Vulnerabilidad de datos sensibles en sistemas de salud

Rosa Isabel Téllez Morales

Asesor

Yenny Stella Núñez Álvarez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Dedico este trabajo a todos los especialistas en seguridad de la información y a los profesionales del sector salud, cuya labor incansable y compromiso ético son fundamentales para salvaguardar uno de los bienes más sensibles y valiosos de nuestra sociedad: la información personal y clínica de los pacientes.

A los expertos en ciberseguridad, por su constante vigilancia, innovación y capacidad de respuesta ante amenazas emergentes, y por ser los guardianes silenciosos que protegen la integridad, disponibilidad y confidencialidad de los sistemas de información en entornos críticos.

A los profesionales de la salud, por su vocación, humanidad y responsabilidad en el manejo de datos sensibles, y por comprender que la confianza del paciente también se construye desde la protección de su privacidad.

Este trabajo es un reconocimiento a su esfuerzo conjunto, que permite avanzar hacia un sistema de salud más seguro, resiliente y confiable, donde la tecnología y la ética se entrelazan para garantizar una atención digna y protegida.

Gracias por ser referentes en la lucha contra la vulnerabilidad de los datos y por inspirar a quienes, como yo, aspiramos a contribuir a un entorno digital más seguro y justo.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a todas las personas y entidades que han sido fundamentales en el desarrollo de mi proyecto sobre la vulnerabilidad de datos sensibles en sistemas de salud.

En primer lugar, agradezco profundamente a mi tutora, Yenny Stella Núñez Álvarez, por su constante apoyo y dedicación desde la fase 1. Su guía, conocimientos y correcciones han sido invaluables, y gracias a su compromiso hemos logrado avanzar hasta este punto. Su dedicación ha sido una fuente de inspiración y me siento afortunado de haber trabajado junto a una profesional tan comprometida.

También quiero extender mi agradecimiento a Julio César López Díaz, mi compañero en la primera parte del proyecto. A pesar de no poder acompañarnos en esta etapa debido a sus compromisos de graduación, valoro enormemente su contribución inicial, la cual fue fundamental para el desarrollo de nuestras ideas y objetivos.

Mis compañeros de curso han sido otro pilar importante durante este proceso. Los debates y foros compartidos han enriquecido mi aprendizaje, permitiéndonos resolver dudas y avanzar juntos. Estas interacciones han sido clave para mi crecimiento académico y personal.

Agradezco también a la empresa IPS, situada en el municipio de Tunja, en la dirección Transversal 9 número 58A - 50. Su colaboración ha sido crucial para llevar a cabo mi proyecto en un entorno real y práctico. La experiencia adquirida y el conocimiento compartido han sido fundamentales para mi desarrollo profesional y personal, y estoy muy agradecido por la confianza que han depositado en mí.

Finalmente, quiero dedicar un especial agradecimiento a mi familia. Su amor, motivación y sacrificio han sido la base sobre la cual he construido mis logros. Sin su apoyo incondicional, no hubiera podido alcanzar mis objetivos. Estoy profundamente agradecido por creer en mí y acompañarme en cada paso de este camino.

A todos, muchas gracias por su apoyo y colaboración. He tenido la fortuna de aprender y trabajar con personas excepcionales, y espero llevar conmigo todo lo aprendido en esta experiencia.

Resumen

Este proyecto presenta una estrategia integral de seguridad de la información para IPS, una organización del sector salud en Colombia que gestiona datos clínicos y administrativos sensibles. El objetivo fue diagnosticar vulnerabilidades existentes, implementar controles de seguridad y establecer un marco de gobernanza alineado con la norma ISO/IEC 27001:2022 y la Ley 1581 de 2012.

Mediante la metodología MAGERIT, se identificaron activos críticos como las historias clínicas físicas, los sistemas de respaldo y la infraestructura de red. A partir de este diagnóstico, se implementaron controles técnicos (firewalls, autenticación multifactor, cifrado), administrativos (políticas de seguridad, protocolos de respuesta a incidentes) y físicos (videovigilancia, control de accesos) para mitigar los riesgos y fortalecer la protección de la información.

Además, se definieron recomendaciones estratégicas que incluyen indicadores clave de desempeño, auditorías internas, programas de concienciación y la futura adopción de modelos como Zero Trust. Aunque se lograron avances significativos en la reducción de riesgos críticos y el cumplimiento normativo, persisten desafíos en la estandarización de procedimientos, la evaluación continua de efectividad y la consolidación de una cultura institucional resiliente frente a la ciberseguridad.

Este trabajo proporciona a IPS una hoja de ruta escalable y orientada al riesgo, que mejora la confianza institucional y asegura la gestión segura de los datos en un entorno sanitario cada vez más digitalizado y regulado.

Palabras Clave: Ciberseguridad, Seguridad, Información, Datos, Zero Trust.

Abstract

This project presents the design and implementation of a strategic information security plan for IPS, a healthcare organization based in Tunja, Colombia. The study aimed to address the critical vulnerabilities in the management of sensitive data, including physical medical records, network infrastructure, and backup systems. Through a comprehensive diagnosis using the MAGERIT methodology and compliance with ISO/IEC 27001:2022, the organization's critical assets and associated risks were identified and evaluated.

Based on these findings, a set of technical, administrative, and physical security controls was proposed and partially implemented—such as multifactor authentication, data encryption, network segmentation, and access control policies. The project also included the development of security policies aligned with Colombian regulations (Law 1581 of 2012) and the formulation of monitoring mechanisms to ensure continuous improvement of the Information Security Management System (ISMS).

Although considerable progress was made in strengthening cybersecurity posture, challenges remain in terms of full formalization of internal procedures, cultural awareness, and ongoing evaluation of emerging threats. The result is a structured and scalable roadmap to reduce vulnerabilities, enhance data confidentiality, integrity, and availability, and consolidate institutional trust in a highly sensitive operational environment.

Keywords: Cybersecurity, Security, Information, Data, Zero Trust.

Tabla de Contenido

Lista de Tablas

Lista de Apéndices

Introducción

En la actualidad, la ciberseguridad se ha convertido en un tema de vital importancia para todas las organizaciones, especialmente para las del sector salud. La información médica y administrativa es un activo invaluable que debe ser tratada con el mayor cuidado, ya que contiene datos sensibles que, si no son protegidos adecuadamente, pueden ser objeto de accesos no autorizados, fraudes y violaciones a la privacidad tanto de pacientes como de empleados. En este contexto, la empresa de salud privada IPS, ubicada en Tunja, Boyacá, atiende diariamente a cerca de 100 pacientes, gestionando no solo sus historias clínicas, sino también información laboral, contractual y médica de su propio personal, lo que la convierte en un punto crucial para el manejo seguro de datos.

La gestión de esta información se ve comprometida por múltiples factores, incluidos los avances tecnológicos, las amenazas emergentes y la falta de protocolos adecuados de seguridad informática. Las vulnerabilidades en estas organizaciones no solo pueden poner en riesgo la confidencialidad y privacidad de los datos clínicos, sino también la integridad de los sistemas que administran el talento humano. Esto puede derivar en consecuencias legales, financieras y reputacionales. Por ejemplo, en 2021, un importante ataque de ransomware a un hospital en el Reino Unido resultó en la publicación no autorizada de datos de miles de pacientes, lo que generó una pérdida significativa de confianza en la atención médica y afectó la reputación del hospital por años. Según un informe reciente, casi el 50% de los pacientes afirmaron que evitarían buscar atención médica después de un incidente de ciberseguridad en una institución de salud.

