITICO
	[E.19] Fugas de información	-	3	3	MA	B	MEDIO
	[E.28] Indisponibilidad del personal	4	-	-	A	M	BAJO
	[A.18] Destrucción de información	4	5	5	A	M	IMPORTANTE
	[A .19] Divulgación de información	-	5	5	MA	B	MEDIO
	[I.8] Fallo de servicios de comunicaciones	4	-	-	MA	B	MEDIO
	[E.2] Errores del administrador	3	3	3	MA	M	BAJO
Manuales de contingencias / Manuales de los Sistemas	[E.18] Destrucción de información	5	5	5	MA	A	CRITICO
	[E.19] Fugas de información	-	4	4	MA	B	MEDIO
	[A.15] Modificación deliberada de la información	-	5	4	M	B	MEDIO
	[A.18] Destrucción de información	5	5	5	MA	A	CRITICO
	[A.19] Divulgación de información	-	4	5	M	M	BAJO
	[E.2] Errores del administrador	4	3	3	M	B	MEDIO

Cuadro 10: (Continuación)

	[E.3] Errores de monitorización (log)	-	3	3	M	M	BAJO
	[E.7] Deficiencias en la organización	-	3	3	A	B	MEDIO
	[E.15] Alteración accidental de la información	-	5	3	M	M	BAJO
Carpetas de archivos compartidos en red - diferentes areas	[E.18] Destrucción de información	-	5	5	MA	M	MEDIO
	[E.19] Fugas de información	-	5	3	A	M	MEDIO
	[E.20] Vulnerabilidades de los programas (software)	3	3	3	MA	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	3	3	3	MA	M	BAJO
	[E.28] Indisponibilidad del persona	3	3	3	MA	A	BAJO
	[A.4] Manipulación de la configuración	-	5	3	A	M	MEDIO
	[A.6] Abuso de privilegios de acceso	4	5	3	A	M	MEDIO
	[A.11] Acceso no autorizado	-	5	5	A	M	MEDIO
	[A.15] Modificación deliberada de la información	-	5	3	A	M	MEDIO
	[A18] Destrucción de información	5	5	5	MA	A	CRITICO
	[A19] Divulgación de información	-	3	5	MA	A	BAJO
	[E.1] Errores de los usuarios	-	3	3	MA	A	BAJO
	[E.15] Alteración accidental de la información	-	3	3	MA	M	MEDIO
	[E.19] Fugas de información	-	3	5	MA	A	BAJO
Backups Correos	[E.18] Destrucción de información	-	5	5	MA	M	MEDIO
	[E.19] Fugas de información	-	3	5	A	M	MEDIO
	[A.19] Divulgación de información	-	3	5	A	M	MEDIO
	[I.8] Fallo de serv icios de comunicaciones	3	3	3	M	A	BAJO
	[E.2] Errores del administrador	3	3	3	M	B	BAJO
	[E.20] Vulnerabilidades de los programas (software)	5	3	3	M	M	MEDIO
Datos de gestión interna	[E.21] Errores de mantenimiento / actualización de programas (software)	-	3	3	M	M	BAJO
	[E.28] Indisponibilidad del personal	-	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	3	3	3	M	B	MEDIO
	[A.6] Abuso de privilegios de acceso	3	5	3	M	B	MEDIO
	[A.11] Acceso no autorizado	-	3	3	M	M	BAJO
	[A.15] Modificación deliberada de la información	-	5	3	M	M	BAJO
	[E.14] Escapes de información	-	5	3	M	M	BAJO
	[E.15] Alteración accidental de la información	-	5	3	M	B	MEDIO
	[A18] Destrucción de información	-	5	5	M	B	MEDIO
	[A19] Divulgación deinformación	-	5	3	M	B	MEDIO
	[A22] Manipulación de programas	-	5	3	M	M	BAJO

Cuadro 10: (Continuación)

	[E.1] Errores de los usuarios	-	5	3	M	M	BAJO
Tipo: [K] Claves criptográficas							
Código QR de Activos Fisicos	[E.15] Alteración accidental de la información	4	5	5	A	B	IMPORTANTE
	[E.2] Errores del administrador	3	5	5	A	B	IMPORTANTE
	[E.4] Errores de configuración	3	5	5	A	B	IMPORTANTE
	[E.20] Vulnerabilidades de los programas (software)	3	5	5	A	B	IMPORTANTE
	[E.14] Escapes de información	-	-	4	M	B	MEDIO
Tipo: [SW] Servicios							
Directorio Activo - Autenticación	[A.4] Manipulación de la configuración	-	5	-	A	B	MEDIO
	[A.6] Abuso de privilegios de acceso	-	5	5	A	B	MEDIO
	[A.15] Modificación deliberada de la información	5	5	-	A	B	MEDIO
	[A.18] Destrucción de información	5	5	5	MA	A	CRITICO
	[A.19] Divulgación de información	3	4	4	A	B	MEDIO
	[I.5] Avería de origen físico o lógico	4	-	-	A	B	MEDIO
Telefonía IP	[I.6] Corte del suministro eléctrico	4	-	-	MA	M	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	MA	M	BAJO
	[I.8] Fallo de servicios de comunicaciones	5	-	-	A	B	MEDIO
	[E.2] Errores del administrador	5	-	-	MA	M	BAJO
	[E.4] Errores de configuración	5	-	-	MA	M	BAJO
	[E.9] Errores de[re-]encaminamiento	4	-	-	MA	M	BAJO
	[E.15] Alteración accidental de la información	-	5	5	A	B	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	2	-	MA	M	BAJO
	[E.25] Pérdida de equipos	5	-	-	A	B	MEDIO
	[E.28] Indisponibilidad del personal	5	-	-	MA	M	BAJO
	[A.4] Manipulación de la configuración	3	4	2	A	B	MEDIO
	[A.6] Abuso de privilegios de acceso	2	3	3	A	B	MEDIO
	[A.11] Acceso no autorizado	4	5	4	A	B	IMPORTANTE
	[A.14] Interceptación de información (escucha)	4	5	5	MA	M	IMPORTANTE
	[A.18] Destrucción de información	5	5	5	MA	A	CRITICO
	[A.19] Divulgación de información	3	4	4	A	B	MEDIO
	[A.23] Manipulación de los equipos	3	2	-	A	B	MEDIO
	[A.25] Robo	4	5	4	MA	B	IMPORTANTE
	[E.2] Errores del administrador	3	3	2	MA	M	BAJO
	[E.4] Errores de configuración	3	2	2	MA	M	BAJO

Cuadro 10: (Continuación)

Página web	[I.10] Degradación de los soportes de almacenamiento de la información	4	-	-	A	M	BAJO
	[E.2] Errores del administrador	3	3	-	A	B	MEDIO
	[E.15] Alteración accidental de la información	3	3	-	A	B	MEDIO
	[E.19] Fugas de información	5	-	-	A	B	MEDIO
	[E.21] Errores de mantenimiento / actualización de programas (software)	-	5	-	A	M	BAJO
	[A.3] Manipulación de los registros de actividad (log)	-	5	4	A	M	BAJO
	[A.11] Acceso no autorizado	4	3	4	A	B	MEDIO
	[A.15] Modificación deliberada de la información	3	3	3	A	B	MEDIO
	[A.19] Divulgación de información	-	-	4	A	M	BAJO
	[E.20] Vulnerabilidades de los programas (software)	-	4	-	A	M	BAJO
	[A.24] Denegación de servicio	4	4	4	A	B	MEDIO
	[A.6] Abuso de privilegios de acceso	3	3	3	A	B	MEDIO
	[E.15] Alteración accidental de la información	3	4	4	A	B	MEDIO
Mesa de ayuda	[E.18] Destrucción de información	5	5	5	MA	B	CRITICO
	[E.19] Fugas de información	-	-	4	A	B	MEDIO
	[E.20] Vulnerabilidades de los programas (software)	-	-	4	MA	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	-	-	MA	M	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	MA	M	BAJO
	[A.4] Manipulación de la configuración	-	5	-	MA	M	BAJO
	[A.6] Abuso de privilegios de acceso	-	-	4	MA	M	BAJO
	[A.15] Modificación deliberada de la información	3	3	3	A	B	MEDIO
	[A18] Destrucción de información	4	4	-	A	B	MEDIO
	[A19] Divulgación de información	-	-	4	MA	B	CRITICO
	[E.2] Errores del administrador	3	3	-	MA	B	CRITICO
	[E.4] Errores de configuración	3	3	-	A	B	MEDIO

Cuadro 10: (Continuación)

	[E.15] Alteración accidental de la información	3	5	-	MA	B	CRITICO
	[E.18] Destrucción de información	5	3	-	MA	B	CRITICO
	[E.19] Fugas de información	-	-	4	MA	B	CRITICO
Intranet	[E.20] Vulnerabilidades de los programas (software)	4	-	-	M	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	M	M	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	M	M	BAJO
	[A.4] Manipulación de la configuración	-	4	-	A	B	MEDIO
	[A.15] Modificación deliberada de la información	3	5	5	A	M	IMPORTANTE
	[A18] Destrucción de información	4	4	-	MA	M	CRITICO
	[A19] Divulgación de información	-	-	4	MA	MA	CRITICO
	[E.8] Difusión de software dañino	3	3	3	M	M	BAJO
	[E.19] Fugas de información	-	-	5	MA	MA	CRITICO
	[A.11] Acceso no autorizado	3	2	2	A	B	MEDIO
Correo electrónico	[A.7] Uso no previsto	3	3	5	A	B	MEDIO
	[A.8] Difusión de software dañino	4	4	4	A	B	MEDIO
	[A30] Ingeniería social (picaresca)	-	-	4	A	B	MEDIO
	[E.2] Errores del administrador	3	3	3	M	M	BAJO
	[E.3] Errores de monitorización (log)	4	-	-	M	M	BAJO
	[E.4] Errores de configuración	4	-	-	M	M	BAJO
	[E.15] Alteración accidental de la información	4	4	-	A	B	MEDIO
Proxy	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	M	B	BAJO
	[A.4] Manipulación de la configuración	4	2	-	M	B	BAJO
	[A.6] Abuso de privilegios de acceso	4	3	-	M	B	BAJO
	[E.28] Indisponibilidad del personal	4	3	-	M	B	BAJO
Sistema de Gestión Documental	[E.15] Alteración accidental de la información	4	4	4	A	A	MEDIO
	[E.18] Destrucción de información	5	5	5	MA	M	CRITICO
	[E.19] Fugas de información	-	4	4	A	A	MEDIO
	[E.20] Vulnerabilidades de	5	-	-	M	B	BAJO

Cuadro 10: (Continuación)

	los programas (software)						
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	M	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	M	B	BAJO
	[A.4] Manipulación de la configuración	5	3	-	A	A	MEDIO
	[A.6] Abuso de privilegios de acceso	3	4	3	A	A	MEDIO
	[A.11] Acceso no autorizado	-	4	3	M	A	BAJO
	[A.15] Modificación deliberada de la información	-	4	4	A	A	MEDIO
	[E.14] Escapes de información	-	3	3	A	A	MEDIO
	[E.15] Alteración accidental de la información	-	4	3	A	A	MEDIO
	[A19] Divulgación de información	-	3	3	A	A	MEDIO
	[E.1] Errores de los usuarios	-	3	2	A	A	MEDIO
Dropbox	[E.1] Errores de los usuarios	-	4	2	M	M	BAJO
	[E.2] Errores del administrador	2	2	2	M	M	BAJO
	[E.15] Alteración accidental de la información	-	3	2	A	A	MEDIO
	[E.18] Destrucción de información	5	5	5	MA	M	CRITICO
	[E.19] Fugas de información	-	3	3	M	A	BAJO
	[A.11] Acceso no autorizado	2	4	4	A	A	MEDIO
	[A.15] Modificación deliberada de la información	-	4	4	A	A	MEDIO
	[A18] Destrucción de información	5	5	5	MA	M	CRITICO
	[A19] Divulgación de información	-	4	3	M	A	BAJO
	[A24] Denegación de servicio	4	4	4	A	A	MEDIO
	[E.8] Difusión de software dañino	5	5	5	MA	M	CRITICO
ERP- Sistema Clínico iMédicalCloud	[E.1] Errores de los usuarios	-	5	5	A	A	MEDIO
	[E.2] Errores del administrador	5	5	5	MA	M	CRITICO
	[E.15] Alteración accidental de la información	-	5	5	A	A	MEDIO
	[E.18] Destrucción de información	5	5	5	MA	B	CRITICO
	[E.19] Fugas de información	-	5	5	A	A	MEDIO
	[A.11] Acceso no autorizado	-	5	5	A	A	MEDIO
	[A.15] Modificación deliberada de la información	-	5	5	A	A	MEDIO
	[A18] Destrucción de información	5	5	5	MA	B	CRITICO

Cuadro 10: (Continuación)

	[A19] Divulgación de información	-	5	5	A	A	MEDIO
	[A24] Denegación de servicio	5	5	5	MA	B	CRITICO
	[E.8] Difusión de software dañino	5	5	5	MA	B	CRITICO
OneDrive	[E.1] Errores de los usuarios	2	3	2	M	A	BAJO
	[E.2] Errores del administrador	3	3	3	M	B	BAJO
	[E.15] Alteración accidental de la información	-	5	4	M	A	MEDIO
	[E.18] Destrucción de información	5	5	5	MA	A	CRITICO
	[E.19] Fugas de información	3	3	3	M	A	BAJO
	[A.11] Acceso no autorizado	-	3	2	M	A	BAJO
	[A.15] Modificación deliberada de la información	-	3	3	M	A	MEDIO
	[A18] Destrucción de información	4	4	4	M	A	MEDIO
	[A19] Divulgación de información	-	3	3	M	A	MEDIO
	[A24] Denegación de servicio	4	4	4	M	A	MEDIO
	[E.8] Difusión de software dañino	5	5	5	MA	A	CRITICO
Anydesk - Remoto a equipos	[A19] Divulgación de información	-	4	3	M	A	MEDIO
	[A18] Destrucción de información	5	5	5	MA	A	CRITICO
	[E.8] Difusión de software dañino	5	5	-	M	A	MEDIO
	[A.15] Modificación deliberada de la información	-	4	2	M	A	MEDIO
	[E.19] Fugas de información	-	4	3	M	A	MEDIO
	[E.18] Destrucción de información	5	5	5	MA	A	CRITICO
Tipo: [SW] Software							
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)	5	5	-	M	A	MEDIO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	M	B	BAJO
	[E.2] Errores del administrador	4	4	-	M	B	BAJO
Antivirus	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	M	B	BAJO
	[E.2] Errores del administrador	4	3	2	M	B	BAJO
	[E.4] Errores de configuración	3	3	-	M	B	BAJO
	[E.15] Alteración accidental de la información	5	5	-	M	A	MEDIO
	[E.18] Destrucción de información	5	3	-	M	A	MEDIO
Plataforma OFFICE 365	[E.24] Caída del sistema por agotamiento de recursos	4	-	-	M	B	BAJO
	[A.11] Acceso no autorizado	-	5	4	M	B	BAJO
	[A.15] Modificación deliberada de la información	-	5	5	M	A	MEDIO
Firewall Seguridad perimetral	[E.21] Errores de mantenimiento / actualización de programas (software)	3	3	-	M	B	BAJO
	[A.4] Manipulación de la configuración	4	3	-	M	A	MEDIO
	[A.6] Abuso de privilegios de acceso	3	3	-	M	A	MEDIO

Cuadro 10: (Continuación)

	[E.28] Indisponibilidad del persona	4	-	-	M	B	BAJO
	[N.*] Desastres naturales	5	-	-	M	A	MEDIO
Monitoreo de Red	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	M	B	BAJO
	[A.4] Manipulación de la configuración	4	3	-	M	B	BAJO
	[A.6] Abuso de privilegios de acceso	3	4	2	M	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	M	B	BAJO
Isabel- Telefonia IP	[I.6] Corte del suministro eléctrico	4	-	-	M	A	MEDIO
	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	MA	B	BAJO
	[I.8] Fallo de servicios de comunicaciones	4	-	3	M	A	MEDIO
	[E.2] Errores del administrador	4	2	-	MA	M	BAJO
	[E.4] Errores de configuración	4	3	-	M	A	MEDIO
	[E.9] Errores de[re-]encaminamiento	4	4	-	MA	M	BAJO
	[E.15] Alteración accidental de la información	-	4	3	M	A	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	-	-	MA	M	BAJO
	[E.25] Pérdida de equipos	4	2	-	MA	M	BAJO
	[E.28] Indisponibilidad del personal	5	2	2	MA	B	BAJO
	[A.4] Manipulación de la configuración	4	3	2	M	A	MEDIO
	[A.6] Abuso de privilegios de acceso	3	4	4	M	A	MEDIO
	[A.11] Acceso no autorizado	3	4	4	M	A	MEDIO
	[A.14] Interceptación de información (escucha)	-	4	4	MA	M	BAJO
	[A.18] Destrucción de información	5	5	5	MA	B	CRITICO
	[A.19] Divulgación de información	-	4	4	M	A	MEDIO
	[A.23] Manipulación de los equipos	3	3	3	MA	A	BAJO
	[A.25] Robo	5	5	5	MA	B	CRITICO
	[E.2] Errores del administrador	4	3	3	M	A	MEDIO
	[E.4] Errores de configuración	4	3	3	M	A	MEDIO
sql- Server.	[E.20] Vulnerabilidades de los programas (software)	-	4	3	A	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	2	-	A	M	BAJO
	[A.4] Manipulación de la configuración	4	4	4	MA	M	MEDIO
	[A.6] Abuso de privilegios de acceso	-	4	4	MA	M	CRITICO
Helisa - Sistema contable	[E.21] Errores de mantenimiento / actualización de programas (software)	4	2	-	A	M	BAJO
	[A.4] Manipulación de la configuración	-	5	5	MA	M	MEDIO

Cuadro 10: (Continuación)

	[A.6] Abuso de privilegios de acceso	4	5	5	MA	B	CRITICO
	[A.11] Acceso no autorizado	-	5	5	MA	M	MEDIO
	[A.15] Modificación deliberada de la información	-	5	5	MA	M	MEDIO
	[A18] Destrucción de información	-	5	5	MA	B	MEDIO
	[A19] Divulgación de información	-	5	5	MA	B	MEDIO
	[A22] Manipulación de programas	-	5	5	M	B	MEDIO
Sistema para Back up	[E.20] Vulnerabilidades de los programas (software)	4	-	-	M	B	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	4	-	-	M	B	BAJO
	[E.28] Indisponibilidad del personal	4	-	-	M	B	BAJO
	[A.4] Manipulación de la configuración	5	5	-	A	A	MEDIO
	[A.6] Abuso de privilegios de acceso	-	5	4	A	A	MEDIO
	[A.15] Modificación deliberada de la información	3	3	3	M	B	BAJO
	[A18] Destrucción de información	4	4	-	M	B	BAJO
	[E.2] Errores del administrador	3	3	-	A	B	MEDIO
	[E.4] Errores de configuración	3	3	-	MA	B	BAJO
	[E.15] Alteración accidental de la información	5	5	-	A	A	MEDIO
	[A19] Divulgación de información	5	3	-	A	A	MEDIO
Tipo: [HW] Hardware							
Servidores	[N.1] Fuego	4	-	-	MA	A	MEDIO
	[N.2] Daños por agua	5	-	-	MA	A	MEDIO
	[N.*] Desastres naturales	5	-	-	MA	B	MEDIO
	[I.5] Avería de origen físico o lógico	4	-	-	MA	A	MEDIO
	[I.6] Corte del suministro eléctrico	5	-	-	A	B	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	A	B	BAJO
	[A25] Robo	5	-	-	MA	B	MEDIO
	[A26] Ataque destructive	5	-	-	A	B	BAJO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	A	B	BAJO
	[N.1] Fuego	5	-	-	MA	M	BAJO
	[N.2] Daños por agua	5	-	-	MA	M	BAJO
	[N.*] Desastres naturales	5	-	-	MA	M	BAJO
	[I.5] Avería de origen físico o lógico	5	-	-	MA	B	MEDIO
	[I.6] Corte del suministro eléctrico	5	-	-	MA	M	BAJO
Almacenamientos	[I.7] Condiciones inadecuadas de	5	-	-	A	M	BAJO