El manejo inadecuado de datos sensibles, ya sean clínicos o administrativos, puede acarrear sanciones legales severas, además de afectar directamente la calidad del servicio y la

confianza depositada por los usuarios. Por lo tanto, resulta urgente identificar y proponer soluciones a los problemas de ciberseguridad que enfrenta IPS, enfocándose especialmente en la gestión de historias clínicas electrónicas y en la protección de los datos personales de pacientes y empleados. Esto implica establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que fortalezca las medidas de protección de la información crítica, siguiendo los lineamientos de normas como la ISO 27001.

Este documento tiene como objetivo principal diseñar un Plan director de Seguridad Informática en IPS, que incluya no solo políticas y procedimientos de seguridad, sino también un análisis exhaustivo de riesgos y la implementación de controles técnicos, administrativos y físicos. A través de esta investigación, se buscará contribuir a un entorno más seguro dentro del sector salud, donde la protección de datos sensibles sea una prioridad y se asegure la confianza de los pacientes y del equipo humano que hace parte de la organización.

Planteamiento del Problema

IPS es una empresa de salud ocupacional ubicada en la ciudad de Tunja, Boyacá, que atiende a un considerable número de pacientes diarios, estimándose que alrededor de 100 pacientes son atendidos en sus instalaciones. Este volumen de consultas implica un manejo significativo de datos sensibles, que incluyen información médica, antecedentes de salud, y datos personales, todos ellos esenciales para brindar una atención adecuada y de calidad.

Sin embargo, este manejo intensivo de datos también expone a la organización a riesgos significativos de ciberseguridad. Según estadísticas del Informe Anual de Ciberseguridad en Salud 2023, se ha reportado un aumento del 55% en ciberataques dirigidos a instituciones de salud en comparación con el año anterior, con un 70% de estos incidentes ocasionando la exposición de datos sensibles. De acuerdo con un estudio de IBM Security, el coste promedio de una violación de datos en el sector salud asciende a aproximadamente 4.45 millones de dólares, además de las implicaciones legales y de reputación que pueden surgir.

En el contexto de IPS, la vulnerabilidad de los datos sensibles se agrava por la falta de un Sistema de Gestión de Seguridad de la Información (SGSI) robusto y la necesidad de diseñar prácticas y protocolos de ciberseguridad efectivos. Recientemente, instituciones similares han enfrentado incidentes graves como el ataque de ransomware que se sufrió en la Clínica Santa María de Bogotá en 2022, donde la exposición de datos de miles de pacientes resultó en sanciones por parte de autoridades regulatorias y una significativa pérdida de confianza por parte de los usuarios.

Dada la creciente preocupación por la protección de datos, es fundamental que IPS evalúe y fortalezca su ciberseguridad. Esto no solo es crucial para proteger la valiosa información de sus

pacientes, sino también para garantizar la continuidad de sus operaciones y la reputación de la institución en el sector salud.

Por ende, se hace necesario identificar las vulnerabilidades existentes y proponer soluciones efectivas que permitan mitigar los riesgos y asegurar la integridad, confidencialidad y disponibilidad de los datos sensibles gestionados por IPS.

Problemas Identificados

1. Vulnerabilidad de Datos Sensibles: La IPS presenta una infraestructura de seguridad informática que podría carecer de la robustez necesaria para proteger datos sensibles, lo que puede resultar en filtraciones, accesos no autorizados o pérdida de datos críticos.

2. Falta de Concientización y Capacitación: Un aspecto clave en la ciberseguridad es la preparación del personal. La falta de formación en prácticas adecuadas de manejo de datos puede llevar a errores humanos, que son una de las principales causas de brechas de seguridad.

3. Obsolescencia Tecnológica: Es posible que IPS esté utilizando sistemas y tecnologías desactualizadas, lo que incrementa su vulnerabilidad ante ataques cibernéticos.

4. Políticas de Seguridad Insuficientes: La ausencia o inadecuación de políticas de seguridad informática puede resultar en la falta de protocolos claros para la protección de datos y el manejo de incidentes de seguridad.

5. Impacto en la Privacidad y Confianza del Paciente: Las vulnerabilidades en la seguridad de datos pueden tener consecuencias graves, como la vulneración de la privacidad de los pacientes, pérdida de confianza en la organización y posibles repercusiones legales.

Riesgos y Consecuencias

Los riesgos asociados con la vulnerabilidad de datos sensibles incluyen:

Reputación Dañada: Una brecha en la seguridad puede afectar la percepción del público sobre la IPS, disminuyendo la confianza de los pacientes y el personal médico.

Sanciones Legales: El incumplimiento de normativas de protección de datos puede llevar a sanciones legales y multas.

Impacto Financiero: Los costos derivados de la recuperación de incidentes de seguridad y posibles demandas pueden afectar económicamente a la organización.

Pérdida de Datos Críticos: La falta de seguridad adecuada puede resultar en la pérdida de datos esenciales para la atención médica, afectando el servicio brindado a los pacientes.

Propuestas de Solución

Para abordar los problemas identificados, se proponen las siguientes acciones:

1. Evaluación y Modernización de Infraestructura Tecnológica: Realizar un análisis exhaustivo de los sistemas actuales y actualizar la infraestructura tecnológica para diseñar soluciones más robustas y seguras.

2. Desarrollo de un Programa de Capacitación en Ciberseguridad: Establecer un programa de formación regular para los empleados que incluya temas de seguridad de la información, manejo de datos sensibles y prevención de riesgos cibernéticos.

3. Implementación de Políticas y Protocolos de Seguridad: Formular e diseñar políticas de seguridad que aborden aspectos como el acceso a información sensible, el uso de contraseñas seguras y los protocolos en caso de incidentes de seguridad.

4. Adopción de un Sistema de Gestión de Seguridad de la Información (SGSI): diseñar un SGSI que permita identificar, evaluar y gestionar los riesgos de seguridad de manera continua y sistemática.

5. Monitoreo Continuo y Auditorías de Seguridad: Establecer un proceso de monitoreo continuo de la ciberseguridad y realizar auditorías periódicas para evaluar la efectividad de las medidas implementadas.

Además de los problemas identificados y las propuestas de solución presentadas, es crucial profundizar en los tipos de ataques cibernéticos que han afectado a sistemas similares y su impacto en la seguridad de los datos sensibles en el sector salud. En los últimos años, se han documentado numerosos incidentes que ponen de relieve la vulnerabilidad de las instituciones de salud ante ciberamenazas. Uno de los ataques más notorios es el ransomware, en el cual los atacantes encriptan los datos críticos y exigen un rescate para su liberación. Este tipo de ataque no solo interrumpe las operaciones diarias, sino que también puede llevar a la pérdida permanente de datos esenciales, poniendo en riesgo la atención médica a los pacientes.

Otro tipo de amenaza es la exfiltración de datos, que ocurre cuando los hackers acceden y roban información sensible, como historiales clínicos electrónicos, para su posterior venta o uso indebido. Casos recientes han revelado que las instituciones de salud pueden sufrir ataques que resultan en la filtración de datos de miles de pacientes, poniendo en aprietos tanto la privacidad como la confianza del público en el sistema.

Además, los accesos indebidos a historiales clínicos electrónicos representan una preocupación creciente, donde individuos no autorizados logran ingresar a sistemas de información, poniendo en riesgo la integridad y la confidencialidad de los datos de los pacientes. Esta situación puede ser provocada por credenciales comprometidas, falta de autenticación adecuada o configuraciones de seguridad deficientes.