Cuadro 10: (Continuación)

	temperatura o humedad						
	[A25] Robo	5	-	-	MA	B	MEDIO
	[A26] Ataque destructive	5	-	-	A	M	BAJO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	A	M	BAJO
	[N.1] Fuego	5	-	-	A	M	BAJO
	[N.2] Daños por agua	5	-	-	A	B	MEDIO
	[N.*] Desastres naturales	5	-	-	A	M	MEDIO
	[I.5] Avería de origen físico o lógico	5	-	-	A	A	MEDIO
	[I.6] Corte del suministro eléctrico	5	-	-	A	M	BAJO
Computadores / Portatiles /Tablet	[I.6] Corte del suministro eléctrico	5	-	-	B	M	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	B	M	BAJO
	[A25] Robo	5	-	-	B	M	BAJO
	[A26] Ataque destructive	5	-	-	B	M	BAJO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	B	M	BAJO
	[E.19] Fugas de información	5	3	-	B	M	BAJO
	[E.25] Pérdida de equipos	5	-	-	B	M	BAJO
	[N.1] Fuego	5	4	-	B	M	BAJO
	[N.2] Daños por agua	5	-	-	B	M	BAJO
	[N.*] Desastres naturales	5	-	-	B	M	BAJO
	[I.5] Avería de origen físico o lógico	5	-	-	B	M	BAJO
	[I.6] Corte del suministro eléctrico	5	-	-	B	M	BAJO
	[E.4] Errores de configuración	5	-	-	B	M	BAJO
Impresoras/Escaner	[I.6] Corte del suministro eléctrico	5	-	-	B	M	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	B	M	BAJO
	[A25] Robo	5	-	-	B	M	BAJO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	B	M	BAJO
	[E.19] Fugas de información	5	-	-	B	M	BAJO
	[E.25] Pérdida de equipos	5	3	-	B	M	BAJO
	[N.1] Fuego	5	-	-	B	M	BAJO
	[N.2] Daños por agua	5	4	-	B	A	MEDIO

Cuadro 10: (Continuación)

	[N.*] Desastres naturales	5	-	-	B	M	BAJO
	[I.5] Avería de origen físico o lógico	5	-	-	B	A	MEDIO
	[I.6] Corte del suministro eléctrico	5	-	-	B	M	BAJO
	[E.4] Errores de configuración	5	-	-	B	M	BAJO
Switches	[E.4] Errores de configuración	5	-	-	B	M	BAJO
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	-	-	B	M	BAJO
	[E.25] Pérdida de equipos	5	-	-	B	M	BAJO
	[A.4] Manipulación de la configuración	5	-	-	B	M	BAJO
	[A.6] Abuso de privilegios de acceso	5	-	-	B	M	BAJO
	[A.11] Acceso no autorizado	5	3	-	M	B	MEDIO
	[A.14] Interceptación de información	5	-	-	B	M	BAJO
	[A.23] Manipulación de los equipos	5	4	-	B	M	BAJO
	[A.25] Robo	5	-	-	M	B	MEDIO
	[E.2] Errores del administrador	5	-	-	B	M	BAJO
	[E.3] Errores de monitorización (log)	5	-	-	B	M	BAJO
	[E.9] Errores de[re-]encaminamiento	5	-	-	B	M	BAJO
Access Point	[A.4] Manipulación de la configuración	5	-	-	M	M	BAJO
	[A.6] Abuso de privilegios de acceso	5	-	-	M	M	BAJO
	[A.11] Acceso no autorizado	5	-	-	M	M	BAJO
	[A.14] Interceptación de información	5	-	-	M	M	BAJO
	[A.23] Manipulación de los equipos	5	-	-	M	M	BAJO
	[A.25] Robo	5	3	-	M	M	BAJO
	[E.2] Errores del administrador	5	-	-	M	M	BAJO
	[E.3] Errores de monitorización (log)	5	4	-	M	M	BAJO
	[E.9] Errores de[re-]encaminamiento	5	-	-	M	M	BAJO
Equipo para Back UP	[I.6] Corte del suministro eléctrico	5	-	-	M	M	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	M	M	BAJO
	[A25] Robo	5	-	-	M	B	MEDIO
	[A26] Ataquedestructive	5	-	-	M	B	MEDIO
	[E.23] Errores de mantenimiento / actualización deequipos (hardware)	5	-	-	M	B	MEDIO
	[E.19] Fugas de información	5	3	-	M	B	MEDIO
	[E.25] Pérdida de equipos	5	-	-	M	B	MEDIO

Cuadro 10: (Continuación)

	[N.1] Fuego	5	4	-	M	B	MEDIO
	[N.2] Daños por agua	5	-	-	M	B	MEDIO
	[N.*] Desastres naturales	5	-	-	M	B	MEDIO
	[I.5] Avería de origen físico o lógico	5	-	-	M	B	MEDIO
	[I.6] Corte del suministro eléctrico	5	-	-	M	M	BAJO
	[E.4] Errores de configuración	5	-	-	M	M	BAJO
Modems	[A25] Robo	5	-	-	B	M	BAJO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	B	M	BAJO
	[E.19] Fugas de información	5	-	-	B	M	BAJO
	[E.25] Pérdida de equipos	5	-	-	B	M	BAJO
	[N.1] Fuego	5	-	-	B	M	BAJO
	[N.2] Daños por agua	5	3	-	B	M	BAJO
	[N.*] Desastres naturales	5	-	-	B	M	BAJO
	[I.5] Avería de origen físico o lógico	5	4	-	B	M	BAJO
	[I.6] Corte del suministro eléctrico	5	-	-	B	M	BAJO
	[E.4] Errores de configuración	5	-	-	B	M	BAJO
Router	[A25] Robo	5	-	-	M	M	BAJO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	M	M	BAJO
	[E.19] Fugas de información	5	-	-	M	M	BAJO
	[E.25] Pérdida de equipos	5	-	-	M	M	BAJO
	[N.1] Fuego	5	-	-	M	M	BAJO
	[N.2] Daños por agua	5	3	-	M	M	BAJO
	[N.*] Desastres naturales	5	-	-	M	M	BAJO
	[I.5] Avería de origen físico o lógico	5	4	-	M	B	MEDIO
	[I.6] Corte del suministro eléctrico	5	-	-	M	M	BAJO
	[E.4] Errores de configuración	5	-	-	M	M	BAJO
DVR	[A25] Robo	5	-	-	M	M	BAJO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	M	M	BAJO
	[E.19] Fugas de información	5	-	-	A	M	BAJO
	[E.25] Pérdida de equipos	5	-	-	A	M	BAJO
	[N.1] Fuego	5	-	-	A	M	BAJO
	[N.2] Daños por agua	5	3	-	A	M	BAJO
	[N.*] Desastres naturales	5	-	-	A	M	BAJO
	[I.5] Avería de origen físico o lógico	5	4	-	M	B	MEDIO

Cuadro 10: (Continuación)

	[I.6] Corte del suministro eléctrico	5	-	-	A	M	BAJO
	[E.4] Errores de configuración	5	-	-	A	M	BAJO
Biometricos	[A25] Robo	5	-	-	M	M	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	M	M	BAJO
	[E.19] Fugas de información	5	-	-	M	M	BAJO
	[E.25] Pérdida de equipos	5	-	-	M	M	MEDIO
	[N.1] Fuego	5	-	-	M	M	BAJO
	[N.2] Daños por agua	5	3	-	M	M	BAJO
	[N.*] Desastres naturales	5	-	-	M	M	BAJO
	[I.5] Avería de origen físico o lógico	5	4	-	M	M	MEDIO
	[I.6] Corte del suministro eléctrico	5	-	-	M	M	BAJO
	[E.4] Errores de configuración	5	3	-	M	M	BAJO
teléfono IP	[I.6] Corte del suministro eléctrico	5	-	-	A	M	BAJO
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	A	M	BAJO
	[A25] Robo	5	-	-	M	M	MEDIO
	[A26] Ataque destructive	5	4	2	M	M	MEDIO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	A	M	BAJO
	[E.19] Fugas de información	5	3	-	A	M	BAJO
	[E.25] Pérdida de equipos	5	-	-	M	M	MEDIO
	[N.1] Fuego	5	4	-	A	M	BAJO
	[N.2] Daños por agua	5	-	-	A	M	BAJO
	[N.*] Desastres naturales	5	-	-	A	M	BAJO
	[I.5] Avería de origen físico o lógico	5	-	-	M	M	MEDIO
	[I.6] Corte del suministro eléctrico	5	-	-	A	M	BAJO
	[E.4] Errores de configuración	5	-	-	M	M	MEDIO
Tipo: [COM] Redes de comunicaciones							
Red LAN	[E.24] Caída del sistema por agotamiento de recursos	5	-	-	MA	B	BAJO
	[E.28] Indisponibilidad del personal	5	-	-	MA	M	BAJO
	[A.12] Análisis de tráfico	-	-	5	MA	B	BAJO
	[A.14] Interceptación de información	-	-	5	A	B	BAJO
	[E.2] Errores del administrador	4	-	-	A	B	BAJO
	[E.3] Errores de monitorización (log)	4	-	-	A	B	BAJO
	[E.9] Errores de[re-]encaminamiento	4	-	-	A	B	BAJO
Red Wifi	[E.24] Caída del sistema por agotamiento de recursos	5	-	-	MA	B	BAJO

Cuadro 10: (Continuación)

	[E.28] Indisponibilidad del personal	5	-	-	MA	M	BAJO
	[A.12] Análisis de tráfico	-	-	5	MA	B	BAJO
	[A.14] Interceptación de información	-	-	5	A	B	BAJO
	[E.2] Errores del administrador	4	-	-	A	B	BAJO
	[E.3] Errores de monitorización (log)	4	-	-	A	B	BAJO
	[E.9] Errores de[re-]encaminamiento	4	-	-	A	B	BAJO
Canales de comunicación contratados /Troncal-movil-internet	[E.9] Errores de[re]encaminamiento	5	-	-	A	B	BAJO
	[E.24] Caída del sistema por agotamiento de recursos	5	-	-	MA	M	BAJO
	[E.28] Indisponibilidad del personal	5	-	5	MA	M	MEDIO
	[A.12] Análisis de tráfico	-	4	5	MA	B	BAJO
	[A.14] Interceptación de información (escucha)	4	-	-	MA	A	BAJO
	[N.1] Fuego	4	-	-	MA	M	BAJO
	[I.5] Avería de origen físico o lógico	4	-	-	MA	M	BAJO
Tipo: [Media] Soportes de información							
Memorias USB	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	B	M	BAJO
	[A25] Robo	5	-	-	B	MA	BAJO
	[A26] Ataque destructive	5	-	-	B	M	BAJO
	[N.1] Fuego	5	-	-	B	M	BAJO
	[N.2] Daños por agua	5	-	-	B	MA	BAJO
	[I.5] Avería de origen físico o lógico	4	-	-	B	MA	BAJO
Discos Duros Externos	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	B	M	BAJO
	[A25] Robo	5	-	-	B	MA	BAJO
	[A26] Ataque destructive	5	-	-	B	M	BAJO
	[N.1] Fuego	5	-	-	B	M	BAJO
	[N.2] Daños por agua	5	-	-	B	MA	BAJO
	[I.5] Avería de origen físico o lógico	4	-	-	B	MA	BAJO
[AUX] Equipamiento auxiliar							
UPS en Centros datos	[I.7] Condiciones inadecuadas de temperatura o humedad	4	-	-	A	B	BAJO
	[A25] Robo	5	-	-	MA	A	BAJO
	[A26] Ataque destructivo	5	-	-	MA	M	BAJO
	[N.2] Daños por agua	4	-	-	MA	M	BAJO
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	-	-	M	B	BAJO
Cableado estructurado	[A26] Ataque destructivo	4	-	-	MA	B	BAJO
	[N.*] Desastres naturales	5	-	-	A	B	BAJO
	[N.1] Fuego	5	-	-	A	M	BAJO

Cuadro 10: (Continuación)

	[N.2] Daños por agua	4	-	-	MA	B	BAJO
	[I.11] Emanaciones electromagnéticas	5	-	-	MA	M	BAJO
Tipo: [L] Instalaciones físicas							
Centros de Datos	[N.2] Daños por agua	4	-	-	MA	M	BAJO
	[N.*] Desastres naturales	5	-	-	MA	M	BAJO
	[I.1] Fuego	5	-	-	MA	A	BAJO
	[E.28] Indisponibilidad del personal	5	-	-	MA	A	BAJO
	[A.11] Acceso no autorizado	5	-	5	MA	A	MEDIO
Tipo: [P] Personal							
Talento Humano	[E.7] Deficiencias en la organización	4	-	-	A	M	BAJO

Fuente: Elaboración propia

Actividad 5. Valoración y tratamiento de resultados de la matriz de riesgos: A continuación, se realiza la valoración, definición del riesgo sobre cada amenaza, se analizan los resultados teniendo en cuenta el nivel de riesgo y su tratamiento, definidos en la tabla de los resultados y teniendo en cuenta los resultados obtenidos de la matriz de riesgos.

Cuadro 11. Niveles de Tratamiento de riesgos

Nivel de Riesgo	Tratamiento del riesgo
Crítico	Se reduce o se mitiga el riesgo por medio de controles.
Importante	Se reduce o mitiga el riesgo por medio de controles preventivos.
Medio	Se transfiere el riesgo por ejemplo tomando un seguro.
Bajo	Finaliza el proceso.

Fuente: Elaboración propia

En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo.

Riesgo = Impacto x Probabilidad

El tratamiento dado al riesgo se enmarca en las siguientes categorías:

- **Aceptar el riesgo:** En el caso de riesgos de corrupción, estos no pueden ser aceptados, este se adopta para los riesgos bajos a los que la entidad no aplica controles, sin embargo, existen escenarios a los cuales no se les puede aplicar controles, pero si requiere de un seguimiento continuo.

- **Reducir el riesgo:** Para mitigar los riesgos de seguridad se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001:2013.

- **Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo y se resuelve no iniciar o no continuar con las actividades que lo producen.

- **Compartir el riesgo:** Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

En la tabla 5 se observa la distribución de amenazas según la valoración de riesgo de la siguiente forma:

Cuadro 12. Matriz de riesgos

Nombre del Activo	Vulnerabilidad	Amenazas	Riesgo
Tipo: [D] Datos			
Base de datos Página Web	Falta de mecanismos control de acceso	[A.11] Acceso no autorizado	Robo, pérdida o adulteración de información.
		[E.2] Errores del administrador	Pérdida de Información
		[E.15] Alteración accidental de la información	Adulteración de información.
	Falta de politicas respecto a abuso de los privilegios de la base de datos	[E.19] Fugas de información	Robo de materiales de formación
		[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de Información
		[A.3] Manipulación de los registros de actividad (log)	Adulteración de información.
	falta de politicas para el manejo de información	[A.15] Modificación deliberada de la información	Robo, pérdida o adulteración de información.
		[A.19] Divulgación de información	Adulteración de información.
		[E.20] Vulnerabilidades de los programas (software)	Indisponibilidad de servicio.

Cuadro 12: (Continuación)

		[A.24] Denegación de servicio	Caída del sistema
		[A.6] Abuso de privilegio os de acceso	Pérdida de confianza y acceso a la información
		[E.15] Alteración accidental de la información	Indisponibilidad de servicio.
Base de datos Intranet	Falta de mecanismos control de acceso	[E.20] Vulnerabilidades de los programas(software)	Indisponibilidad de servicio.
		[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de Información
		[E.28] Indisponibilidad del personal	Pérdida de confianza y acceso a la información
	Falta de politicas respecto a abuso de los privilegios de la base de datos	[A.4] Manipulación de la configuración	Robo, pérdida o adulteración de información.
		[A.15] Modificación deliberada de la información	
		[A18] Destrucción de información	pérdida de Información
	falta de politicas para el manejo de información	[A19] Divulgación de información	Adulteración de información.
		[E.8] Difusión de software dañino	Caída del sistema
		[E.19] Fugas de información	Robo de materiales de formación
		[A.11] Acceso no autorizado	Pérdida de confianza y acceso a la información
Base de datos E-learning	Falta de mecanismos control de acceso	[A.11] Acceso no autorizado	Pérdida de confianza y acceso a la información
		[E.19] Fugas de información	
		[A.15] Modificación deliberada de la información	
		[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de Información
Backups de bases de datos	Falta de mecanismos control de acceso	[E.15] Alteración accidental de la información	Adulteración de información.
		[E.18] Destrucción de información	Pérdida de Información
	Falta de politicas para el manejo de información	[E.19] Fugas de información	Robo o Pérdida de Información.
	Falta de mecanismos de control durante la asignación al instructor.	[E.28] Indisponibilidad del personal	Algunos programas no reciben la totalidad de materiales de formación.
	Falta de politicas respecto a abuso de los privilegios de la base de datos	[A.18] Destrucción de información	pérdida de Información
		[A.19] Divulgación de información	Adulteración de información.
	Denegación al acceso	[I.8] Fallo de servicios de comunicaciones	Inadecuada prestación del servicio
	Habilitación de brechas de seguridad	[E.2] Errores del administrador	Falta de eficiencia para general las respuesta
Manuales de contingencias / Manuales de los Sistemas	Falta de politicas respecto a abuso de los privilegios de la base de datos	[E.18] Destrucción de información	Robo, pérdida o adulteración de información.
		[E.19] Fugas de información	
		[A.15] Modificación deliberada de la información	
		[A.18] Destrucción de información	
		[A.19] Divulgación de información	

Cuadro 12: (Continuación)

	Habilitación de brechas de seguridad	[E.2] Errores del administrador	Falta de eficiencia para general las respuesta
	Falta de politicas para el manejo de información	[E.3] Errores de monitorización (log)	Falta de eficiencia para general las respuesta
		[E.7] Deficiencias en la organización	Abuso de privilegios de acceso
		[E.15] Alteración accidental de la información	Adulteración de información.
Carpetas de archivos compartidos en red - diferentes areas	Falta de politicas respecto a abuso de los privilegios de la base de datos	[E.18] Destrucción de información	Robo, pérdida o adulteración de información.
		[E.19] Fugas de información	
		[E.20] Vulnerabilidades de los programas (software)	
	Falta de mecanismos control de acceso	[E.21] Errores de mantenimiento / actualización de programas (software)	
		[E.28] Indisponibilidad del persona	Falta de eficiencia para general las respuestas
		[A.4] Manipulación de la configuración	
		[A.6] Abuso de privilegios de acceso	
		[A.11] Acceso no autorizado	
	Falta de politicas para el manejo de información	[A.15] Modificación deliberada de la información	Robo, pérdida o adulteración de información.
		[A18] Destrucción de información	
		[A19] Divulgación de información	
		[E.1] Errores de los usuarios	
		[E.15] Alteración accidental de la información	
		[E.19] Fugas de información	
Backups Correos	Falta de politicas para el manejo de información	[E.18] Destrucción de información	Robo, pérdida o adulteración de información
		[E.19] Fugas de información	
		[A.19] Divulgación de información	
		[I.8] Fallo de servicios de comunicaciones	
		[E.2] Errores del administrador	
		[E.20] Vulnerabilidades de los programas (software)	
Datos de gestión interna	Falta de politicas para el manejo de información	[E.21] Errores de mantenimiento /actualización de programas (software)	Copiar los virus a los equipos de computo
		[E.28] Indisponibilidad del personal	Afectación en la integridad de los archivos
		[A.4] Manipulación de la Configuración	Robo o Pérdida de Información.
	Falta de mecanismos control de acceso	[A.6] Abuso de privilegios de acceso	Robo, pérdida o adulteración de información
		[A.11] Acceso no autorizado	
		[A.15] Modificación deliberada de la información	
		[E.14] Escapes de información	
		[E.15] Alteración accidental de la información	
		[A18] Destrucción de información	

Cuadro 12: (Continuación)

		[A19] Divulgación de información	
		[A22] Manipulación de programas	
		[E.1] Errores de los usuarios	
Tipo: [K] Claves criptográficas			
Código QR de Activos Fisicos	Falta de politicas para uso de claves	[E.15] Alteración accidental de la información	Robo, pérdida o adulteración de información
		[E.2] Errores del administrador	
		[E.4] Errores de configuración	
		[E.20] Vulnerabilidades de los programas (software)	
		[E.14] Escapes de información	
Tipo: [SW] Servicios			
Directorio Activo - Autenticación	Falta de mecanismos control de acceso	[A.4] Manipulación de la configuración	Robo o Pérdida de Información.
		[A.6] Abuso de privilegios de acceso	Afectación en la integridad de los archivos
	Falta de politicas para el manejo de información	[A.15] Modificación deliberada de la información	Indisponibilidad de servicio.
		[A.18] Destrucción de información	Robo, pérdida o adulteración de información
		[A.19] Divulgación de información	
Telefonía IP	Falta de mecanismos control de acceso	[I.6] Corte del suministro eléctrico	Extraer el tráfico de la red para obtener la conversación
		[I.7] Condiciones inadecuadas de temperatura o humedad	
		[I.8] Fallo de servicios de comunicaciones	
		[E.2] Errores del administrador	
		[E.4] Errores de configuración	
		[E.9] Errores de[re-]encaminamiento	
		[E.15] Alteración accidental de la información	
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
		[E.25] Pérdida de equipos	
		[E.28] Indisponibilidad del personal	
	Falta de politicas para el manejo de información	[A.4] Manipulación de la configuración	Robo, pérdida o adulteración de información
		[A.6] Abuso de privilegios de acceso	
		[A.11] Acceso no autorizado	
		[A.14] Interceptación de información (escucha)	
		[A.18] Destrucción de información	
		[A.19] Divulgación de información	
		[A.23] Manipulación de los equipos	
		[A.25] Robo	
		[E.2] Errores del administrador	Inadecuada prestación del servicio
		[E.4] Errores de configuración	

Cuadro 12: (Continuación)

Correo electrónico	Falta de mecanismos control de acceso.	[A.7] Uso no previsto	Robo, pérdida o adulteración de información
		[A.8] Difusión de software dañino	
	Falta de politicas para el manejo de información	[A30] Ingeniería social (picaresca)	
		[E.2] Errores del administrador	
		[E.3] Errores de monitorización (log)	
		[E.4] Errores de configuración	
		[E.15] Alteración accidental de la información	
ERP- Sistema Clínico iMédicalCloud	Falta de mecanismos control de acceso	[E.1] Errores de los usuarios	Robo, pérdida o adulteración de información
		[E.2] Errores del administrador	
		[E.15] Alteración accidental de la información	
	No se cuenta con una nube privada	[E.18] Destrucción de información	
		[E.19] Fugas de información	
	Ataque de denegación de servicios	[A.11] Acceso no autorizado	
		[A.15] Modificación deliberada de la información	
		[A18] Destrucción de información	
		[A19] Divulgación de información	
	Denegación al acceso	[A24] Denegación de servicio	Indisponibilidad de servicio.
		[E.8] Difusión de software dañino	
Anydesk - Remoto a equipos	Falta de mecanismos control de acceso	[A19] Divulgación de información	Robo, pérdida o adulteración de información
		[A18] Destrucción de información	
		[E.8] Difusión de software dañino	
		[A.15] Modificación deliberada de la información	
	Falta de politicas para el manejo de información	[E.19] Fugas de información	
		[E.18] Destrucción de información	
Tipo: [SW] Software			
Sistemas operativos	Faltade instalación de parches de seguridad	[E.20] Vulnerabilidades de los programas (software)	Robo, pérdida o adulteración de información.
	Acceso no autorizado por la inadecuada administracion de puertos	[E.21] Errores de mantenimiento / actualización de programas (software)	Inadecuada utilización de las opciones del sistema o herramientas de software
	Habilitacion de brechas se seguridad	[E.2] Errores del administrador	
Antivirus	inoperancia del programa dejando expuesto el PC	[E.21] Errores de mantenimiento / actualización de programas (software)	Robo, pérdida o adulteración de información o sistema
	Acceso no autorizado	[E.2] Errores del administrador	
	Deshabilitar el escaneo a páginas de internet	[E.4] Errores de configuración	
		[E.18] Destrucción de información	
sql- Server.	Acceso no autorizado	[E.20] Vulnerabilidades de los programas (software)	Robo, pérdida o adulteración de información o sistema
		[A.6] Abuso de privilegios de acceso	
	Ejecución de codigo malicioso	[E.21] Errores de mantenimiento /	

Cuadro 12: (Continuación)

		actualización de programas (software)	
		[A.4] Manipulación de la configuración	
Helisa - Sistema contable	Ataques de SQL	[E.21] Errores de mantenimiento / actualización de programas (software)	Caída del sistema
	Falta de politicas de control de acceso	[A.4] Manipulación de la configuración	Robo, pérdida o adulteración de información o sistema
		[A.6] Abuso de privilegios de acceso	
		[A.11] Acceso no autorizado	
		[A.15] Modificación deliberada de la información	
		[A18] Destrucción de información	
		[A19] Divulgación de información	
		[A22] Manipulación de programas	
Tipo: [HW] Hardware			
Servidores	Equipo expuesto a la difusión de software malicioso y acceso no autorizados	[N.1] Fuego	Robo, pérdida o adulteración de información o del sistema
	No contar con politicas de respaldo de la información	[N.2] Daños por agua	Robo, pérdida o adulteración de información
	Intermitencia en el desarrollo de las actividades a cargo.	[N.*] Desastres naturales	Indisponibilidad en el uso del equipo
	Instalación o habilitación de software malicioso	[I.5] Avería de origen físico o lógico	Inadecuado funcionamiento del Equipo de computo
	Habilitación de brechas de seguridad (puertos)	[I.6] Corte del suministro eléctrico	Deficiencia en la prestación de un servicio por el no uso del PC
	Inoperancia del equipo de cómputo y acceso a información	[I.7] Condiciones inadecuadas de temperatura o humedad	
	Daño parcial o permanente en el equipo	[A25] Robo	
	Acceso no autorizado	[A26] Ataque destructivo	Afectación en la integridad de los archivos
	Daño parcial o permanente en el equipo	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Daño en componentes físicos o corrupción de archivos
		[N.1] Fuego	
		[N.2] Daños por agua	
		[N.*] Desastres naturales	
		[I.5] Avería de origen físico o lógico	
		[I.6] Corte del suministro eléctrico	

Cuadro 12: (Continuación)

Computadores / Portatiles /Tablet	Equipo expuesto a la difusión de software malicioso y acceso no autorizados	[I.6] Corte del suministro eléctrico	Robo, pérdida o adulteración de información o del sistema
	No contar con politicas de respaldo de la información	[I.7] Condiciones inadecuadas de temperatura o humedad	Robo, pérdida o adulteracion de información
	Intermitencia en el desarrollo de las actividades a cargo.	[A25] Robo	indisponibilidad en eluso del equipo
	Instalación o habilitación de software malicioso	[A26] Ataque destructivo	
	Habilitación de brechas de seguridad (puertos)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Inadecuado funcionamiento del Equipo de computo
	Inoperancia del equipo de cómputo y acceso a información	[E.19] Fugas de información	Deficiencia en la prestación de un servicio por el no uso del PC
	Daño parcial o permanente en el equipo	[E.25] Pérdida de equipos	Daño en componentes físicos o corrupción de archivos
	Acceso no autorizado	[N.1] Fuego	Afectación en la integridad de los archivos
	Daño parcial o permanente en el equipo	[N.2] Daños por agua	
		[N.*] Desastres naturales	
		[I.5] Avería de origen físico o lógico	
		[I.6] Corte del suministro eléctrico	
		[E.4] Errores de configuración	Robo o pérdida de información
Impresoras/Escaner	Se represan los documentos impresos en la bandeja de salida	[I.6] Corte del suministro eléctrico	Afectación en el uso del servicio
		[I.7] Condiciones inadecuadas de temperatura o humedad	
		[A25] Robo	
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
	Cuando se imprime por USB esta se contamina con virus	[E.19] Fugas de información	
		[E.25] Pérdida de equipos	
		[N.1] Fuego	
	Indisponibilidad en el funcionamiento	[N.2] Daños por agua	Robo o Pérdida de Información.
	Interrupción en el Servicio	[N.*] Desastres naturales	
	Falta de mantenimiento preventivo	[I.5] Avería de origen físico o lógico	
	Interrupción en el Servicio	[I.6] Corte del suministro eléctrico	Afectación en el uso del servicio
		[E.4] Errores de configuración	
Switches/Acces Point	Interrupción en el Servicio	[E.4] Errores de configuración	Afectación en la prestación del servicio
		[E.21] Errores de mantenimiento / actualización de programas (software)	
		[E.25] Pérdida de equipos	
		[A.4] Manipulación de la configuración	
		[A.6] Abuso de privilegios de acceso	
		[A.11] Acceso no autorizado	

Cuadro 12: (Continuación)

		[A.14] Interceptación de información	
		[A.23] Manipulación de los equipos	
		[A.25] Robo	
		[E.2] Errores del administrador	
		[E.3] Errores de monitorización (log)	
		[E.9] Errores de[re-]encaminamiento	
Equipo para Back UP	Falta de mecanismos control de acceso	[E.4] Errores de configuración	Robo, pérdida o adulteración de información o del sistema
		[E.19] Fugas de información	
		[A26] Ataque destructivo	pérdida de Información
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
	Inadecuada ubicación del archivo fisico	[A25] Robo	Deterioro de los archivos fisicos y lógicos
		[I.6] Corte del suministro eléctrico	
		[I.7] Condiciones inadecuadas de temperatura o humedad	
		[E.25] Pérdida de equipos	
		[N.1] Fuego	
		[N.2] Daños por agua	
		[N.*] Desastres naturales	
		[I.5] Avería de origen físico o lógico	
		[I.6] Corte del suministro eléctrico	
Router	Caida total o parcial del servicio de internet	[A25] Robo	Afectación en la prestación del servicio que depende de internet.
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
		[E.19] Fugas de información	
		[E.25] Pérdida de equipos	
		[N.1] Fuego	
		[N.2] Daños por agua	
		[N.*] Desastres naturales	
		[I.5] Avería de origen físico o lógico	
		[I.6] Corte del suministro eléctrico	
	Deficiencia en el acceso a las plataformas web	[E.4] Errores de configuración	Acceso limitado a la información y deterioro en la prestación del servicio
DVR	Falta de politicas de acceso	[A25] Robo	Robo, pérdida o adulteración de información
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
	Falta de cifrado SSL o Equivalente	[E.19] Fugas de información	
	Daño parcial o permanente en el equipo	[E.25] Pérdida de equipos	Daño en componentes físicos
		[N.1] Fuego	
		[N.2] Daños por agua	

Cuadro 12: (Continuación)

		[N.*] Desastres naturales	
	Falta de mantenimiento preventivo	[I.5] Avería de origen físico o lógico	
		[I.6] Corte del suministro eléctrico	
Biometricos	Ataques de inyección de datos biométricos	[A25] Robo	Suplantación de indentidad
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
	sensor puede presentar vulnerabilidades conforme biometría falsa	[E.19] Fugas de información	
	suplantación de identidad haciendo uso inescrupuloso y malicioso	[E.4] Errores de configuración	
Tipo: [COM] Redes de comunicaciones			
Red LAN	Lentitud en el servicio de comunicación	[E.24] Caída del sistema por agotamiento de recursos	Afectación en la calidad y pertinencia del servicio y/o la información.
		[E.28] Indisponibilidad del personal	
	Caída en parcial o total en el servicio	[A.12] Análisis de tráfico	
		[A.14] Interceptación de información	
		[E.2] Errores del administrador	
	Intermitencia en el servicio	[E.3] Errores de monitorización (log)	
		[E.9] Errores de[re-]encaminamiento	
Canales de comunicación contratados /Troncal SIP-movil	Caída en parcial o total en el servicio	[E.9] Errores de[re-]encaminamiento	Afectación en la calidad y pertinencia del servicio y/o la información.
		[E.24] Caída del sistema por agotamiento de recursos	
		[E.28] Indisponibilidad del personal	
		[A.12] Análisis de tráfico	
		[A.14] Interceptación de información (escucha)	
		[N.1] Fuego	
		[I.5] Avería de origen físico o lógico	
		[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipo: [Media] Soportes de información			
Memorias USB- Discos Duros	Equipo expuesto a la difusión de software malicioso y acceso no autorizados / No contar con politicas derespaldo de la información.	[I.7] Condiciones inadecuadas de temperatura o humedad	Robo, pérdida o adulteración de información
		[A25] Robo	
		[A26] Ataque destructivo	
		[N.1] Fuego	
		[N.2] Daños por agua	
	Acceso de Información confidencial por parte de terceros no autorizados	[E.19] Fugas de información	
[AUX] Equipamiento auxiliar			

Cuadro 12: (Continuación)

UPS en Centros datos	Deterioro en la vida útil de los componentes físicos	[I.7] Condiciones inadecuadas de temperatura o humedad	Funcionamiento inadecuado de los componentes que lo integran
		[A25] Robo	
		[A26] Ataque destructivo	
		[N.2] Daños por agua	
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Cableado estructurado	El tendido de cable no cumple según la normatividad vigente y Deterioro en la vida útil de los componentes físicos	[A26] Ataque destructivo	Afectación en la prestación del servicio que depende de internet.
		[N.*] Desastres naturales	
		[N.1] Fuego	
		[N.2] Daños por agua	Funcionamiento inadecuado de los componentes que lo integran
		[I.11] Emanaciones electromagnéticas	
Tipo: [L] Instalaciones físicas			
Centros de Datos	Caída total o parcial del servicio de internet	[N.2] Daños por agua	Afectación en la prestación del servicio que depende de internet.
		[N.*] Desastres naturales	
		[I.1] Fuego	
		[I.7]Condiciones inadecuadas de temperatura o humedad	Funcionamiento inadecuado de los componentes que lo integran
	Falta de politicas de acceso	[A.11] Acceso no autorizado	Hurto de equipos o acceso limitado a la informacion y deterioro en la presetación del servicio.
Tipo: [P] Personal			
Talento Humano	Acceder sin contar con los privilegios a equipos de cómputo o información física	[E.7] Deficiencias en la organización	Robo, pérdida o adulteración de información.
	Uso inadecuado de los permisos otorgados y recursos	[A.11] Acceso no autorizado	
	Instalación y uso de programas no autorizados que pueden habilitar el ingreso de archivos maliciosos o acceso no autorizados	[A.22]Manipulación de programas	
	No asumir su Rol frente a la protección de la información.	[A.28] Indisponibilidad del personal	Afectación en la prestación del servicio, manipulación de información.
	Acceso de Información confidencial por parte de terceros no autorizados	[A.30] Ingeniería social (picaresca)	Robo, pérdida o adulteración de información

Fuente: Elaboración propia

Cuadro 13. Distribución de amenazas según la valoración de su riesgo.

VALORACIÓN DEL RIESGO						
IMPACTO	MA		37	15	22	32
	A		54	47	27	0
	M		54	65	33	0
	B		3	50	2	6
	MB					
RIESGO		MB	B	M	A	MA
		PROBABILIDAD				

Fuente: Elaboración propia

Análisis de resultados teniendo en cuenta los riesgos críticos e Importantes.

Nivel Crítico:

Dentro de la valoración de los riesgos se observan los activos Backups de bases de datos, Manuales de contingencias / Manuales de los Sistemas Carpetas de archivos compartidos en red -diferentes áreas, Directorio Activo – Autenticación, Telefonía IP, Mesa de ayuda, Intranet, Sistema de Gestión Documental, Dropbox, ERP-Sistema Clínico iMédicalCloud, OneDrive, Isabel- Telefonía IP, sql- Server. Helisa - Sistema contable, cada uno de estos activos generan un imparto critico ante cualquier tipo de amenaza su impacto es mayor ya que en estos activos se

almacena información importantes, que puede ser sensible a divulgación, destrucción, fuga de información, alteración accidental, Robo o abuso de privilegios que conllevan a que un riesgo latente para Garper Médica, actualmente no se tiene un control mayor sobre los accesos a los usuarios, el área de tecnología solicita al área de Talento humano informar cada terminación de contrato de forma oportuna para realizar la inactivación de los usuarios a las diferentes plataformas de Garper, para evitar el acceso, hurto de datos o el mismo acceso a las instalaciones de la IPS, en muchas oportunidades se ha presentado que los usuarios se llevan la información, la editar o la borrar generando caos administrativos, y es necesaria la reconstrucción de los datos que se encuentran almacenados por ejemplo en la intranet, carpetas compartidas o Dropbox, sobre el sistema de información iMédicalCloud al no inactivarse los usuarios pueden acceder desde cualquier lugar ya que este sistema no se encuentra con acceso sobre una IP privada de Garper, los usuarios pueden ingresar desde cualquier lugar desde que sepan la URL, teniendo en cuenta lo anterior se genera un riesgo critico ya que a pesar de que la Historia Clínica no se puede editar, con ciertos permisos se puede registrar ciertas actividades a la historia clínica que generen un riesgo para sobre la seguridad e integridad del paciente.

Por otra parte, el activo correspondiente a la telefonía IP, también genera un nivel crítico, la IPS Garper Médica actualizó su servicio de call center, hizo la compra de servidores físicos en las diferentes sedes para lograr la comunicación por medio de un programa llamada Isabell el cual se encuentra instalado bajo el sistema Ubuntu, sin embargo, ha presentado algunas fallas por desconocimiento de las funcionalidades y posibles errores, adicionalmente el sistema no se encuentra visualizado, tampoco se ha realizado un análisis de posibles riesgos por puestos abiertos o por otras causas que puedan generar riesgos en sus servicios, es un riesgo critico ya que corresponde a todas entradas de la IPS es decir la asignación de las citas que es por donde se reciben los recursos de la IPS.

Con respecto a la documentación compartida en red y descargada en equipos de forma local, de forma desordenada y cualquier persona puede ingresar a esta información editarla, eliminarla, corresponde a un riesgo critico que se debe mitigar de forma oportuna para evitar el acceso y edición deliberada a la información.

Nivel Importante:

Analizando los riesgos de nivel importante encontramos los activos como son Base de datos Página Web, Base de datos Intranet, Backups de bases de datos, Código QR de Activos Físicos, Telefonía IP, Intranet, estos activos a pesar de que generaron sobre algunas amenazas riesgos Críticos también presentan un impacto Importante para la IPS sin embargo se pueden mitigar aplicando controles para que la materialización de estos llegue a generar interrupciones sobre la operación de la IPS.

Teniendo en cuenta el activo correspondiente a los activos fijos, Garper Médica ha creado un desarrollo propio que permite llevar una trazabilidad de todos los activos físicos de la organización, sin embargo se debe generar un control más robusto para el acceso a los usuarios ya que si el usuario accede a estos documentos puede observar la Hoja de vida de los equipos, manuales de usuarios, fichas técnicas y demás datos que corresponde a datos internos y creados por Garper Médica, no se encuentra diseñado un sistema de Back up sobre los documentos y módulos de la intranet incluido el módulo de activos fijos para evitar cualquier perdida de información.

Actividad 7: Plan de tratamiento de riesgos

Teniendo en cuenta la identificación de las amenazas a los que se encuentran expuestos los activos de la IPS Garper Médica y sus posibles riesgos se realiza un plan de tratamiento teniendo en cuenta los controles de la norma ISO 27001:2013 y salvaguarda sobre cada activo identificados en la tabla 7.

Cuadro 14. Plan de tratamiento de riesgos.