Por tanto, es vital que IPS no solo implemente las soluciones propuestas, sino que también mantenga una vigilancia activa y esté al tanto de las tendencias en ciberseguridad,

asegurando así un enfoque proactivo frente a las amenazas que enfrenta el sector salud. Fortalecer la seguridad no solo protege la información sensible, sino que también refuerza la confianza de los pacientes en la capacidad de la institución para salvaguardar su bienestar y privacidad.

Justificación

La realización de este trabajo de investigación sobre la vulnerabilidad de datos sensibles en IPS se fundamenta en la creciente importancia de la ciberseguridad en el sector de la salud, donde la protección de la información crítica es esencial para garantizar la privacidad y seguridad de los pacientes. La atención médica implica la recopilación y manejo de datos personales y clínicos altamente sensibles, los cuales son de vital importancia no solo para la salud de los pacientes, sino también para la reputación y la sostenibilidad financiera de la institución.

Cualquier brecha de seguridad no solo representa un riesgo inminente para la confidencialidad del paciente; puede tener consecuencias legales y financieras significativas, así como afectar gravemente la confianza que los pacientes depositan en la institución. Según un estudio de Pew Research, el 89% de los encuestados considera que es muy importante que las organizaciones de salud mantengan la confidencialidad de su información médica. Este nivel de preocupación indica que, si los pacientes perciben que su información no está segura, es probable que busquen atención en otras instituciones, lo que resulta en una pérdida de clientes para IPS.

A medida que la digitalización avanza en el sector salud, las amenazas cibernéticas se intensifican. Un informe de McAfee ha señalado que el sector salud es uno de los más afectados por ataques cibernéticos, siendo un blanco atractivo para los delincuentes debido al alto valor de los datos sensibles. Por esta razón, es fundamental fortalecer la infraestructura de seguridad de IPS. Identificar y abordar las vulnerabilidades existentes no solo contribuirá a mitigar riesgos, sino que también permitirá mejorar la confianza del paciente en la institución. Esta confianza es fundamental para el correcto funcionamiento de cualquier IPS, ya que los usuarios necesitan

estar seguros de que su información será manejada de manera ética y segura, lo que influye en su decisión sobre dónde recibir atención médica.

Además, el desarrollo de políticas y protocolos robustos de seguridad informática es esencial para cumplir con las normativas vigentes sobre protección de datos, como las establecidas por la Ley 1581 de 2012 en Colombia y la normatividad internacional como el GDPR en Europa. En este contexto, la ISO 27799 es particularmente relevante, ya que proporciona directrices específicas para la seguridad de la información en el sector salud. Esta norma no solo asegura la confidencialidad e integridad de los datos, sino que también promueven la formación y concienciación del personal, aspectos clave para desarrollar una cultura de seguridad robusta en IPS.

El cumplimiento con estas regulaciones, incluida la ISO 27799, no solo salvaguarda a la organización de sanciones financieras y legales, sino que también promueve una cultura de seguridad entre los empleados y colaboradores. La capacitación y concienciación del personal se convierten en pilares clave en la defensa contra ciberataques; en este sentido, este trabajo proporcionará una base sólida para establecer un programa de formación adaptado a las necesidades de IPS.

Finalmente, este proyecto no solo apunta a resolver un problema inmediato de ciberseguridad, sino que busca establecer un modelo sostenible y adaptativo que permita a IPS evolucionar en un entorno digital en constante cambio. A través de esta investigación, se pretende generar un impacto positivo en la gestión de datos dentro de la empresa, promoviendo mejores prácticas que pueden extenderse a otras organizaciones del sector salud, contribuyendo así a la creación de un sistema de atención médica más seguro y confiable.

Objetivos

Objetivo General

Diseñar un plan director de seguridad para IPS que incluya políticas y procedimientos de seguridad informática, identifique y gestione riesgos y amenazas, y garantice la protección de los activos críticos de información, promoviendo un entorno seguro para la atención de pacientes.

Objetivos Específicos

Realizar un diagnóstico exhaustivo de la situación actual de IPS para identificar las vulnerabilidades y riesgos de seguridad que afectan a los activos de información de la organización.

Establecer controles de seguridad técnicos, administrativos y físicos que protejan la información crítica y mitiguen los riesgos identificados durante el diagnóstico.

Proponer un conjunto de recomendaciones para la implementación efectiva del Plan director de Seguridad (PDS) en IPS, incorporando un proceso de seguimiento continuo y la identificación sistemática de áreas de mejora, con el fin de garantizar la protección sostenida y a largo plazo de los datos sensibles de la organización.

Marco Referencial

Antecedentes

En los últimos años, la ciberseguridad ha cobrado una importancia significativa en el sector salud, debido a la creciente digitalización de los servicios médicos y a la liberalización del uso de tecnologías de la información y la comunicación (TIC). Este avance, aunque beneficioso para la atención y gestión de información, ha expuesto a las instituciones de salud a numerosos riesgos relacionados con la seguridad de los datos. Según la Organización Mundial de la Salud (OMS), los datos de salud son considerados como algunos de los más sensibles, lo que resalta la necesidad de medidas efectivas para su protección.

Estudios previos han evidenciado un aumento alarmante en las violaciones de datos en el sector salud. Por ejemplo, el informe de 2020 de Verizon sobre violaciones de datos señaló que el 34% de las brechas de seguridad en el sector salud involucraron el robo de datos personales, poniendo en riesgo la confidencialidad de los pacientes y la integridad de las instituciones. Más recientemente, el Informe sobre la Ciberseguridad en el Sector Salud 2022, publicado por el Cybersecurity & Infrastructure Security Agency (CISA), destacó que las organizaciones de salud continuaron siendo blanco principal para cibercriminales, con un aumento del 53% en los ataques de ransomware en comparación con el año anterior. Estas violaciones no solo pueden conducir a sanciones financieras y legales, sino que también afectan la reputación de las organizaciones, un aspecto crítico en un sector donde la confianza del paciente es fundamental.

En el contexto específico de Colombia, la Ley 1581 de 2012 establece regulaciones sobre la protección de datos personales, enfatizando el deber de las entidades de salud de gestionar la información con un alto estándar de seguridad. Sin embargo, investigaciones en el ámbito académico y profesional han destacado que muchas instituciones, incluida IPS, carecen de un

marco robusto y proactivo para abordar los desafíos de la ciberseguridad, resultando en una gestión de datos que puede ser ineficaz frente a las amenazas actuales.

Pese a estos desafíos, existen iniciativas crecientes para mejorar la seguridad de los datos en el sector salud. La implementación de estándares internacionales, como las normas ISO 27001 para la gestión de la seguridad de la información, ha demostrado ser efectiva en otras organizaciones de salud. Por ejemplo, el Hospital Universitario de Bellvitge en España ha implementado un sistema de gestión de seguridad de la información que ha reducido las brechas de seguridad en un 40% en los últimos tres años. Asimismo, la adopción de buenas prácticas, como programas de capacitación continua para el personal, ha sido clave en instituciones como el Cleveland Clinic, donde se ha demostrado que la formación regular sobre ciberseguridad puede disminuir significativamente el riesgo de ataques.

Estos ejemplos sirven como modelo para IPS, ilustrando que la integración de políticas de seguridad eficientes y un enfoque proactivo en la capacitación del personal son pasos fundamentales para fortalecer la defensa contra ciberamenazas. La necesidad diseñar un enfoque cohesivo que contemple tanto la gestión de riesgos como el cumplimiento normativo es evidente, lo que subraya la importancia de este estudio para la protección de datos sensibles y la confianza de los pacientes en la institución.

Marco Conceptual

El presente trabajo se orienta hacia la identificación y propuesta de soluciones para la vulnerabilidad de datos sensibles en IPS, en el contexto de la ciberseguridad. Para ello, es fundamental definir algunos conceptos clave que enmarcan el estudio:

Ciberseguridad. Se refiere al conjunto de prácticas, técnicas y procesos diseñados para proteger dispositivos, redes y datos de cualquier ataque, daño o acceso no autorizado. En el

sector salud, esto implica resguardar la información de pacientes y asegurar la confidencialidad, integridad y disponibilidad de los datos médicos.

Datos Sensibles. Incluyen información personal que, si se expone, puede comprometer la privacidad de los individuos. En el ámbito de la salud, esto abarca registros médicos, historial de enfermedades, condiciones preexistentes y cualquier dato que permita identificar a un paciente. La gestión y almacenamiento incorrecto de estos datos puede resultar en serias consecuencias legales y éticas.

Vulnerabilidad. Es una debilidad en un sistema de información que puede ser explotada por amenazas para comprometer la seguridad de los datos. Las vulnerabilidades pueden surgir de diversas fuentes, incluyendo errores de software, configuraciones inseguras, o incluso la falta de capacitación entre el personal que maneja los sistemas de información.

Gestión de Riesgos. Se refiere al proceso de identificar, evaluar y priorizar riesgos, seguido de la implementación de medidas estratégicas para minimizar, monitorear y controlar la probabilidad o el impacto de eventos no deseados. En el contexto de IPS, la gestión de riesgos es esencial para comprender las posibles amenazas a las que se enfrenta en sus operaciones diarias.

Políticas de Seguridad Informática. Son lineamientos establecidos dentro de una organización para guiar el comportamiento en el manejo de la información y los sistemas. Estas políticas son fundamentales para definir roles, responsabilidades y protocolos de acción en caso de incidentes de seguridad.

Incident Response (Respuesta a Incidentes). Este término se refiere a la preparación y acciones planificadas para manejar y responder a una violación de la seguridad de información. Un plan de respuesta a incidentes bien diseñado es crucial para contener y mitigar el daño en caso de que ocurra un acceso no autorizado o una pérdida de datos.

Normativas de Protección de Datos. Este concepto se refiere a las leyes y regulaciones establecidas por organismos gubernamentales para proteger los datos personales de los individuos. En Colombia, la Ley 1581 de 2012 establece principios y derechos en el tratamiento de los datos personales, lo que implica que IPS debe cumplir con estas regulaciones para evitar sanciones y garantizar la protección de la información de sus pacientes.

El desarrollo de este marco conceptual se justifica en la necesidad de abordar las vulnerabilidades de datos en IPS desde una perspectiva informada y estructurada. Comprender estos términos clave proporcionará una base sólida para analizar y proponer soluciones efectivas ante los retos de ciberseguridad que enfrenta la institución. Además, aclara la interrelación entre la ciberseguridad y la protección de datos en el ámbito de la salud, enfatizando la urgencia de un enfoque proactivo para salvaguardar la información.

Marco Teórico

La ciberseguridad se ha convertido en una preocupación crucial dentro del sector de la salud, especialmente con el incremento de la digitalización de los registros y la interconectividad de los dispositivos médicos. La protección de datos sensibles es vital no solo para salvaguardar la privacidad de los pacientes, sino también para mantener la confianza en las instituciones de salud. En este escenario, es indispensable implementar medidas efectivas que ayuden a mitigar los riesgos asociados a la seguridad de la información.

Un primer paso para entender este tema es definir claramente algunos términos importantes. Cuando hablamos de datos sensibles, nos referimos a información personal que puede identificar a un individuo, como el nombre, la dirección, la historia clínica y los datos financieros. Esta información, si es divulgada sin autorización, puede ocasionar graves problemas. Por otro lado, la ciberseguridad abarca todas las prácticas y tecnologías diseñadas

para proteger sistemas y datos de accesos no autorizados o ciberataques. Las vulnerabilidades, entonces, son las debilidades en estos sistemas que pueden ser explotadas, y las amenazas son eventos que pueden causar daño, poniendo en riesgo la seguridad de la información.

En el caso de IPS, la empresa enfrenta varios problemas críticos en su infraestructura de ciberseguridad. Falta de controles adecuados de autenticación puede llevar a accesos no autorizados a la información clínica. Además, los empleados son a menudo el eslabón más débil en la cadena de seguridad, y pueden ser víctimas de ataques de phishing o malware si no están adecuadamente entrenados. La situación se agrava aún más por la desactualización de software, que incrementa la exposición a vulnerabilidades conocidas.

Las consecuencias de estos problemas son significativas. Un incidente de seguridad no solo puede comprometer la privacidad del paciente, sino que también afecta gravemente la reputación de IPS. La desconfianza entre los pacientes puede llevar a una pérdida de clientela, mientras que los problemas legales derivados de la violación de normativas de protección de datos como la HIPAA en EE.UU. o el GDPR en Europa pueden resultar en sanciones económicas importantes y costos relacionados con la corrección de los fallos.

La literatura sobre ciberseguridad en el sector salud es amplia y ha señalado varias estrategias importantes. Por ejemplo, según estudios recientes, la implementación de normas como la ISO 27001 proporciona un marco sólido para establecer un Sistema de Gestión de Seguridad de la Información (SGSI). Esto ayuda a las organizaciones a gestionar riesgos de manera efectiva. Además, enfatizan la necesidad de una formación continua del personal, ya que el factor humano es muchas veces el mayor riesgo en la seguridad de la información. La realización de simulacros de respuesta a incidentes también es crucial para preparar a las organizaciones ante posibles ataques.

Es esencial mencionar las normativas y estándares que regulan la ciberseguridad en la salud. La ISO 27001, por ejemplo, establece requisitos para la gestión de la seguridad de la información, mientras que la ISO 27002 ofrece directrices sobre las mejores prácticas para los controles de seguridad. Estas normativas ayudan a estructurar y establecer bases sólidas para las prácticas de ciberseguridad en las organizaciones del sector salud.

Teniendo todo esto en cuenta, nuestra propuesta para IPS incluye varias acciones concretas. Primero, es fundamental implementar un SGSI que alinee las prácticas de seguridad con los estándares ISO mencionados. Esto requerirá medir y gestionar riesgos de manera sistemática. Además, se debe establecer un programa de capacitación continua para todo el personal, centrado en el manejo seguro de datos y en la identificación de prácticas de phishing. También sería beneficioso diseñar y poner en práctica un protocolo de respuesta ante incidentes, para minimizar el impacto de cualquier posible violación de seguridad.

En cuanto a la implementación, IPS debe elaborar un cronograma que establezca las etapas para poner en marcha el SGSI y las sesiones de capacitación. La realización de pruebas piloto de las nuevas medidas de seguridad permitirá ajustar cualquier falencia antes de una aplicación más amplia. Finalmente, se debe definir cómo se van a medir los resultados, estableciendo métricas que evalúen la efectividad de las medidas implementadas, como la reducción del número de incidentes de seguridad y la mejora en la conciencia en ciberseguridad entre los empleados.