Nombre del Activo	Vulnerabilidad	Amenazas	Riesgo	Plan de tratamiento del riesgo		
				Tratamiento	Control ISO 27002:2013	Salvaguarda Propuesta
Tipo: [D] Datos						
Base de datos Página Web	Falta de mecanismos control de acceso	[A.11] Acceso no autorizado	Robo, pérdida o adulteración de información.	Mitigar el Riesgo	9.1.1 Política de control de accesos	Definir política de control acceso al archivo central de la dependencia a través de mecanismos eficientes que permitan el ingreso solo a personal autorizado. Según su cargo.
		[E.2] Errores del administrador	Pérdida de Información		11.1.4 Protección contra amenazas externas y del ambiente	Controlar el exceso de temperatura producto de la humedad. Reubicar el archivo centra en otro sitio.
		[E.15] Alteración accidental de la información	Adulteración de información.		9.4.1 Restricción del acceso a la información.	
	Falta de politicas respecto a abuso de los privilegios de la base de datos	[E.19] Fugas de información	Robo de materiales de formación		9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Implementar políticas de respaldo de información así mismo revisar contantemente los privilegios de los usuarios para evitar la edición deliberada de la información, realizando así concientización sobre seguridad de la información y de esta forma lograr un entorno seguro.
		[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de Information		14.2.2 Procedimientos de control de cambios en los sistemas.	
		[A.3] Manipulación de los registros de actividad (log)	Adulteración de información.		9.2.5 Revisión de los derechos de acceso de los usuarios.	

Cuadro 14: (Continuación)

	falta de politicas para el manejo de información	[A.15] Modificación deliberada de la información	Robo, pérdida o adulteración de información.		7.2.2 Concienciación, educación y capacitación en segur. de la informac.	
		[A.19] Divulgación de información	Adulteración de información.			
		[E.20] Vulnerabilidades de los programas (software)	Indisponibilidad de servicio.		14.2.6 Seguridad en entornos de desarrollo.	
		[A.24] Denegación de servicio	Caída del sistema			
		[A.6] Abuso de privilegios de acceso	Pérdida de confianza y acceso a la información		14.2.4 Restricciones a los cambios en los paquetes de software.	
		[E.15] Alteración accidental de la información	Indisponibilidad de servicio.		9.4.1 Restricción del acceso a la información	
Base de datos Intranet	Falta de mecanismos control de acceso	[E.20] Vulnerabilidades de los programas(software)	Indisponibilidad de servicio.	Mitigar el Riesgo	11.2.4 Mantenimiento de equipos	Definir plan de actualización y verificación de su correcto funcionamiento
		[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de Información		9.1.1 Política de control de accesos	
		[E.28] Indisponibilidad del personal	Pérdida de confianza y acceso a la información		9.4.1 Restricción del acceso a la información.	
	Falta de politicas respecto a abuso de los privilegios de la base de datos	[A.4] Manipulación de la configuración	Robo, pérdida o adulteración de información.		9.2.3 Gestión de los derechos de acceso con privilegios especiales	
		[A.15] Modificación deliberada de la información				
		[A18] Destrucción de información	pérdida de Información			
	falta de politicas para el manejo de información	[A19] Divulgación de información	Adulteración de información.		7.2.2 Concienciación, educación y capacitación en segur. de la información	
		[E.8] Difusión de software dañino	Caída del sistema			
		[E.19] Fugas de información	Robo de materiales de formación			
		[A.11] Acceso no autorizado	Pérdida de confianza y acceso a la información			

Cuadro 14: (Continuación)

Base de datos E-learning	Falta de mecanismos control de acceso	[A.11] Acceso no autorizado	Pérdida de confianza y acceso a la información	Mitigar el Riesgo	9.4.1 Restricción del acceso a la información.	Definir y capacitar sobre la creación de contraseñas teniendo en cuenta una estructura segura y robusta.
		[E.19] Fugas de información				
		[A.15] Modificación deliberada de la información				
		[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de Información		9.1.1 Política de control de accesos	
Backups de bases de datos	Falta de mecanismos control de acceso	[E.15] Alteración accidental de la información	Adulteración de información.	Mitigar el Riesgo	9.4.1 Restricción del acceso a la información.	Implementar políticas correspondientes a seguridad de la información, robustez en contraseñas e implementación de Back up deforma automatizada, ante cualquier perdida de información se cuente con un registro de actividad y poder rápidamente restablecer los datos que fueron vulnerados o robados.
		[E.18] Destrucción de información	Pérdida de Información			
	Falta de politicas para el manejo de información	[E.19] Fugas de información	Robo o Pérdida de Información.		5.1.1 Conjunto de políticas para la seguridad de la información	
	Falta de mecanismos de control durante la asignación al instructor.	[E.28] Indisponibilidad del personal	Algunos programas no reciben la totalidad de materiales de formación.		12.3.1 Copias de seguridad de la información	
	Falta de políticas respecto a abuso de los privilegios de la base de datos	[A.18] Destrucción de información	pérdida de Información		12.4.3 Registros de actividad del administrador y operador del sistema.	
		[A.19] Divulgación de información	Adulteración de información.		12.4.1 Registro y gestión de eventos de actividad.	
	Denegación al acceso	[I.8] Fallo de servicios de comunicaciones	Inadecuada prestación del servicio		12.4.2 Protección de los registros de información.	
	Habilitación de brechas de seguridad	[E.2] Errores del administrador	Falta de eficiencia para general las respuesta		2.6.1 Gestión de las vulnerabilidades técnicas.	
Manuales de contingencias / Manuales de los Sistemas	Falta de politicas respecto a abuso de los privilegios de la base de datos	[E.18] Destrucción de información	Robo, pérdida o adulteración de información.	Mitigar el Riesgo	9.2.4 Gestión de información confidencial de autenticación de usuarios.	Definir un plan de capacitaciones al personal correspondiente a la seguridad de la información y las responsabilidades ante cualquier
		[E.19] Fugas de información				
		[A.15] Modificación				

Cuadro 14: (Continuación)

		deliberada de la información				abuso o adulteración de la información
		[A.18] Destrucción de información				
		[A.19] Divulgación de información				
	Habilitación de brechas de seguridad	[E.2] Errores del administrador	Falta de eficiencia para general las respuestas		16.1.1 Responsabilidades y procedimientos.	
	Falta de politicas para el manejo de información	[E.3] Errores de monitorización (log)	Falta de eficiencia para general las respuesta		7.2.2 Concienciación, educación y capacitación en segur. de la información	
		[E.7] Deficiencias en la organización	Abuso de privilegios de acceso			
		[E.15] Alteración accidental de la información	Adulteración de información.			
Carpetas de archivos compartidos en red -diferentes áreas	Falta de políticas respecto a abuso de los privilegios de la base de datos	[E.18] Destrucción de información	Robo, pérdida o adulteración de información.	Mitigar el Riesgo	6.1.1 Asignación de responsabilidades para la segur. de la información.	Definir un plan de capacitaciones al personal correspondiente a la seguridad de la información, responsabilidades y acciones ante cualquier abuso o adulteración de la información
		[E.19] Fugas de información				
		[E.20] Vulnerabilidades de los programas (software)				
	Falta de mecanismos control de acceso	[E.21] Errores de mantenimiento / actualización de programas (software)				
		[E.28] Indisponibilidad del persona	Falta de eficiencia para general las respuestas		9.1 Requisitos de negocio para el control de accesos.	
		[A.4] Manipulación de la configuración				
		[A.6] Abuso de privilegios de acceso				
		[A.11] Acceso no autorizado				
	Falta de políticas para el manejo de información	[A.15] Modificación deliberada de la información	Robo, pérdida o adulteración de información.		7.2.2 Concienciación, educación y capacitación en segur. de la información	
		[A18] Destrucción de información				
		[A19] Divulgación de información				

Cuadro 14: (Continuación)

		[E.1] Errores de los usuarios				
		[E.15] Alteración accidental de la información				
		[E.19] Fugas de información				
Backups Correos	Falta de politicas para el manejo de información	[E.18] Destrucción de información	Robo, pérdida o adulteración de información	Mitigar el Riesgo	12.3.1 Copias de seguridad de la información.	Definir un cronograma para la revisión de la información que esta se encuentre debidamente clasificada, trazabilidad de las copias y log de actividades sobre posible adulteración fuga de información
		[E.19] Fugas de información				
		[A.19] Divulgación de información				
		[I.8] Fallo de servicios de comunicaciones				
		[E.2] Errores del administrador				
		[E.20] Vulnerabilidades de los programas (software)				
Datos de gestión interna	Falta de politicas para el manejo de información	[E.21] Errores de mantenimiento /actualización de programas (software)	Copiar los virus a los equipos de computo	Mitigar el Riesgo	11.2.4 Mantenimiento de equipos	Establecer plan de mantenimiento y actualización de software
		[E.28] Indisponibilidad del personal	Afectación en la integridad de los archivos		6.1.1 Asignación de responsabilidades para la segur. de la información.	Definir un cronograma para la revisión de la información que esta se encuentre debidamente clasificada, trazabilidad de las copias y log de actividades sobre posible adulteración fuga de información.
		[A.4] Manipulación de la configuración	Robo o Pérdida de Información.			
	Falta de mecanismos control de acceso	[A.6] Abuso de privilegios de acceso	Robo, pérdida o adulteración de información		6.1.1 Asignación de responsabilidades para la segur. de la información.	Definir política de control acceso al archivo central de la dependencia a través de mecanismos eficientes que permita el ingreso solo a personal autorizado. Sagun el cargo.
		[A.11] Acceso no autorizado				
		[A.15] Modificación deliberada de la información				
		[E.14] Escapes de información				
		[E.15] Alteración accidental de la información				
		[A18] Destrucción de información				

Cuadro 14: (Continuación)

		[A19] Divulgación de información				
		[A22] Manipulación de programas				
		[E.1] Errores de los usuarios				
Tipo: [K] Claves criptográficas						
Código QR de Activos Fisicos	Falta de politicas para uso de claves	[E.15] Alteración accidental de la información	Robo, pérdida o adulteración de información	Mitigar el Riesgo	10.1.2 Gestión de claves.	Implementar políticas que tengan en cuenta la generación uso, protección, distribución y renovación. Manejo de solicitudes legales teniendo en cuenta la clasificación de la información
		[E.2] Errores del administrador				
		[E.4] Errores de configuración				
		[E.20] Vulnerabilidades de los programas (software)				
		[E.14] Escapes de información				
Tipo: [SW] Servicios						
Directorio Activo - Autenticación	Falta de mecanismos control de acceso	[A.4] Manipulación de la configuración	Robo o Pérdida de Información.	Mitigar el Riesgo	9.1.2 Control de acceso a las redes y servicios asociados.	Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información.
		[A.6] Abuso de privilegios de acceso	Afectación en la integridad de los archivos		9.1.1 Política de control de accesos	
	Falta de politicas para el manejo de información	[A.15] Modificación deliberada de la información	Indisponibilidad de servicio.			
		[A.18] Destrucción de información	Robo, pérdida o adulteración de información		7.2.2 Concienciación, educación y capacitación en segur. de la información	Desarrollar un plan de capacitación para que los empleados sean conscientes y que cumplan con las responsabilidades relacionadas con la seguridad de la información
		[A.19] Divulgación de información				
Telefonía IP	Falta de mecanismos control de acceso	[I.6] Corte del suministro eléctrico	Extraer el tráfico de la red para obtener la conversación	Mitigar el Riesgo	11.2.2 Servicios de suministro	Conectar a una UPS o al sistema regulado para evitar afectación por fallas en el fluido eléctrico
		[I.7] Condiciones inadecuadas de temperatura o humedad				
		[I.8] Fallo de servicios de comunicaciones			14.1.2 Seguridad de las comunicacione	Implementar políticas de control de acceso

Cuadro 14: (Continuación)

		[E.2] Errores del administrador			s en servicios accesibles por redes públicas.	y configuración del firewall
		[E.4] Errores de configuración				
		[E.9] Errores de[re-]encaminamiento				
		[E.15] Alteración accidental de la información				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)				
		[E.25] Pérdida de equipos				
		[E.28] Indisponibilidad del personal				
	Falta de politicas para el manejo de información	[A.4] Manipulación de la configuración	Robo, pérdida o adulteración de información		13.1.2 Mecanismos de seguridad asociados a servicios en red.	Mantener la seguridad de la información intercambiada dentro de una organización y con cualquier otra entidad.
		[A.6] Abuso de privilegios de acceso				
		[A.11] Acceso no autorizado				
		[A.14] Interceptación de información (escucha)				
		[A.18] Destrucción de información				
		[A.19] Divulgación de información				
		[A.23] Manipulación de los equipos				
		[A.25] Robo				
		[E.2] Errores del administrador	Inadecuada prestación del servicio		16.1.2 Notificación de los eventos de seguridad de la información.	
		[E.4] Errores de configuración				
Correo electrónico	Falta de mecanismos control de acceso.	[A.7] Uso no previsto	Robo, pérdida o adulteración de información	Mitigar el Riesgo	9.1.2 Control de acceso a las redes y servicios asociados.	Implementar políticas de control de acceso
		[A.8] Difusión de software dañino				
	Falta de politicas para el manejo de información	[A30] Ingeniería social (picaresca)			9.3.1 Uso de información confidencial para la autenticación.	Desarrollar un plan de capacitación para que los empleados sean
		[E.2] Errores del administrador				

Cuadro 14: (Continuación)

		[E.3] Errores de monitorización (log)				conscientes y que cumplan con las responsabilidades relacionadas con la seguridad de la información
		[E.4] Errores de configuración				
		[E.15] Alteración accidental de la información				
ERP- Sistema Clínico iMédicalCloud	Falta de mecanismos control de acceso	[E.1] Errores de los usuarios	Robo, pérdida o adulteración de información	Mitigar el Riesgo	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	Desarrollar un plan de capacitación para que los empleados sean conscientes y que cumplan con las responsabilidades relacionadas con la seguridad de la información
		[E.2] Errores del administrador				
		[E.15] Alteración accidental de la información				
	No se cuenta con una nube privada	[E.18] Destrucción de información			5.1.1 Conjunto de políticas para la seguridad de la información.	
		[E.19] Fugas de información				
	Ataque de denegación de servicios	[A.11] Acceso no autorizado			9.1.1 Política de control de accesos.	
		[A.15] Modificación deliberada de la información				
		[A18] Destrucción de información				
		[A19] Divulgación de información				
	Denegación al acceso	[A24] Denegación de servicio	Indisponibilidad de servicio.		18.1.4 Protección de datos y privacidad de la información personal.	
		[E.8] Difusión de software dañino			16.1.5 Respuesta a los incidentes de seguridad	
Anydesk - Remoto a equipos	Falta de mecanismos control de acceso	[A19] Divulgación de información	Robo, pérdida o adulteración de información	Mitigar el Riesgo	9.4.1 Restricción del acceso a la información.	Plan de capacitación sobre el uso adecuado de los recursos informáticos y aplicación de políticas de seguridad
		[A18] Destrucción de información				
		[E.8] Difusión de software dañino				
		[A.15] Modificación deliberada de la información				
	Falta de politicas para el manejo de información	[E.19] Fugas de información				
		[E.18] Destrucción de información				
Tipo: [SW] Software						

Cuadro 14: (Continuación)

Sistemas operativos	Faltade instalación de parches de seguridad	[E.20] Vulnerabilidades de los programas (software)	Robo, pérdida o adulteración de información.	Mitigar el Riesgo	12.6.1 Gestión de las vulnerabilidades técnicas.	Definir plan de mantenimiento y actualización del sistema operativo
	Acceso no autorizado por la inadecuada administración de puertos	[E.21] Errores de mantenimiento / actualización de programas (software)	Inadecuada utilización de las opciones del sistema o herramientas de software		9.1.1 Política de control de accesos.	Implementar políticas de control de acceso y configuración del firewall
	Habilitación de brechas se seguridad	[E.2] Errores del administrador			12.2.1 Controles contra software malicioso	Instalar software antivirus, Antispyware y mantener actualizada la base de datos.
Antivirus	inoperancia del programa dejando expuesto el PC	[E.21] Errores de mantenimiento / actualización de programas (software)	Robo, pérdida o adulteración de información o sistema	Mitigar el Riesgo	1.2.4 Mantenimiento de equipos	Definir plan de mantenimiento, actualización del sistema operativo y programas asociados
	Acceso no autorizado	[E.2] Errores del administrador			7.2.2 Conciencia, educación y entrenamiento de seguridad de la información	Definir plan de capacitación sobre la adopción de políticas de seguridad para proteger la información y los equipos.
	Deshabilitar el escaneo a páginas de internet	[E.4] Errores de configuración				
		[E.18] Destrucción de información				
sql- Server.	Acceso no autorizado	[E.20] Vulnerabilidades de los programas (software)	Robo, pérdida o adulteración de información o sistema	Mitigar el Riesgo	11.2.4 Mantenimiento de equipos	Definir plan de actualización y verificación de su correcto funcionamiento
		[A.6] Abuso de privilegios de acceso			9.2.3 Gestión de los derechos de acceso con privilegios especiales.	
	Ejecución de codigo malicioso	[E.21] Errores de mantenimiento / actualización de programas (software)			12.6.2 Restricciones en la instalación de software.	
		[A.4] Manipulación de la configuración			12.2.1 Controles contra el código malicioso.	
Helisa - Sistema contable	Ataques de SQL	[E.21] Errores de mantenimiento / actualización de programas (software)	Caída del sistema	Mitigar el Riesgo	12.6.2 Restricciones en la instalación de software.	
	Falta de politicas de	[A.4] Manipulación de la configuración	Robo, pérdida o adulteración		9.1.1 Política de control de accesos.	