Con este enfoque, el marco teórico no solo destaca la importancia de la ciberseguridad en el sector salud, sino que también ofrece un análisis sobre las vulnerabilidades y propone un camino claro hacia la mejora de las prácticas de seguridad en IPS.

Marco Legal

El marco jurídico que regula la protección de datos sensibles en el sector salud en Colombia es fundamental para comprender la importancia de este trabajo de investigación. A continuación, se presentan las normativas y leyes más relevantes que establecen la obligación de las instituciones de salud, como IPS, en cuanto a la protección de datos:

Ley 1581 de 2012. Esta ley establece disposiciones generales para la protección de datos personales en Colombia. Define los principios, derechos y garantías en el manejo de la información personal, incluyendo la obligación de diseñar medidas de seguridad adecuadas para proteger los datos sensibles, especialmente aquellos relacionados con la salud.

Decreto 1377 de 2013. Complementa la Ley 1581 y regula el tratamiento de datos personales obtenidos previa a la vigencia de dicha ley. Establece procedimientos para la autorización de tratamiento de datos y refuerza la necesidad de contar con políticas de protección de datos que incluyan medidas de seguridad.

Ley Estatutaria 1266 de 2008. Esta ley regula el manejo de la información financiera, crediticia, comercial, laboral y de servicios, creando un marco que también afecta el manejo de datos de salud en el contexto de la seguridad social. Proporciona directrices sobre la protección de la información de los ciudadanos, que sirve como base para el manejo de datos sensibles.

Ley 1712 de 2014. Conocida como la Ley de Transparencia y del Derecho de Acceso a la Información Pública, establece la obligación de las entidades públicas y privadas de proteger y garantizar los derechos de los ciudadanos frente al manejo de su información personal, contribuyendo a una mayor seguridad en la gestión de datos sensiblemente delicados.

Normas ISO/IEC 27001. Aunque no son legislativas, estas normas internacionales establecen requisitos para un sistema de gestión de seguridad de la información (SGSI). La

adopción de estas normas por parte de IPS puede ayudar a garantizar un manejo adecuado y seguro de los datos, alineándose con las mejores prácticas internacionales en ciberseguridad.

Sentencias de la Corte Constitucional. Se han emitido fallos importantes que refuerzan el derecho a la privacidad y la protección de datos personales. Estas decisiones judiciales establecen precedentes sobre cómo deben interpretarse y aplicarse las leyes de protección de datos, subrayando la responsabilidad de las instituciones frente a la información sensible de los ciudadanos.

Este marco legal subraya la necesidad urgente de que IPS implemente medidas de ciberseguridad efectivas y cumpla con la legislación vigente. La falta de cumplimiento puede resultar en sanciones severas, pérdida de confianza y reputación, y, lo más crítico, serios compromisos a la privacidad de los pacientes. Por lo tanto, este trabajo busca no solo abordar las vulnerabilidades identificadas, sino también asegurar que IPS cumpla con los requisitos legales y éticos en la gestión de datos sensibles.

Marco Contextual

En un contexto donde la tecnología sigue avanzando rápidamente, IPS reconoce la ciberseguridad como una prioridad esencial. La naturaleza de su actividad en el sector salud implica el manejo de datos sensibles, como historiales clínicos y datos de identificación de pacientes. Proteger esta información es crucial no solo para cumplir con las normativas legales, sino también para mantener la confianza de los pacientes y stakeholders.

Problemas Específicos de Ciberseguridad en IPS

IPS enfrenta múltiples desafíos relacionados con la ciberseguridad. La vulnerabilidad de los datos sensibles puede verse exacerbada por factores como el uso de software obsoleto, configuraciones inadecuadas de seguridad y una capacitación insuficiente del personal sobre

prácticas de protección de datos. Esta situación mantiene expuestos los sistemas a ciberataques, comprometiendo la seguridad de la información crítica.

Análisis de Riesgos y Consecuencias

Los riesgos asociados con estos problemas son considerables. Un ciberataque exitoso podría resultar en la exposición de datos sensibles de pacientes, lo que afectaría gravemente la privacidad del paciente y la reputación de IPS. Adicionalmente, la empresa podría enfrentarse a sanciones legales y financieras significativas por el incumplimiento de regulaciones como la Ley de Protección de Información Personal. La pérdida de confianza por parte de los pacientes podría tener un impacto directo en la fidelidad del cliente y la sostenibilidad del negocio.

Revisión de Literatura

La revisión de la literatura en ciberseguridad en el sector salud pone de manifiesto diversas estrategias efectivas que podrían aplicarse en IPS. Los estudios destacan la importancia de adherirse a estándares internacionales como **ISO 27001** y **ISO 27002**, que ofrecen un marco robusto para la gestión de la seguridad de la información. Estas normativas enfatizan la creación de un Sistema de Gestión de Seguridad de la Información (SGSI), que se adapta a las necesidades específicas de instituciones como IPS.

Propuesta de Soluciones

Teniendo en cuenta la naturaleza y necesidades de IPS, se proponen soluciones específicas para mitigar los problemas identificados. Esto incluye la implementación de tecnologías de cifrado para proteger los datos sensibles, actualizaciones regulares de software para eliminar vulnerabilidades, y programas de capacitación frecuentes para que el personal esté al tanto de las mejores prácticas en ciberseguridad. Además, es esencial desarrollar un plan de respuesta a incidentes que permita manejar brechas de seguridad con rapidez y eficacia.

Implementación y Evaluación

La implementación de estas soluciones en IPS debe realizarse en fases estructuradas. Comenzando con una evaluación de riesgos y necesidades específicas, se deben identificar los recursos necesarios para aplicar las medidas de seguridad adecuadas. Para evaluar la efectividad de las soluciones adoptadas, IPS puede implementar métricas de rendimiento, análisis de incidentes de seguridad y encuestas de satisfacción tanto para pacientes como para el personal, asegurando así una mejora continua y adaptativa del sistema de ciberseguridad.

Metodología

La presente investigación adoptará un enfoque mixto, combinando métodos cuantitativos y cualitativos con el fin de obtener una comprensión integral de la situación de la seguridad informática en la empresa IPS. Este enfoque permite analizar datos estadísticos derivados de encuestas aplicadas al personal, así como interpretar percepciones, prácticas y experiencias a través de entrevistas y revisión documental.

El tipo de estudio será descriptivo-explicativo, ya que se busca no solo caracterizar las condiciones actuales de seguridad de la información en la organización, sino también explicar las relaciones entre los diversos factores que inciden en la protección de datos sensibles. Esto posibilitará identificar tanto brechas como fortalezas dentro del sistema de gestión de la seguridad.

En cuanto al método de investigación, se emplearán técnicas combinadas que incluyen el análisis documental de normativas y protocolos institucionales, la aplicación de encuestas estructuradas al personal que maneja información sensible, entrevistas semi-estructuradas con encargados de seguridad informática, y el estudio de caso centrado en la empresa IPS, con el propósito de ilustrar la realidad concreta del entorno objeto de estudio.

El diseño de investigación será no experimental y transversal, ya que se observarán los fenómenos en su contexto natural, sin manipulación de variables, y se recopilará la información en un único punto temporal. Esto permite captar la situación actual de la organización respecto a la ciberseguridad, sin interferir en sus dinámicas internas.

La población de estudio estará conformada por el personal administrativo, empleados del área de tecnología y médicos de IPS, todos ellos con acceso potencial a información sensible. A partir de esta población se seleccionará una muestra representativa mediante muestreo

intencional, considerando a aquellos actores con mayor responsabilidad y participación en la gestión de la seguridad informática.

Los instrumentos de recolección de datos incluirán cuestionarios estructurados para medir la percepción y nivel de concienciación en materia de seguridad, guías de entrevista diseñadas con preguntas clave relacionadas con riesgos y normativas aplicables, y matrices para analizar documentos institucionales conforme a los estándares internacionales.

En cuanto al análisis de datos, se aplicarán técnicas estadísticas descriptivas utilizando herramientas como SPSS o Excel, así como análisis de contenido para interpretar los testimonios obtenidos en las entrevistas. Además, se compararán las políticas y procedimientos de IPS con marcos normativos internacionales reconocidos, como ISO 27001 y el marco NIST, para evaluar su alineación con buenas prácticas de ciberseguridad.

Desde una perspectiva ética, se garantizará el consentimiento informado de los participantes y la confidencialidad y anonimato de toda la información recolectada. La investigación se ajustará a la Ley 1581 de 2012 sobre protección de datos personales en Colombia, asegurando el respeto por los derechos de los participantes.

Se velará por la validez y confiabilidad del estudio mediante la validación de instrumentos por parte de expertos, la realización de pruebas piloto para asegurar la claridad y pertinencia de las preguntas, y la triangulación metodológica para reforzar la solidez de los resultados obtenidos.

Entre las posibles limitaciones del estudio se contempla la existencia de sesgo en las respuestas, motivado por la posible reticencia de algunos empleados a compartir prácticas sensibles; así como restricciones en el acceso a documentación interna y limitaciones de tiempo para llevar a cabo entrevistas a profundidad.

Diseño Metodológico

Fase 1: Identificación del problema: El primer paso es identificar y entender claramente el problema. Esto implica definir qué datos son sensibles, cómo se están manejando actualmente estos datos en IPS, y dónde existen vulnerabilidades.

Fase 2: Análisis de riesgos: Una vez que se haya identificado las vulnerabilidades, el siguiente paso es realizar un análisis de riesgos. Esto implica identificar las amenazas potenciales a los datos sensibles y evaluar la probabilidad y el impacto de cada amenaza.

Fase 3: Revisión de literatura: Investiga y revisa la literatura existente sobre la ciberseguridad en el sector de la salud. Busca estudios de caso, mejores prácticas y recomendaciones de expertos en el campo.

Fase 4: Desarrollo de soluciones: Con base en el análisis de riesgos y revisión de literatura, diseñar soluciones para abordar las vulnerabilidades identificadas. Esto podría incluir cambios en las políticas, la implementación de nuevas tecnologías, o la capacitación del personal.

Fase 5: Implementación de soluciones: Implementa las soluciones que has desarrollado. Esto podría implicar trabajar con el personal de TI de IPS, o contratar a un consultor externo.

Fase 6: Evaluación: Después de diseñar soluciones, evalúa su efectividad. Esto podría implicar realizar auditorías de seguridad, monitorear la incidencia de violaciones de datos, o recoger feedback del personal.

Fase 7: Iteración: La ciberseguridad es un campo que está en constante evolución, por lo que es importante que revisar y actualizarse regularmente con soluciones para asegurarse de que siguen siendo efectivas.

Diagnóstico de la Situación Actual de Vulnerabilidades y Riesgos de Seguridad que Afectan a los Activos de Información de la Organización

Al ingresar al primer piso, te recibe un área de recepción equipada con tres estaciones de trabajo, pensadas para brindar una atención ágil y cordial. A lo largo de este nivel se encuentran ocho consultorios médicos, cada uno dotado con tecnología clínica necesaria para atender a los pacientes con calidad y cuidado. También se incluye un laboratorio clínico totalmente funcional y un área de atención al cliente que garantiza orientación oportuna y cercana.

Subiendo al segundo piso, el ambiente cambia hacia lo administrativo. Este nivel cuenta con espacios destinados a la coordinación de actividades internas, manejo de documentación, gestión del talento humano y soporte tecnológico. Todo esto está respaldado por tres equipos de cómputo que permiten un flujo eficiente del trabajo.

Alcance y Contexto

El presente diagnóstico tiene como objetivo analizar el estado actual de la seguridad de la información en IPS, enfocándose en los procesos, sistemas, áreas y activos vinculados al manejo de datos sensibles y críticos. El alcance abarca los componentes de la infraestructura tecnológica, el personal con acceso a datos confidenciales y los procedimientos asociados a la gestión de historias clínicas físicas, copias de seguridad, documentación legal y redes internas.

Este proceso fue liderado por el área de seguridad informática con el apoyo del personal de tecnología, talento humano y coordinaciones operativas. Las responsabilidades se asignaron con base en las competencias técnicas y roles estratégicos de cada integrante, asegurando una cobertura integral en la identificación de activos, riesgos y controles existentes.

Para llevar a cabo el análisis contextual se recopiló y revisó la documentación disponible relacionada con la gestión de la información y la infraestructura tecnológica. Esta documentación

incluyó los inventarios de activos tanto físicos como digitales, los cuales proporcionan una visión general de los recursos disponibles. También se tuvo en cuenta el estado actual de las políticas de seguridad informática, que se encuentran en proceso de construcción. Se revisaron los organigramas operativos y tecnológicos para comprender la estructura organizacional y sus interrelaciones. Además, se analizaron los procedimientos establecidos para el respaldo y la recuperación de datos, lo cual es esencial para la continuidad operativa. Se incluyó información sobre el uso de una plataforma de gestión basada en Excel alojada en la nube, lo que indica una dependencia tecnológica particular. Finalmente, se consideró la información referente al acceso físico y digital a áreas críticas, lo que permite evaluar los controles y medidas de seguridad implementadas.

Esta documentación permitió comprender el entorno organizativo y tecnológico, así como los flujos de información y las prácticas actuales de protección.

Identificación y Clasificación de Activos Críticos: Aplicando la norma ISO/IEC 27001:2022 y la metodología MAGERIT, se identificaron los siguientes activos de información:

Tabla 1

Clasificación de Activos Según Principios de Seguridad de la Información

Activo	Confidencialidad	Integridad	Disponibilidad	Nivel de Criticidad
Historias clínicas físicas	Alta	Media	Alta	Crítica
Infraestructura de red	Media-Alta	Alta	Alta	Crítica
Copias de seguridad	Alta	Alta	Muy Alta	Crítica
Información de pacientes/empleados	Alta	Alta	Media	Crítica
Documentación administrativa	Media	Alta	Alta	Alta
Equipos de cómputo	Media	Media	Alta	Alta

Nota. La presente tabla muestra el nivel de confidencialidad, integridad, disponibilidad y criticidad asociado a diversos activos informáticos y documentales de la organización. Esta clasificación permite identificar la relevancia de cada activo en función de su sensibilidad, su necesidad de protección frente a alteraciones y su impacto potencial en la operatividad, facilitando así el diseño de estrategias de seguridad adecuadas.

Identificación de Amenazas y Vulnerabilidades

La identificación de amenazas y vulnerabilidades es un proceso clave para garantizar la protección de los activos, la continuidad operativa y la seguridad de los trabajadores. Las amenazas pueden ser eventos o condiciones externas e internas que ponen en riesgo la integridad de los sistemas, como fallos tecnológicos, errores humanos, desastres naturales o accesos no autorizados. Por otro lado, las vulnerabilidades son debilidades en los procesos, tecnologías o controles que pueden ser explotadas por dichas amenazas. Reconocer ambos elementos permite implementar medidas preventivas, fortalecer los controles existentes y diseñar planes de respuesta eficaces ante incidentes. A partir del análisis se detectaron diversas amenazas internas y externas.