Cuadro 14: (Continuación)

	control de acceso	[A.6] Abuso de privilegios de acceso	de información o sistema		9.2.6 Retirada o adaptación de los derechos de acceso	
		[A.11] Acceso no autorizado			9.2.1 Gestión de altas/bajas en el registro de usuarios.	
		[A.15] Modificación deliberada de la información			9.2.3 Gestión de derechos de acceso privilegiados	Establecer políticas de control de acceso y privilegios. Sagun Rol del funcionario.
		[A18] Destrucción de información				
		[A19] Divulgación de información				
		[A22] Manipulación de programas				
Tipo: [HW] Hardware						
Servidores	Equipo expuesto a la difusión de software malicioso y acceso no autorizados	[N.1] Fuego	Robo, pérdida o adulteración de información o del sistema	Mitigar el Riesgo	12.3.1 Respaldo de información	Realizar plan de respaldo de la información producida en la dependencia de formación.
	No contar con politicas de respaldo de la información	[N.2] Daños por agua	Robo, pérdida o adulteración de información			
	Intermitencia en el desarrollo de las actividades a cargo.	[N.*] Desastres naturales	Indisponibilidad en el uso del equipo			
	Instalación o habilitación de software malicioso	[I.5] Avería de origen físico o lógico	Inadecuado funcionamiento del Equipo de computo		11.2.4 Mantenimiento de equipos	Plan de mantenimiento y verificación de los dispositivos, para prevenir fallas y deterioro
	Habilitación de brechas de seguridad (puertos)	[I.6] Corte del suministro eléctrico	Deficiencia en la prestación de un servicio por el no uso del PC		11.2.2 Servicios de suministro	Instalar UPS o sistema regulado para garantizar el fluido eléctrico y no sé presente perdida de información y afectaciones a los equipos de Computo
	Inoperancia del equipo de cómputo y acceso a información	[I.7] Condiciones inadecuadas de temperatura o humedad			11.1.4 Protección contra amenazas externas y del ambiente	Plan de mitigación por el exceso de luz natural que afecta los equipos

Cuadro 14: (Continuación)

	Daño parcial o permanente en el equipo	[A25] Robo			12.3.1 Respaldo de información	Realizar plan de respaldo de la información producida en la dependencia de fo
	Acceso no autorizado	[A26] Ataque destructivo	Afectación en la integridad de los archivos			
	Daño parcial o permanente en el equipo	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Daño en componentes físicos o corrupción de archivos		11.2.2 Servicios de suministro	Instalar UPS o sistema regulado para garantizar el fluido eléctrico y no sé presente perdida de información y afectaciones a los equipos de cómputo.
		[N.1] Fuego				
		[N.2] Daños por agua				
		[N.*] Desastres naturales				
		[I.5] Avería de origen físico o lógico				
		[I.6] Corte del suministro eléctrico				
Computadores / Portatiles /Tablet	Equipo expuesto a la difusión de software malicioso y acceso no autorizados	[I.6] Corte del suministro eléctrico	Robo, pérdida o adulteración de información o del sistema	Mitigar el Riesgo	11.2.2 Servicios de suministro	Conectar a una UPS o al sistema regulado para evitar afectación por fallas en el fluido eléctrico
	No contar con politicas de respaldo de la información	[I.7] Condiciones inadecuadas de temperatura o humedad	Robo, pérdida o adulteracion de información		11.1.4 Protección contra amenazas externas y del ambiente	Definir un plan para controlar la baja temperatura producida por la humedad
	Intermitencia en el desarrollo de las actividades a cargo.	[A25] Robo	indisponibilidad en eluso del equipo		12.3.1 Respaldo de información	Realizar plan de respaldo de la información producida en la dependencia de formación.
	Instalación o habilitación de software malicioso	[A26] Ataque destructivo				
	Habilitación de brechas de seguridad (puertos)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Inadecuado funcionamiento del Equipo de computo			
	Inoperancia del equipo de cómputo y acceso a información	[E.19] Fugas de información	Deficiencia en la prestación de un servicio por el no uso del PC			

Cuadro 14: (Continuación)

	Daño parcial o permanente en el equipo	[E.25] Pérdida de equipos	Daño en componentes físicos o corrupción de archivos			
	Acceso no autorizado	[N.1] Fuego	Afectación en la integridad de los archivos		11.1.4 Protección contra amenazas externas y del ambiente	Plan de mitigación por el exceso de luz natural que afecta los equipos
	Daño parcial o permanente en el equipo	[N.2] Daños por agua				
		[N.*] Desastres naturales				
		[I.5] Avería de origen físico o lógico				
		[I.6] Corte del suministro eléctrico				
		[E.4] Errores de configuración	Robo o pérdida de información		12.3.1 Respaldo de información	Realizar plan de respaldo de la información producida en la dependencia de formación.
Impresoras/Escaner	Se represan los documentos impresos en la bandeja de salida	[I.6] Corte del suministro eléctrico	Afectación en el uso del servicio	Mitigar el Riesgo	11.1.4 Protección contra amenazas externas y del ambiente	Plan para mitigación de posibles riesgos derivados por la naturaleza o accesos no permitidos
		[I.7] Condiciones inadecuadas de temperatura o humedad				
		[A25] Robo				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)				
	Cuando se imprime por USB esta se contamina con virus	[E.19] Fugas de información				
		[E.25] Pérdida de equipos				
		[N.1] Fuego				
	Indisponibilidad en el funcionamiento	[N.2] Daños por agua	Robo o Pérdida de Información.			
	Interrupción en el Servicio	[N.*] Desastres naturales			11.2.4 Mantenimiento de los equipos.	Plan de mantenimiento y verificación de los dispositivos, para prevenir fallas y deterioro
	Falta de mantenimiento preventivo	[I.5] Avería de origen físico o lógico				
	Interrupción en el Servicio	[I.6] Corte del suministro eléctrico	Afectación en el uso del servicio			
		[E.4] Errores de configuración				

Cuadro 14: (Continuación)

Switches/Access Point	Interrupción en el Servicio	[E.4] Errores de configuración	Afectación en la prestación del servicio	Mitigar el Riesgo	11.1.4 Protección contra amenazas externas y del ambiente	Plan para mitigación de posibles riesgos derivados por la naturaleza o accesos no permitidos
		[E.21] Errores de mantenimiento / actualización de programas (software)				
		[E.25] Pérdida de equipos				
		[A.4] Manipulación de la configuración			9.2.3 Gestión de derechos de acceso privilegiados	
		[A.6] Abuso de privilegios de acceso				
		[A.11] Acceso no autorizado				Establecer políticas de control de acceso y privilegios. Según Rol del funcionario
		[A.14] Interceptación de información				
		[A.23] Manipulación de los equipos				
		[A.25] Robo				
		[E.2] Errores del administrador				
		[E.3] Errores de monitorización (log)			11.2.4 Mantenimiento de equipos	Plan de mantenimiento y verificación de los dispositivos, para prevenir fallas y deterioro
		[E.9] Errores de[re-]encaminamiento				
Equipo para Back UP	Falta de mecanismos control de acceso	[E.4] Errores de configuración	Robo, pérdida o adulteración de información o del sistema	Mitigar el Riesgo	9.1.2 Control de acceso a las redes y servicios asociados.	Asegurar el acceso de usuarios autorizados y prevenir el acceso n autorizado a los servicios y servicios de información
		[E.19] Fugas de información				
		[A26] Ataque destructivo	pérdida de Información			
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)				
	Inadecuada ubicación del archivo fisico	[A25] Robo	Deterioro de los archivos físicos y lógicos		11.1.4 Protección contra las amenazas externas y ambientales.	Prevenir pérdidas, daños, hurtos o comprometer los activos, así como la interrupción de las actividades de la organización.
		[I.6] Corte del suministro eléctrico				
		[I.7] Condiciones inadecuadas de temperatura o humedad				
		[E.25] Pérdida de equipos				

Cuadro 14: (Continuación)

		[N.1] Fuego				
		[N.2] Daños por agua				
		[N.*] Desastres naturales				
		[I.5] Avería de origen físico o lógico				
		[I.6] Corte del suministro eléctrico				
Router	Caida total o parcial del servicio de internet	[A25] Robo	Afectación en la prestación del servicio que depende de internet.	Mitigar el Riesgo	11.2.2 Instalaciones de suministro.	Establecer medidas de control para el suministro necesario para mantener operativas las instalaciones y los equipos
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)				
		[E.19] Fugas de información				
		[E.25] Pérdida de equipos				
		[N.1] Fuego				
		[N.2] Daños por agua				
		[N.*] Desastres naturales				
		[I.5] Avería de origen físico o lógico				
		[I.6] Corte del suministro eléctrico				
	Deficiencia en el acceso a las plataformas web	[E.4] Errores de configuración	Acceso limitado a la información y deterioro en la prestación del servicio		7.2.2 Conciencia, educación y entrenamiento de seguridad de la información	Establecer un plan de configuración, actualización y verificación de buenas prácticas para el acceso a la información a través de políticas de seguridad y acceso a la información.
DVR	Falta de políticas de acceso	[A25] Robo	Robo, pérdida o adulteración de información	Mitigar el Riesgo	9.1.1 Política de control de acceso	Definir politicas de control de acceso y otorgamiento de privilegios en función al Rol.
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)				
	Falta de cifrado SSL o Equivalente	[E.19] Fugas de información				
	Daño parcial o permanente en el equipo	[E.25] Pérdida de equipos	Daño en componentes físicos		11.2.2 Instalaciones de suministro.	Instalar UPS o sistema regulado para garantizar el fluido eléctrico y
		[N.1] Fuego				

Cuadro 14: (Continuación)

		[N.2] Daños por agua				no sé presente perdida de información y afectaciones
		[N.*] Desastres naturales				
	Falta de mantenimiento preventivo	[I.5] Avería de origen físico o lógico				
		[I.6] Corte del suministro eléctrico				
Biometricos	Ataques de inyección de datos biométricos	[A25] Robo	Suplantación de indentidad	Mitigar el Riesgo	9.4.2 Procedimientos seguros de inicio de sesión.	se debe considerar la autenticación sólida por encima y más allá de la simple identificación de usuario y contraseña. (Controles adicionales físicos o lógicos)
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)				
	sensor puede presentar vulnerabilidades conforme biometría falsa	[E.19] Fugas de información				
	suplantación de identidad haciendo uso inescrupuloso y malicioso	[E.4] Errores de configuración				
Tipo: [COM] Redes de comunicaciones						
Red LAN	Lentitud en el servicio de comunicación	[E.24] Caída del sistema por agotamiento de recursos	Afectación en la calidad y pertinencia del servicio y/o la información.	Mitigar el Riesgo	15.1.1 Política de seguridad de la información en las relaciones con el proveedor	Negociar con el proveedor una ampliación en el ancho de banda, el cual permita mejorar el tiempo de cargue de las aplicaciones web y dar respuesta eficiente a las tareas asignadas que dependen de este servicio.
		[E.28] Indisponibilidad del personal				
	Caída en parcial o total en el servicio	[A.12] Análisis de tráfico				
		[A.14] Interceptación de información				
		[E.2] Errores del administrador				
	Intermitencia en el servicio	[E.3] Errores de monitorización (log)				
		[E.9] Errores de[re-]encaminamiento				
Canales de comunicación contratados /Troncal SIP-movil	Caída en parcial o total en el servicio	[E.9] Errores de[re-]encaminamiento	Afectación en la calidad y pertinencia del servicio y/o la información.	Mitigar el Riesgo	14.1.2 Aseguramiento o de servicios de aplicación en redes públicas	Instalar y configurar adecuado firewall y Router.
		[E.24] Caída del sistema por agotamiento de recursos				

Cuadro 14: (Continuación)

		[E.28] Indisponibilidad del personal				
		[A.12] Análisis de tráfico				
		[A.14] Interceptación de información (escucha)				
		[N.1] Fuego				
		[I.5] Avería de origen físico o lógico				
		[E.21] Errores de mantenimiento / actualización de programas (software)			13.1.1 Controles de redes	
Tipo: [Media] Soportes de información						
Memorias USB-Discos Duros	Equipo expuesto a la difusión de software malicioso y acceso no autorizados / No contar con politicas derespaldo de la información.	[I.7] Condiciones inadecuadas de temperatura o humedad	Robo, pérdida o adulteración de información	Mitigar el Riesgo	12.2.1 Controles contra software malicioso	controlar el uso de memoria USB evitando así la propagación de archivos maliciosos en los equipos.
		[A25] Robo				
		[A26] Ataque destructivo				
		[N.1] Fuego				
		[N.2] Daños por agua				
	Acceso de Información confidencial por parte de terceros no autorizados	[E.19] Fugas de información			9.1.1 Política de control de accesos.	Definir las pautas generales para asegurar un acceso controlado a la Información
Tipo: [AUX] Equipamiento auxiliar						
UPS en Centros datos	Deterioro en la vida útil de los componentes físicos	[I.7] Condiciones inadecuadas de temperatura o humedad	Funcionamiento inadecuado de los componentes que lo integran	Mitigar el Riesgo	11.1.4 Protección contra amenazas externas y del ambiente	Plan de mantenimiento y verificación de los dispositivos y accesos, para prevenir fallas, deterioro o ataques por terceros
		[A25] Robo				
		[A26] Ataque destructivo				
		[N.2] Daños por agua				
		[E.23] Errores de mantenimiento / actualiz ación de equipos (hardware)			11.2.4 Mantenimiento de equipos	
Cableado estructurado	El tendido de cable no cumple según la	[A26] Ataque destructivo	Afectación en la prestación del servicio		11.1.2 Controles físicos de entrada	

Cuadro 14: (Continuación)

	normatividad vigente y Deterioro en la vida útil de los componentes físicos	[N.*] Desastres naturales	que depende de internet.		11.1.4 Protección contra amenazas externas y del ambiente	
		[N.1] Fuego				
		[N.2] Daños por agua	Funcionamiento inadecuado de los componentes que lo integran			
		[I.11] Emanaciones electromagnéticas				
Tipo: [L] Instalaciones físicas						
Centros de Datos	Caída total o parcial del servicio de internet	[N.2] Daños por agua	Afectación en la prestación del servicio que depende de internet.	Mitigar el Riesgo	17.1.1 Planificación de la continuidad de la seguridad de la información	Crear plan de contingencia para continuar con la prestación de los servicios.
		[N.*] Desastres naturales				
		[I.1] Fuego				
		[I.7]Condiciones inadecuadas de temperatura o humedad	Funcionamiento inadecuado de los componentes que lo integran		11.1.4 Protección contra amenazas externas y del ambiente	Definir un plan que determine las condiciones de seguridad para que no sé afecte el gabinete por la humedad
	Falta de politicas de acceso	[A.11] Acceso no autorizado	Hurto de equipos o acceso limitado a la informacion y deterioro en la presetación del servicio.		7.2.2 Conciencia, educación y entrenamiento de seguridad de la información	Establecer un plan de configuración, actualización y verificación de buenas prácticas para el acceso a la información a través de políticas de seguridad y acceso a la información.
Tipo: [P] Personal						
Talento Humano	Acceder sin contar con los privilegios a equipos de cómputo o información física	[E.7] Deficiencias en la organización	Robo, pérdida o adulteración de información.	Mitigar el Riesgo	9.2.3 Gestión de derechos de acceso privilegiados	Establecer plan de capacitación al personal de la dependencia sobre políticas de seguridad y uso adecuado de los recursos TIC
	Uso inadecuado de los permisos otorgados y recursos	[A.11] Acceso no autorizado			9.1.1 Política de control de acceso	Definir políticas de control de acceso y otorgamiento de privilegios en función al Rol.

Cuadro 14: (Continuación)

	Instalación y uso de programas no autorizados que pueden habilitar el ingreso de archivos maliciosos o acceso no autorizados	[A.22] Manipulación de programas			7.2.2 Conciencia, educación y entrenamiento de seguridad de la información	Establecer plan de capacitación al personal de la dependencia sobre políticas de seguridad y uso adecuado de los recursos TIC
	No asumir su Rol frente a la protección de la información.	[A.28] Indisponibilidad del personal	Afectación en la prestación del servicio, manipulación de información.			Establecer plan de capacitación al personal de la dependencia sobre políticas de seguridad de la información y uso adecuado de los recursos TIC. Igualmente, la normatividad sobre la protección de los datos personales
	Acceso de Información confidencial por parte de terceros no autorizados	[A.30] Ingeniería social (picaresca)	Robo, pérdida o adulteración de información			

Fuente: Elaboración propia

Actividad 8. Documento de aplicabilidad.

La declaración de aplicabilidad SOA de la norma ISO/IEC 27001:2013, de Sistemas de Gestión de Seguridad de la Información (SGSI), es un instrumento desarrollado por la relación completa de los controles de seguridad de la información evaluables, que se indican en el anexo A de la norma.

Las características de este documento de aplicabilidad corresponden a la inclusión de controles teniendo en cuenta el estándar, la definición de la aplicabilidad de o no, con las respectivas justificaciones de dichos controles, de esta forma permite la trazabilidad entre los controles de aplicabilidad y la realizar de los procesos ejecutados en la IPS Garper Médica SAS.

La presente declaración contiene controles que son importantes para la IPS Garper Médica SAS, con sus justificaciones de inclusión o exclusión de algunos controles.

Cuadro 15. Declaración de aplicabilidad

Garper Médica	**GARCIA PÉREZ MÉDICA Y COMPAÑÍA SAS-GARPER MÉDICA-** **Declaración de aplicabilidad (SOA)**							**Código:**	**GCA-FT-03**
								Versión:	**1**
								Fecha:	**1/04/2021**
								Páginas:	**1 de 1**
En la presente declaración se definen los controles que son relevantes para la IPS GARPER MÉDICA SAS. en este se encuentra el control planteado, la justificada y la exclusión de algunos de los controles. LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas, RRA: resultado de la valoración de riesgos								Elaboró: Ing. Irma Criollo Betancourt	
Sección	**Objetivo de control**	**Descripción del control ISO 27002:2013**	**Control Seleccionado**	**Justificación de exclusión**	**Razones de selección**				**Control planeado**
					LR	**CO**	**BR/BP**	**RRA**	
5.	**POLITICAS DE SEGURIDAD.**								
5.1	**Directrices de la Dirección en seguridad de la información.**								
5.1.1	Conjunto de políticas para la seguridad de la información.	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.	SI		X		X		Definir políticas correspondientes a seguridad de la información, robustez en contraseñas e implementación de Back up de forma automatizada, ante cualquier perdida de información se cuente con un registro de actividad y poder rápidamente restablecer los datos que fueron vulnerados o robados.
5.1.2	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,	SI		X		X		Mediante un plan de auditoria bajo el modelo PHVA, se medirá la efectividad de las políticas establecidas y de esta forma se tomarán las medidas correctivas.

		adecuación y eficacia continuas.							
6.	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.**								
6.1	**Organización interna.**								
6.1.1	Asignación de responsabilidades para la seguridad de la información.	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	SI				X		Definir un plan de capacitaciones al personal correspondiente a la seguridad de la información, responsabilidades y acciones ante cualquier abuso o adulteración de la información
6.1.2	Segregación de tareas.	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	SI				X		Definir las responsabilidades de cada funcionario frente a la adopción de las políticas definidas.
6.1.3	Contacto con las autoridades.	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes	SI			X	X		Definir los canales de comunicación adecuados para el registro de acontecimientos de seguridad.
6.1.4	Contacto con grupos de interés especial.	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones	SI				X		Definir las relaciones adecuadas para recibir informes y noticias respecto a amenazas e incidentes de seguridad.

		profesionales especializadas en seguridad							
6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto	Si		X	X	X	X	Definir la política de seguridad de la información.
6.2	**Dispositivos para movilidad y teletrabajo.**								
6.2.1	Política de dispositivos Móviles	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles	Si		X	X	X	X	Definir una política para el correcto manejo de los dispositivos Móviles, asegurando su segura operación
6.2.2	Teletrabajo.	Control: Se deberían 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	SI		x	x	x	x	Definir las políticas necesarias para el manejo de la información que se descarga de los diferentes sistemas así mismo los controles necesarios sobre las conexiones remotas.
7.	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**								
7.1	**Antes de la contratación.**								

7.1.1	Investigación de antecedentes.	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían 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.	SI		X	X	X		Generar un manual correspondiente a las pautas para la vinculación del personal respecto a políticas de seguridad y confidencialidad de la información.
7.1.2	Términos y condiciones de contratación.	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.	SI		X	X	X		Establecer un acuerdo de confidencialidad dentro de la contratación, definir sobre el reglamento de control interno las consecuencias de su no cumplimiento y de cometer actos de inseguridad.
7.2	**Durante la contratación.**								
7.2.1	Responsabilidades de la dirección.	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y	SI		X	X	X		Definir los procedimientos necesarios para el cumplimiento estricto de las políticas establecidas.

		procedimientos establecidos por la organización.							
7.2.2	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, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo	SI		X	X	X	X	Desarrollar un plan de capacitación para que los empleados sean conscientes y que cumplan con las responsabilidades relacionadas con la seguridad de la información
7.2.3	Proceso disciplinario.	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI			X	X		Definir el proceso formal para establecer las acciones que tomará la IPS en contra del funcionario si comente acciones de violación a la seguridad de la información
7.3	**Terminación o cambio de empleo**								

7.3.1	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 contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	SI			X	X		Definir los controles y responsabilidades respecto al proceso formal de paz y salvo teniendo en cuenta la terminación del contrato, de esta forma realizar un proceso formas de inactivación de los usuarios en todas las plataformas de la IPS
8.	**GESTIÓN DE ACTIVOS.**								
8.1	**Responsabilidad sobre los activos.**								
8.1.1	Inventario de activos.	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	SI		X		X	X	Definir un procedimiento formar la marcación correcta de todos los activos para llevar el control de estos y la correcta identificación.
8.1.2	Propiedad de los activos.	Control: Los activos mantenidos en el inventario deberían tener un propietario	SI		X		X	X	Mantener actualizada la matriz de valoración de los activos

8.1.3	Uso aceptable de los activos.	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI				X	X	Mantener actualizada la plataforma de intranet - Activos Fijos para el correcto registro e identificación de los activos, con todos los parámetros necesarios
8.1.4	Devolución de activos.	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI		X	X	X	X	Definir un proceso de paz y salvo en cuanto se termine su contrato así mismo cuando se trate de préstamos.
8.2	**Clasificación de la información.**								
8.2.1	Clasificación de la información	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada	SI				X	X	Definir el proceso necesario para que la información reciba el nivel de protección y este sea apropiado de acuerdo con el tipo de clasificación determinado por Garper Medica S.A.S

8.2.2	Etiquetado y manipulado de la información.	Control: Se debería 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	SI			X	X		Definir un procedimiento formal para el correcto etiquetado de los activos de información, de acuerdo a la clasificación de la información como clasificada, reservada o pública. Ley 1712 de 2014.
8.2.3	Manipulación de activos.	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptada por la organización.	SI				X		Definir un procedimiento formal que defina la manera en que se debe manejar la información de acuerdo con su clasificación en clasificada, reservada o pública. Ley 1712 de 2017
8.3	**Manejo de los soportes de almacenamiento.**								
8.3.1	Gestión de soportes extraíbles.	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI			x	X		Definir un procedimiento para el análisis de los medios extraíbles de esta forma evitar virus o robo de información así mismo definir la activación o no de este medio.

8.3.2	Disposición de los medios	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	SI			x	X		Implementar el control de desactivación de los puestos para evitar el uso de medios extraíbles
8.3.3	Soportes físicos en tránsito.	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	SI			x	X		Definir un procedimiento formal que establezca la manera correcta en que se deben destruir los medios de almacenamiento de información, dependiendo de su naturaleza. También que se defina los responsables de este procedimiento en cada uno de sus pasos.
9.	**CONTROL DE ACCESOS.**								
9.1	**Requisitos de negocio para el control de accesos.**								
9.1.1	Política de control de accesos.	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	SI			x	X		Definir las pautas generales para asegurar un acceso controlado a la Información de la plataforma informática de Garper Médica S.A.S, así como el uso de medios de computación o móvil.

9.1.2	Control de acceso a las redes y servicios asociados.	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI			x	X		Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información.
9.2	**Gestión de acceso de usuario.**								
9.2.1	Gestión de altas/bajas en el registro de usuarios.	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SI			x	X		Definir el procedimiento formal para la activación de accesos a la red de datos, a través de los mecanismos que tenga establecidos la Entidad.
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	SI			x	X		Definir un procedimiento de Gestión de usuarios para la solicitud de acceso de los usuarios a los sistemas, y de la cancelación del acceso otorgado
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI			X	X		Implementar políticas de respaldo de información así mismo revisar contantemente los privilegios de los usuarios para evitar la edición deliberada de la información, realizando así concientización sobre

									seguridad de la información, y de esta forma lograr un entorno seguro.
9.2.4	Gestión de información confidencial de autenticación de usuarios.	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	SI			X	X		En el procedimiento de Gestión de Usuarios se debe establecer la manera en que se entrega la clave secreta de autenticación de los usuarios para garantizar su confidencialidad.
9.2.5	Revisión de los derechos de acceso de los usuarios.	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	SI			X	X		En el procedimiento de Gestión de usuarios debe incluir la periodicidad con que los administradores de cada Sistema de Información depurarán los usuarios de los sistemas de información
9.2.6	Retirada o adaptación 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 deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	SI			X	X		En el procedimiento de Gestión de usuarios debe incluir lo correspondiente al retiro de privilegio de acceso de los usuarios que ya no labore en la Entidad o ya no tengan un contrato suscrito vigente
9.3	**Responsabilidades del usuario.**								

9.3.1	Uso de información confidencial para la autenticación.	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI			X	X		Definir la política del buen uso de las contraseñas.
9.4	**Control de acceso a sistemas y aplicaciones.**								
9.4.1	Restricción del acceso a la información.	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	SI			X	x		Definir una política respecto al control de acceso a las diferentes aplicaciones.
9.4.2	Procedimientos seguros de inicio de sesión.	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	SI			X	x		Definir una política de control de acceso a las aplicaciones que defina los procedimientos de ingreso seguro a las aplicaciones
9.4.3	Gestión de contraseñas de usuario.	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	SI			X	x		Definir una política de control de acceso a las aplicaciones que incluye los procedimientos en relación con la administración de claves y el restablecimiento de llaves dañadas u olvidadas, para garantizar la confidencialidad de la clave

9.4.4	Uso de herramientas de administración de sistemas.	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	SI			X	x		Definir una política de control de acceso a las aplicaciones y el uso de programas que de tipo privilegiado.
9.4.5	Control de acceso al código fuente de los programas.	Control: Se debería restringir el acceso a los códigos fuente de los programas.	SI			X	X		Definir una política de control de acceso a las aplicaciones y al código fuente de los programas, a través de niveles y privilegios de acceso.
10.	**CIFRADO.**								
10.1	**Controles criptográficos.**								
10.1.1	Política de uso de los controles criptográficos.	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	SI				x		Definir una política sobre el uso de controles criptográficos para la protección de la información.
10.1.2	Gestión de claves.	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	SI				x		Implementar políticas que tengan en cuenta la generación uso, protección, distribución y renovación. Manejo de solicitudes legales teniendo en cuenta la clasificación de la información

11.	**SEGURIDAD FÍSICA Y AMBIENTAL.**								
11.1	**Áreas seguras.**								
11.1.1	Perímetro de seguridad física.	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.	SI				x		Definir una política de seguridad en el acceso a las áreas restringidas como Centros de Datos y de Telecomunicaciones
11.1.2	Controles físicos de entrada.	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	SI				x		Definir una política de seguridad en el acceso a las áreas restringidas tales como los Centros de Datos y Telecomunicaciones, áreas de Gestión Documental y archivo.
11.1.3	Seguridad de oficinas, despachos y recursos.	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	SI				x		Definir una política de seguridad en el acceso a las áreas oficinas en general de la Entidad.
11.1.4	Protección contra las amenazas externas y ambientales.	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI				x		Controlar el exceso de temperatura producto de la humedad. Reubicar el archivo centra en otro sitio

11.1.5	El trabajo en áreas seguras.	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI				X		Definir una política de seguridad en el acceso a las áreas seguras de la Entidad
11.1.6	Áreas de acceso público, carga y descarga.	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI				X		Definir una política de seguridad en el acceso a las áreas seguras de la Entidad
11.2	**Seguridad de los equipos.**								
11.2.1	Emplazamiento y protección de equipos.	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	SI			X	X		Definir un procedimiento formal y guía sobre las ubicaciones autorizadas para los equipos para que queden protegidos de accesos no autorizados
11.2.2	Instalaciones de suministro.	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los	SI			X	X		Definir un procedimiento formal para la revisión del estado de todos los servicios de suministro que están relacionados con los equipos para evaluar si la capacidad

		servicios de suministro.							está acorde a la cantidad de equipos.
11.2.3	Seguridad del cableado.	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	SI				X		Definir un procedimiento formal para el suministro de cableado estructurado, que incluya normas de seguridad y controles de acceso a cajas de inspección.
11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI			X	X		Establecer plan de mantenimiento y actualización de software.
11.2.5	Salida de activos fuera de las dependencias de la empresa.	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	SI				X		Establecer procedimiento formal para el retiro de activos de la Entidad.
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Control: Se deberían 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	SI				X		Los equipos que se autorizan para ser trasladados o mantenerse fuera de la Entidad se deben proteger con pólizas de seguros y controles de seguridad informática.

		de dichas instalaciones.							
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	SI				X		Definir un procedimiento formal que establezca la manera correcta en que se deben destruir los medios de almacenamiento de información, dependiendo de su naturaleza. También que se defina los responsables de este procedimiento en cada uno de sus pasos.
11.2.8	Equipo informático de usuario desatendido.	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	SI			X	X		Establecer formalmente los procedimientos mediante el cual los sistemas desatendidos quedan protegidos a través de políticas del directorio activo
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	Control: Se debería 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.	SI			X	X		Definir una política de escritorio limpio y pantalla limpia que incluya escritorios físicos, medios removibles y equipos
12.	**SEGURIDAD EN LA OPERATIVA.**								

12.1	**Responsabilidades y procedimientos de operación.**								
12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.			X	X	X		Crear manuales de procedimientos e instructivos de los sistemas de la Entidad.
12.1.2	Gestión de cambios.	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI		X	X	X		Definir un proceso formal para tramitar y asegurar los cambios en los sistemas de información que administra la Dirección de Tecnología, con el fin de minimizar la probabilidad de interrupciones y cambios no autorizados.
12.1.3	Gestión de capacidades.	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	SI		X	X	X		Definir planes de Gestión de la capacidad con proyección mínimo a cinco años, para determinar los recursos que se necesitan a nivel de tecnología para que estén acorde a la demanda de la Entidad

12.1.4	Separación de entornos de desarrollo, prueba y producción.	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	SI		X	X	X		Definir ambientes de desarrollos, pruebas y producción para cada sistema de información de la Entidad, para la realización de pruebas de seguridad y operación antes de lanzar a producción
12.2	**Protección contra código malicioso.**								
12.2.1	Controles contra el código malicioso.	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI			X	X		Establecer dentro de los planes de formación lo referente a la toma de conciencia en temas de Seguridad de la Información
12.3	**Copias de seguridad.**								
12.3.1	Copias de seguridad de la información.	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	SI		X	X	X		Definir un cronograma para la revisión de la información que esta se encuentre debidamente clasificada, trazabilidad de las copias y log de actividades sobre posible adulteración fuga de información

12.4	Registro de actividad y supervisión.								
12.4.1	Registro y gestión de eventos de actividad.	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI		X	X	X		Definir política de retención de logs en el tiempo, en cada uno de los sistemas a cargo de la Dirección de Tecnología.
12.4.2	Protección de los registros de información.	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	SI		X		X		Definir política de retención de logs que indique la periodicidad con la cual se hará copia de seguridad de estos registros.
12.4.3	Registros de actividad del administrador y operador del sistema.	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	SI		X		X		Definir política de retención de logs que incluya los registros de actividades de los administradores de los sistemas.
12.4.4	Sincronización de relojes.	Control: Los relojes de todos los sistemas de procesamiento de informaciones pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única	SI				X		Mantener la sincronización de relojes a través del servicio NTP del Directorio Activo que se encuentra sincronizado con la hora legal colombiana. Incluir esta directriz dentro de la política de retención de logs

		fuente de referencia de tiempo							
12.5	**Control del software en explotación.**								
12.5.1	Instalación del software en sistemas en producción.	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI		X	X	X		Implementar los controles de administrador para no permitir la instalación y manejo de sistemas no autorizados.
12.6	**Gestión de la vulnerabilidad técnica.**								
12.6.1	Gestión de las vulnerabilidades técnicas.	Control: Se debería 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 para tratar el riesgo asociado.	SI			X	X		Definir un procedimiento formal para la detección de vulnerabilidades técnicas de los sistemas de información para tomar acciones de manera preventiva.
12.6.2	Restricciones en la instalación de software.	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	SI			X	X		Implementar los controles de administrador para no permitir la instalación y manejo de sistemas no autorizados.
12.7	**Consideraciones de las auditorías de los sistemas de información.**								

12.7.1	Controles de auditoría de los sistemas de información.	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI		X	X	X		Implementar controles de log para verificar las actividades que se puedan presentan ante vulnerabilidades en los diferentes sistemas
13.	**SEGURIDAD EN LAS TELECOMUNICACIONES.**								
13.1	**Gestión de la seguridad en las redes.**								
13.1.1	Controles de red.	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI				X		Definir los procedimientos formales para el monitoreo y control de la información de los sistemas a cargo de la Jefe de Tecnología.
13.1.2	Mecanismos de seguridad asociados a servicios en red.	Control: Se deberían 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 servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI		X		X		Definir los Acuerdos de Nivel de Servicio para todos los servicios que presta.

13.1.3	Segregación de redes.	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	SI		X		X		Definir procedimiento formal para la segmentación de la red a través de VLANs
13.2	**Intercambio de información con partes externas.**								
13.2.1	Políticas y procedimientos de intercambio de información.	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	SI		X	X	X	X	Diseñar políticas, procedimientos y controles de transferencia de información para proteger la información que se envía a través de los diferentes medios de comunicación.
13.2.2	Acuerdos de intercambio.	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	SI		X	X	X	X	Definir acuerdos entre la Entidad y partes externas para la transferencia segura de la información.
13.2.3	Mensajería electrónica.	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	SI		X		X	X	Definir dentro de la política de tratamiento de la información los lineamientos para el uso de mensajería electrónica autorizada por la Dirección de Tecnología, que es el correo electrónico corporativo.

13.2.4	Acuerdos de confidencialidad y secreto.	Control: Se deberían 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	SI		X	X	X	X	Definir dentro de la política de tratamiento de la información los Acuerdos de confidencialidad de la información.
14.	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**								
14.1	**Requisitos de seguridad de los sistemas de información.**								
14.1.1	Análisis y especificación de los requisitos de seguridad.	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI		X	X	X	X	Establecer los requisitos de seguridad que deben cumplir todos los sistemas de información nuevos de la Entidad y cuando se les realicen mejoras en cada una de las fases del desarrollo, y definir un procedimiento para su aplicación.
14.1.2	Seguridad de las comunicaciones en servicios accesibles por	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades	SI		X	X	X	X	Definir los procedimientos formales para la información que es transmitida por redes públicas

	redes públicas.	fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.							
14.1.3	Protección de las transacciones por redes telemáticas.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería 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.	SI		X	X	X	X	Definir los procedimientos formales para la información que es transmitida por redes públicas.
14.2	**Seguridad en los procesos de desarrollo y soporte.**								
14.2.1	Política de desarrollo seguro de software.	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	SI		X	X	X	X	Establecer una política de desarrollo seguro que garantice que las aplicaciones cumplan con los requerimientos de seguridad en cada una de las fases de desarrollo.

14.2.2	Procedimientos de control de cambios en los sistemas.	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	SI		X	X	X	X	Definir un proceso formal para tramitar y asegurar los cambios en los sistemas de información que administra la Dirección de Tecnología, con el fin de minimizar la probabilidad de interrupciones y cambios no autorizados
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 deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	SI		X	X	X	X	Definir procedimientos formales de pruebas a los sistemas de información luego de que se realicen cambios a las plataformas que los soportan (sistemas operativos, plataforma SAN, red, etc)
14.2.4	Restricciones a los cambios en los paquetes de software.	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente	SI		X	X	X	X	Dentro de la política de desarrollo seguro se debe incluir los lineamientos para que a los paquetes de software no se les realice cambios a menos que sea estrictamente necesario y realizarlos bajo controles de seguridad.

14.2.5	Principios de construcción de sistemas seguros	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	SI		X	X	X	X	Establecer una política de desarrollo seguro que garantice que las aplicaciones cumplan con los requerimientos de seguridad en cada una de las fases de desarrollo.
14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	SI		X	X	X	X	Establecer una política de desarrollo seguro que garantice que las aplicaciones tengan ambientes de desarrollos seguros.
14.2.7	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI		X	X	X	X	Establecer una política de desarrollo seguro que garantice que los desarrollos contratados con terceros cumplan con lo requerido
14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.	SI		X	X	X	X	Establecer una política de desarrollo seguro que garantice que se realicen las pruebas necesarias de

									funcionalidad antes de la puesta en marcha del sistema.
14.2.9	Pruebas de aceptación.	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	SI		X	X	X	X	Establecer una política de desarrollo seguro que garantice que se realicen las pruebas necesarias de funcionalidad antes de la puesta en marcha del sistema.
14.3	**Datos de prueba.**								
14.3.1	Protección de los datos utilizados en pruebas.	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.	SI			X	X	X	Establecer una política de desarrollo seguro que garantice que los datos de prueba se seleccionan, se protegen y se controlan cuidadosamente.
15.	**RELACIONES CON SUMINISTRADORES.**								
15.1	**Seguridad de la información en las relaciones con suministradores.**								
15.1.1	Política de seguridad de la información para suministradores.	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 deberían acordar con estos y se	SI		X	X	X		La política de Seguridad de la Información debe incluir acuerdos de confidencialidad con proveedores.

		deberían documentar.							
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	Control: Se deberían 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.	SI		X	X	X		Definir los acuerdos de confidencialidad y reserva en el manejo de la información con proveedores.
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	SI		X	X	X		Definir un listado maestro de los requisitos a exigir a cada proveedor dependiendo del tipo de servicio a suministrar, para mitigar riesgos de seguridad de la información.
15.2	**Gestión de la prestación del servicio por suministradores.**								
15.2.1	Supervisión y revisión de los servicios	Las organizaciones deberían hacer seguimiento, revisar y	SI				X	X	Dentro del proceso de evaluación de proveedores se debe incluir lo correspondiente

	prestados por terceros.	auditar con regularidad la prestación de servicios de los proveedores.							a la seguridad de la información.
15.2.2	Gestión de cambios en los servicios prestados por terceros.	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la informaciones existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos	SI				X	X	Establecer una política de cambios a los servicios del proveedor.
16.	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**								
16.1	**Gestión de incidentes de seguridad de la información y mejoras.**								
16.1.1	Responsabilidades y procedimientos.	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz	SI				X		Definir un cronograma para la revisión de la información que esta se encuentre debidamente clasificada, trazabilidad de las copias y log de actividades sobre posible adulteración o fuga de información.

		y ordenada a los incidentes de seguridad de la información.							
16.1.2	Notificación de los eventos de seguridad de la información.	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	SI				X		Definir un procedimiento formal para gestionar adecuadamente los incidentes de seguridad de la información, que establezca los canales apropiados para el reporte de dichos eventos.
16.1.3	Notificación de puntos débiles de la seguridad.	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	SI				X		Establecer planes de concientización al personal sobre la seguridad de la información y la importancia de reportar cualquier debilidad que observen en los sistemas de información.
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.	SI						Definir política de control acceso al archivo central de la dependencia a través de mecanismos eficientes que permita el ingreso solo a personal autorizado. Según su cargo

16.1.5	Respuesta a los incidentes de seguridad.	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI				X		Establecer el procedimiento formal para la respuesta ante un incidente de seguridad, recolección de evidencias, identificar fuentes de ataque, aplicar estrategias de recuperación y erradicación de la falla de seguridad.
16.1.6	Aprendizaje de los incidentes de seguridad de la información.	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.	SI				X		Establecer una metodología para el manejo de lecciones aprendidas con respecto a incidentes de seguridad de la información, que incluya el mantener un listado de incidentes, bases de conocimiento, actualizar matriz de riesgos y capacitaciones a los usuarios.
16.1.7	Recolección de evidencia	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI				X		Establecer el procedimiento formal para la respuesta ante un incidente de seguridad, recolección de evidencias, identificar fuentes de ataque, aplicar estrategias de recuperación y erradicación de la falla de seguridad.
17.	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**								
17.1	**Continuidad de la seguridad de la información.**								

17.1.1	Planificación de la continuidad de la seguridad de la información.	Control: La organización debería 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.	SI		X	X	X		Establecer un plan de continuidad que garantice la operatividad de la organización en caso de que los procesos críticos fallen
17.1.2	Implantación de la continuidad de la seguridad de la información.	Control: La organización debería 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.	SI		X	X	X		Implementar un plan de continuidad que garantice la operatividad de la organización en caso de que los procesos críticos fallen
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e	SI				X	X	Evaluar el plan de continuidad que garantice la operatividad de la organización en caso de que los procesos críticos fallen

	la información.	implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas							
17.2	**Redundancias.**								
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI				X	X	Mantener los controles actuales implementados y extenderlos a los componentes de red.
18.	**CUMPLIMIENTO.**								
18.1	**Cumplimiento de los requisitos legales y contractuales.**								
18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	SI		X	X	X		Definir el normo grama que incluya lo relacionado a la Seguridad de la Información.