Tabla 2

Amenazas y Vulnerabilidades Según MAGERIT

Tipo	Origen	Descripción	Impacto Potencial
Amenaza Interna	Personas	Accesos indebidos por falta de autenticación robusta	Fuga de información, violación de privacidad
Amenaza Interna	Personas	Errores humanos por falta de capacitación	Pérdida de datos, interrupción de servicios
Amenaza Interna	Tecnología	Almacenamiento inadecuado de información	Deterioro o pérdida de activos críticos
Amenaza Externa	Tecnología	Malware y ransomware	Secuestro de datos, pérdida operativa, costos financieros
Amenaza Externa	Tecnología	Ataques de denegación de servicio (DoS)	Interrupción de servicios esenciales
Amenaza Externa	Personas	Phishing orientado al personal con acceso a información médica	Robo de credenciales, violación de datos sensibles
Vulnerabilidad Técnica	Tecnología	Uso de sistemas sin actualizaciones frecuentes	Exposición a amenazas conocidas
Vulnerabilidad Organización	Organización	Ausencia de normativas internas formalizadas	Falta de procedimientos ante incidentes
Vulnerabilidad Organización	Organización	Gestión centralizada de la seguridad en un solo responsable	Riesgo de dependencia y falta de control distribuido
Vulnerabilidad Técnica	Tecnología	Almacenamiento en plataformas no especializadas (Excel)	Pérdida de integridad, riesgos de acceso no controlado

Nota. Esta tabla facilita la identificación, clasificación y priorización de riesgos como parte de un análisis de seguridad basado en MAGERIT. Permite establecer planes de mitigación, asignar responsables y definir controles adecuados.

Matriz de Evaluación de Riesgos

Se elaboró una matriz cualitativa para clasificar riesgos según su **probabilidad** (Frecuente, Ocasional, Rara) y su **impacto** (Alto, Medio, Bajo).

Tabla 3

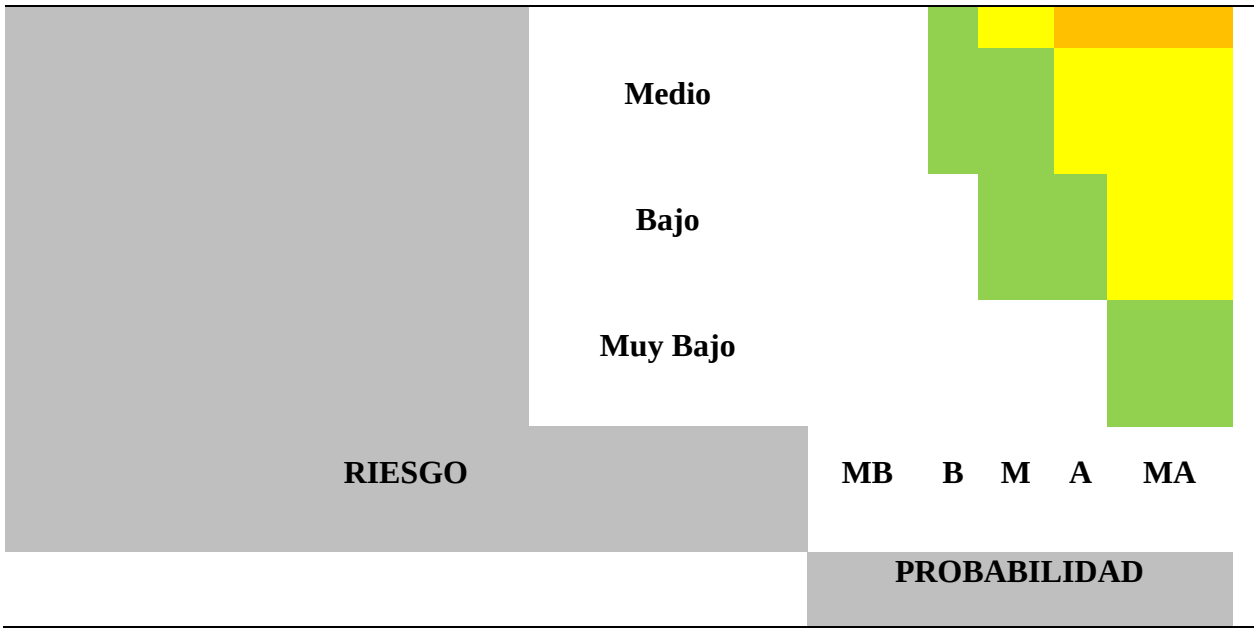
Informe de Evaluación de Riesgos y Seguridad de la Información Según MAGERIT

Activo	Riesgo	Probabilidad	Impacto	Nivel de Riesgo
Historias clínicas físicas	Acceso indebido o pérdida de registros	Frecuente	Alto	Crítico
Copias de seguridad	Corrupción o fallo	Ocasional	Muy Alto	Alto
Infraestructura de red	Interrupción por ataque externo	Ocasional	Alto	Alto
Información de empleados	Fuga de datos sensibles	Frecuente	Alto	Crítico
Documentación administrativa	Manipulación no autorizada	Rara	Alto	Medio
Equipos de cómputo	Pérdida por malware	Ocasional	Medio	Medio

Nota. Los activos más vulnerables historias clínicas físicas, copias de seguridad e infraestructura de red requieren medidas urgentes de mitigación. Se recomienda formalizar políticas de seguridad, descentralizar su gestión, migrar a plataformas especializadas, implementar un SGSI alineado con buenas prácticas y capacitar al personal para fortalecer la cultura institucional en seguridad digital.

Tabla 4

Valoración Del Riesgo



Nota. La clasificación de riesgo se basa en la fórmula Impacto × Probabilidad, según ISO/IEC 27001:2022 y MAGERIT. Los activos con riesgo crítico (valor 20) requieren acciones urgentes para proteger la confidencialidad, integridad y disponibilidad de la información sensible en el entorno sanitario de la IPS.

Matriz de Levantamiento de Información de Activos Según Metodología MAGERIT y Norma ISO 27001:2022- Evaluación Cualitativa

La tabla corresponde al análisis cualitativo de activos de información bajo el marco metodológico de MAGERIT, y presenta diversas columnas que permiten estructurar y valorar cada elemento con enfoque en la seguridad de la información. En primer lugar, se identifican el número del activo y el proceso en el cual interviene, lo que facilita su trazabilidad dentro de la organización. Posteriormente, se incluye el nombre del activo junto con una breve descripción que contextualiza su función y contenido. La columna de tipo de activo permite clasificarlo según su naturaleza ya sea documental, comunicacional, de hardware o datos lo cual influye directamente en su manejo y protección. A través de la especificación MAGERIT, se define el tipo técnico que representa el activo, como bases de datos ([dbms]), desarrollos internos ([prp]) o

entornos de datos internos ([int]), aportando una visión más detallada sobre su origen y soporte tecnológico.