18.1.2	Derechos de propiedad intelectual (DPI).	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	SI		X	X	X		Establecer procedimiento formal para asegurar el cumplimiento de los requisitos legales relacionados con derechos de propiedad intelectual.
18.1.3	Protección de los registros de la organización.	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	SI		X		X		Establecer procedimiento formal para proteger los registros de la IPS de acuerdo a los requisitos legales existentes aplicables a la Cámara de Comercio de Cúcuta.
18.1.4	Protección de datos y privacidad de la información personal.	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se	SI		X		X		Mantener e implementar los manuales de políticas y procedimientos establecidos para la protección de datos personales.

		exige en la legislación y la reglamentación pertinente.							
18.1.5	Regulación de los controles criptográficos.	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.			X		X		Implementar controles criptográficos para garantizar la confidencialidad e integridad de la información.
18.2	**Revisiones de la seguridad de la información.**								
18.2.1	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 (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	SI		X		X		Plan anual de auditorías de seguridad de la información
18.2.2	Cumplimiento de las políticas y	Control: Los directores deberían revisar con regularidad el cumplimiento del	SI		X	X	X		Por ser una entidad que maneja recursos públicos, es recomendable acatar las indicaciones del Gobierno

	normas de seguridad.	procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridades apropiadas, y cualquier otro requisito de seguridad.							nacional sobre la inclusión de la seguridad de la información en todos sus procesos.
18.2.3	Comprobación del cumplimiento.	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI		X	X	X		Plan anual de revisión de controles técnicos en los sistemas de información de la Entidad para el cumplimiento de las políticas y normas de seguridad de la información.

Fuente: Elaboración propia.

6.3 ELABORAR POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN QUE PERMITA GESTIONAR LOS RIESGOS Y AMENAZAS, CON EL FIN DE PREVENIR ALGÚN EVENTO CIBERNÉTICO Y DE ESTA FORMA SE PUEDA TENER TRANQUILIDAD EN EL MANEJO Y SEGURIDAD DE LOS SISTEMAS CRÍTICOS DE INFORMACIÓN DE LA IPS GARPER MÉDICA SAS.

Garper Médica S.A.S diseña un modelo de gestión de seguridad de la información como el instrumento que permite identificar y minimizar los riesgos a los cuales se exponen la información, apoya la disminución de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.[42]

Las políticas y lineamiento expuestos en el presente manual serán de aplicabilidad y cumplimiento por todos los funcionarios, contratistas y en general a toda persona que tenga algún tipo de trato con Garper Médica S.A.S y cuenten con acceso a los sistemas de información dentro o fuera de las instalaciones de la IPS.

Política de control de acceso:

Objetivo: Definir las pautas generales para asegurar un acceso controlado, a la Información de la plataforma informática de Garper Médica S.A.S, así como el uso de medios de computación o móvil.

- El área de TIC será el responsable de crear el usuario y la contraseña del primer ingreso a los aplicativos institucionales del personal autorizado por el área de talento humano.
- Las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se le dé a las claves asignadas.

[42] DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *2021*. Libro II - Catálogo de Elementos. 20 p.

- El área de talento Humano será el responsable de informar al área de TIC la terminación de contrato del funcionario con el fin de que:

    1- El área de TIC realice el Back up de la información que se encuentre almacenada en el equipo del funcionario y que corresponda a activos de información.
    2- El área de TIC realice la inactivación del usuario en las diferentes plataformas institucionales.
    3- El área de TIC verifique la entrega adecuada de la información y activos físicos.
    4- El área de TIC sea partícipe de firmar los paz y salvos, debe dejar las observaciones necesarias dentro del formato establecido por los líderes de los procesos.

- Los usuarios solo tendrán acceso a los datos y recursos autorizados por Garper Médica S.A.S y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
- Los dispositivos electrónicos de propiedad Garper Médica S.A.S (computadoras, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad y de esta forma se asignará un código para su uso.
- Todas las copias de información críticas deben ser almacenadas en un área apropiada con los revisiones y controles ambientales aplicables y de acceso físico.
- Garper Médica S.A.S facilitará al usuario los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de Garper Médica S.A.S, los funcionarios o usuarios solo podrán realizar backup de información pública. Para copiar cualquier tipo de información clasificada como confidencial o restringida debe pedir autorización a su jefe inmediato, de acuerdo con las normas sobre clasificación de la información.

- Habitualmente, el personal TIC realizará una auditoria a los computadores para revisión de los programas y documentos utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerado como violación a las Políticas de Seguridad de la Información de Garper Médica S.A.S estos serán borrados o desinstalados.
- Queda completamente restringido el uso de medios extraíbles como USB, Discos Duros, en las estaciones de ciertos equipos de trabajo si así se dispone por el Jefe de Tecnología y la gerencia ya que son a través de estos medios donde se presentan más vulnerabilidad, ataques de virus informáticos, pérdida de información, entre otros daños que logren llegar a presentar los equipos de cómputo determinados.

Política de Clasificación de la Información.

Objetivo: Gestionar las acciones necesarias para que la información reciba el nivel de protección sea apropiado de acuerdo con el tipo de clasificación establecido por Garper Médica S.A.S.

- Aplicar el uso apropiado de la intranet delimitando a que área se debe permitir la lectura, visualización y descarga, así mismo definir los niveles de clasificación de la información (Pública, uso interno, confidencial o restringida).
- Toda la comunicación o representación de datos digitales escritos en cualquier medio, ya sea magnético, papel u otro que genere Garper Médica S.A.S (Ej: historias clínicas, exámenes de laboratorio, patologías, imágenes diagnósticas, entre otras), se considera como información.
- El propietario de la información o a quien delegue, será el responsable de clasificar la información teniendo en cuenta los riesgos, amenazas e impactos en caso de materialización de éstos.

Política de Seguridad para los usuarios de activos de información.

Objetivo: Verificar que los funcionarios, contratistas y demás colaboradores de Garper Médica S.A.S, comprendan sus responsabilidades y funciones, con el fin de reducir el riesgo de hurto, fraude o uso improcedente de la información y de las instalaciones.

- Los recursos tecnológicos y de software asignados a los funcionarios de Garper Médica S.A.S son responsabilidad de cada uno.
- Los usuarios son los responsables de la información que administren en sus equipos personales; deberán abstenerse de almacenar en ellos información no institucional.
- Los usuarios solo tendrán acceso a los datos y recursos autorizados por Garper Médica S.A.S y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
- Es responsabilidad de cada usuario resguardar la información que esté incluida en documentos, formatos, listados, etc.; los cuales son el efecto de los métodos informáticos.
- Los dispositivos electrónicos de propiedad Garper Médica S.A.S (computadoras, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.
- Cualquier acontecimiento o posible incidente que afecte la seguridad de la información, deberá ser reportado inmediatamente al área de TIC de Garper Médica S.A.S.
- Los jefes de las diferentes áreas de Garper Médica S.A.S en conjunto con el Comité de TIC propiciarán actividades para concientizar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial.
- Se debe hacer un uso responsable, controlado de las redes internas, asumiendo el compromiso que esta es una herramienta importante para

Garper Médica S.A.S y que su buen uso va en pro del buen trabajo y estabilidad de las estructuras tecnológicas que se brindan a cada uno de los colaboradores.

Políticas específicas para funcionarios y personal del Área de TIC.

Objetivo: Garantizar que los funcionarios área de TIC aseguren una adecuada protección de la información de la cual son responsables de su administración.

- Los usuarios y claves correspondientes a accesos administradores del personal del área de TIC son de uso personal e intransferible, el personal del área de TIC no debe dar a conocer sus claves de usuario a personal ajeno a su área.
- El personal del área de TIC debe emplear obligatoriamente claves o contraseñas con un alto nivel de complejidad.
- Para el cambio o retiro de equipos de cómputo por daño u obsolescencia, se deben seguir políticas de saneamiento; es decir, llevar a cabo mejores prácticas para la eliminación de la información de acuerdo con el software disponible en la entidad. (Ej. formateo o borrado seguro de información).
- Los funcionarios encargados de realizar la instalación o distribución de software sólo instalarán productos con licencia y software autorizado.
- El personal del área de TIC no otorgará privilegios especiales a usuarios sobre las estaciones de trabajo sin la autorización correspondiente del Jefe de TIC de Garper Médica S.A.S.
- El personal del área de TIC está obligado a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a resguardarla para evitar su publicidad.
- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar por quien designe al Jefe de TIC de Información de

Garper Médica S.A.S, de tal forma que asegure su protección y disposición en un futuro.

- El software licenciado y registrado como software adquirido, será únicamente instalado en equipos y servidores de propiedad de Garper Médica S.A.S excepto aquellas empresas que mantengan un convenio contractual con Garper Médica S.A.S para la ejecución de las actividades requiera el acceso al software.
- Garper Médica S.A.S, instalará copia de los programas que han sido obtenidos legalmente en los equipos asignados y en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización por parte del Jefe de TIC de Garper Médica S.A.S puede implicar amenazas legales y de seguridad de la información para la entidad, por lo cual esta práctica no está autorizada. El área de Tic, deberá llevar el control de las cantidades de licencias disponibles.
- Cumplir siempre con el registro en la bitácora GTI-FT-05 Formato bitácora de ingreso a centros de Cableado y data center, de las personas que ingresen y que hayan sido autorizadas previamente por el Jefe de TIC de Garper Médica S.A.S o por quien éste delegue.
- Por defecto deben ser bloqueados todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la entidad a través del Comité de TIC o el Jefe de TIC de Información de Garper Médica S.A.S.
- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
- Los medios y equipos donde se almacena, procesan o comunica la información, deben conservar las medidas de protección físicas y lógicas que permitan su monitoreo y correcto estado de funcionamiento; para ello se debe ejecutar los mantenimientos preventivos y correctivos que se requieran.

Políticas específicas para la protección de la Página web.

Objetivo: Salvaguardar la integridad de la página Web institucional.

- Los responsables de áreas que soliciten publicar información institucional en la página Web deben preparar y depurar la información de su área o dependencia y reportar al área de TIC, para su estudio quien será responsable de verificar ortografía, redacción e imagen corporativa de la información a publicar.
- Se socializará sobre el comité de Sistemas todos aquellos ajustes y mejoras que se realicen en el sitio web de Garper Médica S.A.S intranet, E-learning siempre y cuando estas mejoras sean significativas y vayan en pro de mejorar la producción en cada uno de estos sitios web, se bebe hacer formal bajo el formato GTI-FT-18 Formato de entrega para publicación en Herramientas tecnológicas, se deberá tener especial cuidado en la información que es publicada en la web y debe ser la autorizada por las áreas y con nivel de clasificación pública.
- El área de TIC es el responsable de realizar las copias de seguridad de la página web y mantendrá el histórico respectivo.

Política de respaldo y restauración de información

Objetivo: Asegurar que la información crítica para la entidad se encuentre disponible en situaciones de contingencia y poder asegurar la continuidad del negocio.

- La información de cada sistema debe ser respalda regularmente en medios de almacenamiento como discos externos, servidores de almacenamiento o el medio que disponga Garper Médica S.A.S.
- El área de Tic son los responsables de la ejecución y custodia de las copias de seguridad según el procedimiento determinado.

- Todas las copias de información crítica deben ser almacenadas en un área adecuada con los controles ambientales aplicables y con control de acceso físico.
- Las copias de respaldo se almacenarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal, entre otros.
- El plan de contingencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, actualizado y periódicamente probado y revisado.
- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; para lo cual Garper Médica S.A.S dispone de un espacio con límite de gigas para cada área o servicio para el almacenamiento de la información en los servidores.
- Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera del edificio en donde se encuentre el Data Center de Garper Médica S.A.S. Las restauraciones de copias de respaldo en ambientes de producción deben estar debidamente aprobada por el propietario de la información. Periódicamente desde el área de TIC se verificará la correcta ejecución de los procesos de backup ejecutados.
- Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada. Este proceso deberá ser controlado y aprobado por las áreas de Revisoría Fiscal y/o Control Interno.
- Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización de los recursos de almacenamiento que entrega Garper Médica S.A.S a los usuarios de esta forma se podrá garantizar desde TIC la copia de seguridad.

Política de gestión de activos de información

Objetivo Establecer la forma en que se logra mantener la protección adecuada de los activos de información.

- Garper Médica S.A.S mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el área de TIC.
- Garper Médica S.A.S, en cabeza de sus líderes de áreas es el propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones, hardware o infraestructura de tecnología de la información y comunicaciones (TIC)

Política de uso de los activos.

Objetivo: Resguardar de forma apropiada los activos de información mediante la asignación de estos a los usuarios finales que deban disponer de acuerdo con sus roles y funciones.

- Los activos de información pertenecen a Garper Médica S.A.S y el uso de estos deben emplearse exclusivamente con propósitos laborales. Los activos de información de Hardware suministrados por el contratista o de terceras partes, serán administrados y estarán bajo la vigilancia del personal de TIC de Garper Médica S.A.S y deberán cumplir con políticas de seguridad de la información, tal como control de acceso a redes y aplicativos, entre otros.
- Los usuarios deberán utilizar únicamente software, programas y equipos autorizados por el área de TIC de Garper Médica S.A.S.

- Garper Médica S.A.S facilitará al usuario los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de Garper Médica S.A.S.
- Garper Médica S.A.S no se hará responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.
- Todos los requerimientos de aplicativos, TIC y equipos informáticos que requieran un nivel de aprobación, deben ser solicitados, analizados y aprobados por el Jefe de TIC de Garper Médica S.A.S.
- Queda totalmente restringido el uso de medios extraíbles como USB, Discos Duros, en las estaciones de ciertos equipos de trabajo si así se dispone por el Jefe de Tecnología y la gerencia
- Estarán bajo custodia de TIC de Información de Garper Médica S.A.S, los medios magnéticos/electrónicos (CD, DVD u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso; adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet.
- Las contraseñas de administración de los equipos informáticos, TIC de información o aplicativos estarán bajo la responsabilidad del funcionario que tenga la administración de los servicios TIC.
- En caso de ser necesario y previa autorización del Comité de TIC o de la oficina asesora de TIC de información de Garper Médica S.A.S, los funcionarios de Garper Médica S.A.S podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban a través de internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.
- Los usuarios no podrán efectuar ninguna de las siguientes actividades:
    - Instalar software en cualquier equipo instalado en áreas físicas de Garper Médica S.A.S.

- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de Garper Médica S.A.S.
- Modificar, revisar, transformar o adaptar cualquier software propiedad de Garper Médica S.A.S.
- Descompilar o realizar ingeniería inversa en cualquier software de propiedad de Garper Médica S.A.S.
- Copiar o distribuir cualquier software de propiedad de Garper Médica S.A.S. El usuario deberá informar al jefe inmediato de cualquier violación de las políticas de seguridad o uso indebido del cual tenga conocimiento.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.
- Ningún usuario deberá acceder a la red o a los servicios de TIC, utilizando una cuenta de usuario o clave de otro usuario.
- Todos los archivos provenientes de equipos externos de Garper Médica S.A.S deben ser revisados para detención de virus antes de ser utilizados en la red de Garper Médica S.A.S.

Política de uso de Internet.

Objetivo Instaurar lineamientos que garanticen la navegación segura y el uso apropiado de la red por parte de los usuarios finales, evitando pérdida, alteraciones no autorizadas o uso inadecuado de la información en las aplicaciones web.

- La navegación en Internet debe realizarse de forma razonable y con propósitos laborares.
- No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de Garper Médica S.A.S o que representen peligro para la entidad como: pornografía, terrorismo, segregación racial, música, redes sociales u otras fuentes.

- El acceso a sitios WEB con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del Comité de TIC ó Jefe de TIC De Garper Médica S.A.S.
- La descarga de archivos de Internet debe ser con propósitos labores y de forma razonable para no afectar el servicio de Internet.
- Los documentos o software que se descarguen de Internet deben tener las debidas licencias o permisos de uso, respetando siempre la propiedad intelectual del mismo

Política de uso de discos de red o carpetas virtuales.

Objetivo Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

- Para que los usuarios tengan acceso a la información en los discos de red, el jefe inmediato deberá enviar una solicitud a la mesa de ayuda del área de TIC de Garper Médica S.A.S, autorizando el acceso y permisos correspondientes al rol y funciones a desempeñar. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
- Garper Médica S.A.S suministrará una cuota de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información que crea importante y sobre ella se garantizará la disponibilidad en caso de daños en el equipo asignado.
- La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.
- La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.

- Está prohibido almacenar en las estaciones de trabajo (computadores de escritorio o portátiles, tablets, celulares inteligentes, etc.), o en los discos de red de propiedad de la entidad, archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso.
- Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización del jefe inmediato.
- Se prohíbe el uso de información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

Política de uso de impresoras y del servicio de Impresión.

Objetivo Asegurar la operación correcta y segura de las impresoras y del servicio de Impresión en las diferentes áreas de Garper Médica S.A.S.

- Los documentos que se impriman en las impresoras de Garper Médica S.A.S deben ser de carácter institucional.
- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras (y/o cualquier equipo de cómputo). En caso de presentarse alguna falla, esta se debe reportar al área de TIC por medio de su mesa de ayuda.
- Agregar o alinear la presente política con la de política de cero papeles, si existe.

Política de uso de puntos de red de datos.

Objetivo Asegurar la operación correcta y segura de los puntos de red instalados en la entidad.

- Los usuarios deberán emplear los puntos de red para la conexión de equipos informáticos estándar. Los equipos de uso personal, que no sean de propiedad de Garper Médica S.A.S, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el área de TIC e infraestructura. Se deberá identificar el equipo por medio de la MAC.
- La instalación, activación y gestión de los puntos de red es responsabilidad del área de infraestructura y redes.

Política de seguridad del centro de datos (DataCenter)

Objetivo Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte

- No se permite el ingreso al centro de datos, al personal que no esté formalmente autorizado. Se debe llevar un control de ingreso y salida del personal que visite el centro de datos.
- El área de TIC e infraestructura debe garantizar que el control de acceso al centro de datos de Garper Médica S.A.S cuente con dispositivos de control necesarios (electrónicos de autenticación o TIC de control biométrico) para asegurar accesos autorizados.
- El área de TIC e infraestructura deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.
- La limpieza y aseo del centro de datos estará a cargo del área de TIC e infraestructura. En caso contrario, deberá ser supervisado por personal de esta área si el aseo lo llegase a realizar personal ajeno a ésta.

- En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio. El centro de datos debe estar provisto de:

  - Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación.
  - Pisos elaborados con materiales no combustibles.
  - Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración. - Unidades de potencia ininterrumpida UPS, que proporcione respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
  - Alarma de detención de humo y TIC automáticos de extinción de fuego, conectada a un sistema central.
  - Los cables de potencia deben estar separados de los de comunicaciones (datos), siguiendo las normas técnicas.
  - La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizadas por el comité de seguridad de la información o jefe de TIC de Información de Garper Médica S.A.S.
  - Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por el área de TIC.
  - Las puertas de acceso al centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario de la actividad se ubicará dentro del centro de datos.
  - Cuando se requiera realizar actividad sobre algún armario (rack), este deberá siempre estar y/o quedar ordenado, cerrado y con llave cuando se finalice la actividad. - Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

- Los equipos del centro de datos que se requieran deben estar monitoreados para poder detectar las fallas que se puedan presentar.

Políticas de seguridad de los equipos de cómputo.

Objetivo Asegurar la protección de la información procesada en los equipos de cómputo.

- Dar cumplimiento a las siguientes normas de seguridad:
- Encender y apagar correctamente el equipo de cómputo.
- No colocar encima de los equipos de cómputo ningún objeto que pueda caer y dañarlos.
- Toda CPU que se encuentre en servicio no debe estar en el piso sin ningún tipo de soporte.
- No consumir alimentos ni bebidas cerca al equipo de cómputo.
- Limpiar regularmente el equipo de cómputo asignado.
- Conectar a la red de energía regulada únicamente equipos de cómputo y tecnológicos de propiedad de Garper Médica S.A.S. Equipos ajenos a Garper Médica S.A.S y autorizados para su uso dentro de la institución se deben conectar a la red no regulada.
- Seguridad del cableado: los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- Deben existir planos que describan las conexiones del cableado
- El acceso a los centros de cableado, deben estar protegidos.

Mantenimiento de los equipos de cómputo:

- Las actividades de mantenimiento tanto preventivo como correctivo debe registrarse para cada equipo de cómputo.

- Las actividades de mantenimiento de los servidores, comunicación, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.

- Los equipos que requieran salir de las instalaciones de Garper Médica S.A.S para reparaciones o mantenimientos deben estar debidamente autorizados y se deben garantizar que en dichos elementos no se encuentre información confidencial.

- Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información confidencial contenida en ella. Realizar copia de información.
- El retiro e ingreso de todo activo de información de propiedad de los usuarios de Garper Médica S.A.S utilizados para fines personales, se realizará mediante los procedimientos establecidos por la entidad. Garper Médica S.A.S no se hace responsable de los daños ocasionados a los bienes del usuario al haberse conectado a la red eléctrica de Garper Médica S.A.S. El retiro e ingreso de todo activo de información de los visitantes (consultores, pasantes, visitantes, pacientes y sus familias), será registrado y controlado en las porterías. El personal de vigilancia registrará las características de la identificación del activo de información en el formato destinado para tal fin.
- El traslado entre dependencias de Garper Médica S.A.S de todo activo de información (equipos de cómputo), está a cargo del área Administrativa (Activos Fijos) para el control de Inventarios.

Política de escritorio, pantalla limpia y de equipos desatendidos.

Objetivo: Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de información durante y fuera del horario de trabajo normal de los usuarios.

- El personal de Garper Médica S.A.S o contratistas debe conservar su escritorio libre de información confidencial, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- El personal de Garper Médica S.A.S debe bloquear la pantalla de su computador con el protector de pantalla en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba ausentarse del puesto de trabajo.
- Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
- Almacenar bajo llave y cuando corresponda, los documentos en físico y/o medios informáticos en gabinetes u otro tipo de mobiliario seguro, cuando no estén siendo utilizados, especialmente fuera del horario de trabajo.
- No se deben utilizar fotocopiadoras, escáner, equipos de fax, cámaras digitales y en general equipos tecnológicos que no se encuentren configurados a la red de Garper Médica S.A.S.
- Se establece un papel tapiz, así como un protector de pantalla corporativos, los cuales no deben ser cambiados ni modificados salvo sea autorizado por el Jefe TIC de Garper Médica para su debida implementación.

Política de uso de correo electrónico.

Objetivo: Establecer una serie de directrices para el uso responsable del correo electrónico institucional.

- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de correo institucional; toda información o contenido que sea transmitido por las cuentas de correo de este sitio, son responsabilidad únicamente del dueño de la cuenta.
- La cuenta de correo es personal e intransferible, siendo su responsabilidad salvaguardar la clave de acceso, cambiándola en forma periódica, ni prestar la clave en ninguna circunstancia, pues su uso recae bajo su responsabilidad. Así mismo, el usuario se compromete a notificar personalmente al administrador de correo electrónico de manera inmediata la pérdida de su contraseña o acceso no autorizado por parte de terceros a su cuenta.
- Se requiere que la primera vez que el usuario ingrese a su cuenta de correo cambie su clave. Por motivos de seguridad, es recomendable cambiar la clave, como mínimo, cada tres meses. El correo electrónico es una herramienta de trabajo para uso exclusivamente de la Institución, no es una herramienta de difusión masiva e indiscriminada de información.
- Los miembros de Garper Médica S.A.S deben ser cuidadosos cuando decidan abrir los archivos adjuntos en mensajes de remitentes desconocidos o sospechosos, para evitar descarga de algún virus informático o programa sospechoso.
- Será responsabilidad del administrador de las cuentas de office 365 tener copias de respaldo (Backups) de los mensajes de las carpetas de correo electrónico.
- Es responsabilidad del propietario de la cuenta mantener el buzón por debajo de su capacidad para evitar que se sature (eliminando regularmente mensajes antiguos, etc.). Si el buzón llega a saturarse no podrán recibirse mensajes nuevos mientras permanezca saturado. No se deben distribuir listas de direcciones de Correos de la Institución sin expresa autorización del Jefe de TIC de Información De Garper Médica S.A.S.
- El usuario es responsable de difundir su cuenta de correo, por lo tanto, la publicación de esta en sitios web, listas de correo, inscripciones a sitios de interés, provocara probablemente, el ataque continuo de correo basura (Spam)

con publicidad en internet, por lo tanto, no se puede divulgar la cuenta de correo en estos medios.

Condiciones de uso

- ✓ Podrán tener correo electrónico Institucional todas aquellas personas de las diferentes áreas administrativas y asistenciales que se considere tenga necesidad de este servicio y tengan un vínculo laboral con Garper Médica S.A.S, las cuales serán asignadas con previa autorización del Jefe de TIC de Información De Garper Médica S.A.S.

- ✓ Los usuarios podrán tener correo institucional siempre y cuando cumplan con los términos de condiciones y las normas internas de la Institución; como también deberá tener claro que es para uso exclusivo de Garper Médica S.A.S mas no para uso de tipo personal o comercial.

- ✓ Se deberá usar lenguaje apropiado para los mensajes y manejar conductas de cortesía al momento del uso.

Están completamente prohibidas las siguientes actividades:

- ✓ Utilizar el correo electrónico para cualquier propósito personal de índole comercial o financiero.

- ✓ No se debe participar en la propagación de “cartas en cadenas”, ni en esquemas piramidales de índole político, religioso o temas similares.

- ✓ Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados.

- ✓ Distribuir mensajes ofensivos, con palabras inapropiadas o que vulneren la integridad o buen nombre de la institución o de las personas.

- ✓ Leer correos ajenos, generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.

- ✓ Violar los derechos de cualquier persona o Institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.

- ✓ Usar el correo con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil o maliciosa.

- ✓ Enviar por correo electrónico material que contenga virus de software, o cualquier otro código de computadora, archivos o programas diseñados para, destruir o limitar el funcionamiento de algún software o disco duro de computadora o equipo de telecomunicaciones.

- ✓ El usuario se responsabiliza de mantener la confidencialidad de su contraseña y cuenta y de todas las actividades que se efectúen bajo éstas, con el fin de que en toda información o contenido se mantenga su seguridad.

Política para desarrollo externo de software.

Objetivo: Velar porque el desarrollo externo de software cumpla con los requerimientos de seguridad esperados, con buenas prácticas para desarrollo seguro, así como con metodologías para la realización de pruebas de aceptación y seguridad. Además, asegurar que todo software desarrollado externamente cuente con el nivel de soporte requerido por Garper Médica S.A.S.

- El propietario de los TIC de información o a quien delegue es responsable de realizar las pruebas para asegurar que los TIC de información cumplan con los requerimientos de seguridad establecidos antes del paso a producción de los TIC. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- El área de TIC debe contar con TIC de control de versiones para administrar los cambios de los TIC de información de Garper Médica S.A.S.
- El área de TIC debe asegurar que los TIC de información desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- El área de TIC, a través de sus funcionarios, debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- Validar que los desarrolladores de los TIC de información empleen buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- El área de TIC debe contar con un contrato de soporte vigente o asegurar la prestación de soporte por parte del proveedor de software (SLA). Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de Garper Médica S.A.S; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Validar que los desarrolladores construyan los aplicativos de tal manera que se efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable.
- Verificar que en los desarrollos efectuados se asegure la validación de la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de

caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

- Validar que en los desarrollos ejecutados existan los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Validar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

Política para seguridad de equipos y activos fuera de las instalaciones.

Objetivo: Proteger los activos y equipos de la organización que se encuentren fuera de las instalaciones.

- La asignación de equipos de cómputo debe ser realizada por el jefe de área y esta debe quedar documentada detallando el equipo asignado y usuario a quien se responsabiliza.
- El uso de equipos de cómputo y activos de información fuera de las instalaciones de Garper Médica S.A.S, debe ser autorizado por el jefe del área respectiva.
- Todo equipo de cómputo que sea retirado de Garper Médica S.A.S por aprobación del jefe de área para funciones del cargo, debe ser registrado en las bitácoras llevadas por la empresa de vigilancia al momento de ser retirado e ingresado de las instalaciones.
- Todo equipo que sea retirado de Garper Médica S.A.S no debe ser desatendido en áreas de acceso público y deben seguirse las directrices de la política de escritorio, pantalla limpia y equipos desatendidos.

- Cuando el usuario viaje con un equipo de cómputo portátil de propiedad de Garper Médica S.A.S, éste debe ser transportado como equipaje de mano y de forma disimulada.
- Se deben observar siempre las instrucciones del fabricante para proteger los equipos contra exposiciones a campos electromagnéticos, fuertes entradas de polvo, humedad, entre otros.

Política para seguridad de oficinas e instalaciones

Objetivo: Proveer mecanismos de control y seguridad física en aquellas áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren equipos y demás infraestructura de soporte a los sistemas de información que se consideren áreas seguras y de acceso restringido.

- Mantener de manera discreta el centro de datos, las oficinas TIC y demás áreas donde se almacene información sensible, sin señales externas o internas de tal manera que las actividades de procesamiento de información se mantengan reservadas.
- No dejar solos en las oficinas o áreas seguras a personal ajeno al área (visitantes, proveedores, entre otros).
- Las puertas y ventanas de oficinas y recintos se deben mantener cerradas cuando se termine la jornada laboral (en áreas que aplique) o cuando no haya vigilancia y se debe contar con protección externa para las ventanas ubicadas en niveles bajos.
- Almacenar los equipos redundantes y la información de resguardo (Backup) en un sitio seguro y distante del lugar de procesamiento de información.
- Las visitas autorizadas para ingresar a áreas seguras donde se maneja información sensible deben quedar registrado en bitácoras de control y durante la permanencia en éstas debe haber acompañamiento siempre por personal debidamente autorizado y que haga parte del área.

- El acceso a áreas seguras donde se procesa o almacena información sensible debe ser controlado y restringido solo a personas autorizadas.
- Todo lugar de trabajo en que exista algún riesgo de incendio ya sea por la estructura del edificio o por la naturaleza del trabajo que se realiza, debe contar con extintores de incendio, de acuerdo al tipo de material combustible o inflamable.
- En áreas donde existan, se almacenen, trasvasijen o procesen sustancias inflamables o de fácil combustión, deberá establecerse una estricta prohibición de fumar.
- Almacenar los materiales peligrosos o combustibles en lugares seguros y bajo condiciones de seguridad.
- No se deben ingerir alimentos y/o bebidas en cercanías a los equipos y/o dispositivos de cómputo.
- Los funcionarios y terceros deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren dentro de las instalaciones.
- Mantener vigilancia continua dentro de las instalaciones de Garper Médica S.A.S.

7 CONCLUSIONES

Finalmente se logra el diseño de la etapa de planificación de un sistema de gestión de seguridad de la información para el área de tecnología de la IPS Garper médica SAS basado en la norma ISO/IEC 27001:2013, esta corresponde a una necesidad importante para alcanzar las metas relacionadas al crecimiento de la organización, adicionalmente la identificación de los activos de información es un proceso base para las etapas de identificación de riesgos y asignación de controles, las etapas descritas correspondientes a la implementación de un SGSI están directamente relacionadas a la consolidación organizada de políticas de seguridad con base a los activos de la clínica.

Se determina el estado de los lineamientos de seguridad implementados en la IPS Garper Médica, logrando la identificación de madurez tecnológica, lo anterior con base en el instrumento de evaluación MSPI de Min TIC, logrando analizar los resultados de acuerdo con un valor asignado sobre cada control teniendo en cuenta la norma ISO/IEC 27001:2013, definiendo aspectos relevantes de la evaluación y detalle de dominios fuertes que tiene Garper Médica Sas.

Posteriormente se contempla una labor de monitoreo y control de efectividad del SGSI, se logra el análisis de las vulnerabilidades y riesgos que son importantes definir a partir del análisis individual de cada activo de la organización y sus posibles situaciones de riesgo.

Se elaboran las políticas necesarias que permiten la gestión de los riesgos y amenazas para la prevención de un evento cibernético, siendo más efectivos al interior de la IPS y mostrando un crecimiento.

Toda organización, sin importar el nicho de mercado, requiere la implementación de un SGSI mediante el cual se gestionen herramientas y procesos que aseguren la integridad, confidencialidad y disponibilidad de la información.

8 RECOMENDACIONES

- Es importante tener e implementar un buen SGSI, ya que es la mejor manera para identificar riesgos en la IPS Garper Médica SAS, lo cual permite gestionar los controles pertinentes con el fin de mantener la confidencialidad, integridad y disponibilidad de la información en sus diferentes procesos informáticos.

- El nivel de implementación del SGSI en la IPS no es óptimo para el tiempo que lleva de funcionamiento la IPS. Las características y objetivos no son tan claros dentro del alcance que se tiene establecido y se evidencia poco trabajo al respecto: La alta dirección debe ser consciente que con la madurez del sistema se tendrán que tener nuevos controles que en algunos casos conllevan una inversión económica para poder implementarlos , por lo cual siempre deben estar enterados de lo que se planifico, lo que se desarrolló, lo que se implementó y de lo que se mejoró, siempre serán parte activa dentro del ciclo de Planear, Hacer, Verificar y Actuar.

- Es claro que los esfuerzos que se han realizado por los responsables de la planificación del SGSI, son evidentes, sin embargo, es necesario que esta área cuente con el apoyo de toda la organización, y de esta forma conocer sus responsabilidades y gestión dentro de la misma.

- La medición de los controles, análisis de riesgos y aplicabilidad de las políticas debe estar apoyado a todo el equipo, ya que, si se deja en el toda la carga y la responsabilidad a una sola área, se podría saturar en la gestión, ya que el sistema en si no es estático sino cambiante teniendo en cuenta los objetivos del negocio.

BIBLIOGRAFÍA[YN2]

CARBAJOSA Ana, Ciberataque a un hospital alemán en tiempos de pandemia. [Sitio web]. [Consulta: el 15 de abril de 2021] Disponible en: https://elpais.com/internacional/2020-10-03/ciberataque-a-un-hospital-aleman-en-tiempos-de-pandemia.html

CASTAÑEDA, Daniel Hernán, CÁRDENAS Andrés, Implementación de un sistema de gestión en seguridad de la información para el hospital agua de dios, Universidad Piloto De Colombia en el Año 2018.

CASTRO Gil, Manuel A. Gestión de Proyectos con Microsoft Project 2013. España: Editorial RA-MA.

CHRISTOPHER J. Alberts; OCTAVE catalogue of practices, version 2.0, *2021*, Carnegie Mellon, Software Engineering Institute, pp.56-64

COLOMBIA. CONGRESO DE LA REPUBLICA. ley 1273 de 2009. [Consulta: el 05 de enero del 2021] Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado. Diario Oficial. Bogotá: El Congreso, 2009. 2 p

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *2021*. Libro II - Catálogo de Elementos. pp 20.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. pp 20.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: © Ministerio de Hacienda y Administraciones Públicas.

DUARTE, María Carolina. Diseño de políticas de seguridad de la información para la unidad de tecnología de la cámara de comercio de Cúcuta. Trabajo de grado. Cúcuta: UNAD, Facultad de Ingenierías, Departamento de Seguridad informática, 2019.

ESCUELA EUROPEA DE EXCELENCIA. 10.2. No conformidad y acción correctiva. [Sitio web]. https://www.nueva-iso-9001-2015.com/10-2-no-conformidad-y-accion-correctiva/ .

ESCUELA EUROPEA DE EXCELENCIA. Gestión de Riesgos: Identificación y Análisis de Riesgos. [Sitio web]. [Consulta: el 15 de abril de 2021]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2016/07/gestion-de-riesgos-identificacion-analisis/

ESCUELA EUROPEA DE EXCELENCIA. Gestión de Riesgos: Identificación y Análisis de Riesgos. [Sitio web]. [consulta: 15 de abril de 2021]. Disponible en:https://www.escuelaeuropeaexcelencia.com/2016/07/gestion-de-riesgos-identificacion-analisis/

ESCUELA EUROPEA DE EXCELENCIA. Metodología Mehari para el análisis de Riesgos en SGSI. Sitio web [Consulta: 11 de diciembre del 2021], Disponible en: https://www.pmg-ssi.com/2021/09/metodologia-mehari-para-el-analisis-de-riesgos-en-sgsi/

GARPER MÉDICA SAS. Reseña histórica. [Sitio web]. [Consulta: 02 de Mayo del 2021], Disponible en: https://www.garperMédica.com/nosotros_resena_historica.html

HURTADO, Martha. Gestión del riesgo Metodologías OCTAVE Y MAGERIT. Universidad Piloto de Colombia, 2020 1, pp. 1-11.

INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? 2021, de Gobierno de España [Sitio web]. https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian .

INSTITUTO NACIONAL DE CIBERSEGURIDAD - INCIBE. Ciberseguridad para tu sector salud. SECtoriza2, [Sitio web]. [Consulta: el 12 de noviembre del 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sectoriza2-ciberseguridad-especifica-el-sector-salud

ISO 27000.ES. El portal de ISO 27001 en español. [Sitio web]. [Consulta: el 16 de mayo del 2021]. Disponible en: http://www.iso27000.es/iso27000.html

ISO27000.ES. Temas relacionados con los SGSI y la seguridad de la información. [Sitio web]. [Consulta: el 15 de abril de 2021]. Disponible en: http://www.iso27000.es/

ISO27000.ES. Temas relacionados con los SGSI y la seguridad de la información. [Sitio web]. [Consulta: el 15 de abril de 2021] Disponible en: http://www.iso27000.es/

ISOTOOLS EXCELLENCE. ISO 27001 y la gestión de los riesgos de la seguridad de la información en PYMEs. 2021, de PMG SSI Sitio web: [Sitio web]. [Consulta: el 15 de abril de 2021] https://www.pmg-ssi.com/2014/08/iso-27001-gestion-riesgos-seguridad-informacion-pymes/

MAYA ARANGO, Paula Andrea, Plan de implementación del SGSI basado en la norma ISO 27001:2013. Universidad Oberta de Catalunya 2016.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. (2017). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España: © Ministerio de Hacienda y Administraciones Públicas

MINTIC. Guía para la implementación de seguridad de la información en una MiPyme. [Sitio web]: [Sitio web]. [Consulta: 15 de abril de 2021]. Disponible en:https://www.mintic.gov.co/gestionti/615/articles482_Guia_Seguridad_informacion_Mypimes.pdf

MINTIC.GOV. Guía de Gestión de Riesgos. Gestión y Privacidad de la Información. [Sitio web]. [Consulta: 15 de abril de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles5482_G7_Gestion_Riesgos.pdf

MINTIC.GOV. Guía de Gestión de Riesgos. Gestión y Privacidad de la Información. [Sitio web]. [Consulta: el 15 de abril de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles5482_G7_Gestion_Riesgos.pdf

NECTEC.COM. ¿Qué es seguridad informática? [Sitio web]. [Consulta: el 15 de abril de 2021]. Disponible en: https://www.netec.com/que-es-seguridad-informatica.

NEIRA LOPEZ, Agustín. ISO 27000. 2021, de Lead Tutor ISO 27001 [Sitio web]: [Consulta: 20 de diciembre]. Disponle en: https://www.iso27000.es/sgsi.html

NORMAS-ISO.COM. ISO 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN [Sitio web]. [Consulta: 15 de abril de 2021]. Disponible en: https://www.normas-iso.com/iso-27001/

NORMAS-ISO.COM. ISO 27001 seguridad de la información .ISO 27001 gestión de la seguridad de la información. [Sitio web]. [Consulta: el 15 de abril de 2021] Disponible en: https://www.normas-iso.com/iso-27001/

NORMAS-ISO.COM. ISO 27001 SEGURIDAD DE LA INFORMACIÓN. [Sitio web]. [Consulta: 15 de abril de 2020]. Disponible en: https://www.normas-iso.com/

PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA. Software ISO Calidad. 2021, de ISOTools [Sitio web]. [Consulta: 15 de abril de 2020]. Disponible https://www.isotools.org/normas/calidad/iso-9001/ .

ROMERO de Castro, Martha Irene. (2018). La seguridad en términos generales. En INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES (13- 22). Manabí: Innovación y Desarrollo,S.L.

SANTIAGO, Enrique Javier, SANCHEZ Jesús. Riesgos de ciberseguridad en las empresas. Universidad Alfonso X el Sabio, Escuela Politécnica Superior. Villanueva de la Cañada Madrid. [Sitio web]. [Consulta: 10 de septiembre del 2021]. Disponible en http://www.uax.es/publicacion/riesgos-de-ciberseguridad-en-las-empresas