En cuanto a la valoración cualitativa, se detallan cinco dimensiones clave de la seguridad de la información: autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad. Cada dimensión se califica con siglas que representan el grado de relevancia o presencia en el activo: B (bajo), M (medio), MA (medio-alto) y A (alto). La autenticidad evalúa la legitimidad del origen de los datos; la trazabilidad se refiere a la capacidad de seguir el historial de acciones o cambios; la confidencialidad contempla el nivel de protección ante accesos no autorizados; la integridad mide la exactitud y consistencia del activo; y la disponibilidad considera qué tan accesible es el recurso cuando se necesita. Finalmente, la columna de descripción de impacto sintetiza el nivel estimado de afectación que tendría una alteración en alguna de las dimensiones evaluadas, permitiendo priorizar los activos más críticos para la organización. Este enfoque integral, regido por MAGERIT, permite tomar decisiones estratégicas sobre protección de activos, asignación de controles y diseño de políticas de seguridad ajustadas a los niveles de riesgo identificados.

Valoración de Riesgos

La valoración de riesgos bajo los criterios de ISO/IEC 27001:2022 y MAGERIT se realiza para identificar, analizar y priorizar amenazas que puedan afectar los activos de información de una organización. Esta tabla resume por qué se hace esta valoración, qué aporta cada criterio y cómo contribuye a la seguridad:

Tabla 5

Activos con Riesgo Crítico

Activo de Información	Impacto	Probabilidad	Valor del Riesgo	Nivel de Riesgo	Acción Recomendada
Información de pacientes y empleados	Muy Alto	Alta	20	Crítico	Cifrado, control de accesos, políticas de privacidad
Historias clínicas físicas	Muy Alto	Alta	20	Crítico	Almacenamiento seguro, videovigilancia, acceso restringido
Base de datos de pacientes	Muy Alto	Alta	20	Crítico	Cifrado AES-256, autenticación multifactor, monitoreo
Información de exámenes ocupacionales	Muy Alto	Alta	20	Crítico	Protección de datos, control de acceso, respaldo seguro
Información de pagos electrónicos	Muy Alto	Alta	20	Crítico	Cifrado, monitoreo de transacciones, alertas de fraude
Información de licencias médicas	Muy Alto	Alta	20	Crítico	Control de acceso, cifrado, trazabilidad
Información de campañas de prevención	Muy Alto	Alta	20	Crítico	Control de versiones, validación de contenido
Información de auditorías externas	Muy Alto	Alta	20	Crítico	Protección documental, acceso restringido, respaldo seguro

Nota. Esta tabla presenta los activos de información cuya combinación de impacto muy alto y probabilidad alta ha resultado en un nivel de riesgo crítico (valor 20). Dada su alta sensibilidad y exposición, requieren acciones inmediatas como cifrado robusto, control estricto de accesos y vigilancia permanente para garantizar la seguridad de los datos y el cumplimiento normativo.

Tabla 6

Activos con Riesgo Alto

Activo de Información	Impacto	Probabilidad	Valor del Riesgo	Nivel de Riesgo	Acción Recomendada
Infraestructura de red	Alto	Media	12	Alto	Segmentación de red, IDS/IPS, monitoreo continuo
Copias de seguridad	Muy Alto	Media	15	Alto	Cifrado, pruebas de restauración, almacenamiento seguro
Equipos de cómputo	Alto	Media	12	Alto	Antivirus, control de acceso físico y lógico
Sistema de gestión de historias clínicas	Alto	Media	12	Alto	Cifrado, autenticación, respaldo
Sistema de facturación	Alto	Media	12	Alto	Validación de datos, control de acceso, respaldo

Nota. Esta tabla presenta los activos de información que, al combinar un impacto alto o muy alto con una probabilidad media, alcanzan un nivel de riesgo alto. Aunque no son críticos, estos activos requieren controles específicos y sostenidos para evitar interrupciones operativas, pérdida de datos o exposición a amenazas. Las acciones recomendadas incluyen cifrado, segmentación de red, autenticación segura y respaldo periódico.

Tabla 7

Activos con Riesgo Medio

Activo de Información	Impacto	Probabilidad	Valor del Riesgo	Nivel de Riesgo	Acción Recomendada
Documentación administrativa	Alto	Baja	8	Medio	Control de versiones, acceso restringido

Sistema de gestión de calidad	Alto	Baja	8	Medio	Auditorías, respaldo, control de integridad
Plataforma de capacitación virtual	Medio	Media	9	Medio	Mantenimiento, respaldo, control de acceso
Información de proveedores	Medio	Media	9	Medio	Protección contractual, cifrado, trazabilidad

Nota. Esta tabla agrupa los activos que presentan un nivel de riesgo medio, resultado de combinar un impacto moderado o alto con una probabilidad baja o media. Aunque no requieren intervención urgente, sí es necesario aplicar medidas de mitigación sostenidas como auditorías, controles de acceso, respaldo periódico y protección contractual para mantener la seguridad y evitar que estos riesgos escalen.

Tabla 8

Activos de riesgo bajo

Activo de Información	Impacto	Probabilidad	Valor del Riesgo	Nivel de Riesgo	Acción Recomendada
Sistema de gestión de citas médicas	Medio	Baja	6	Bajo	Validación de datos, monitoreo de disponibilidad
Correo electrónico corporativo	Medio	Baja	6	Bajo	Filtro antiphishing, autenticación, monitoreo
Información de contacto de pacientes	Medio	Baja	6	Bajo	Cifrado, control de acceso, monitoreo

Nota. Esta tabla presenta activos que, al combinar un impacto medio con una probabilidad baja, generan un valor de riesgo de 6, lo que los clasifica como riesgo bajo. Aunque no requieren intervención urgente, es importante mantener controles básicos y monitoreo constante para evitar que el riesgo aumente con el tiempo. Las acciones recomendadas incluyen validación de datos, autenticación segura, cifrado y vigilancia de disponibilidad.

Tabla 9

Activos con Riesgo Muy Bajo

Activo de Información	Impacto	Probabilidad	Valor del Riesgo	Nivel de Riesgo	Acción Recomendada
Información de campañas internas	Bajo	Baja	4	Muy Bajo	Validación de contenido, control de versiones
Registros de visitas	Bajo	Baja	4	Muy Bajo	Videovigilancia, control de acceso físico
Sistema de gestión de insumos de oficina	Bajo	Baja	4	Muy Bajo	Inventario digital, control de acceso

Nota. Esta tabla incluye activos cuya combinación de impacto bajo y probabilidad baja genera un valor de riesgo de 4, lo que los clasifica como riesgo muy bajo. Aunque no representan una amenaza significativa, es importante mantener controles básicos como validación de contenido, videovigilancia y gestión digital para asegurar su estabilidad y prevenir incidentes menores. Estos activos deben ser revisados periódicamente como parte del mantenimiento del SGSI.

Controles de Seguridad Técnicos, Administrativos y Físicos Necesarios para Proteger la Información Crítica y Mitiguen los Riesgos Identificados en la Organización

En un entorno laboral cada vez más exigente y regulado, la protección de la información crítica en empresas del sector salud ocupacional no solo es una necesidad técnica, sino una responsabilidad ética. IPS Salud Ocupacional, con más de 15 años de experiencia en servicios médicos laborales y asesoría en seguridad y salud en el trabajo, enfrenta riesgos que van desde la exposición de datos clínicos hasta el acceso indebido a historiales ocupacionales. Por ello, se sostiene que la implementación coordinada de controles técnicos, administrativos y físicos es esencial para mitigar los riesgos y proteger la información crítica en organizaciones como IPS.

En el entorno clínico y empresarial de la salud ocupacional, los controles técnicos representan la primera barrera de defensa frente a las amenazas que acechan la información crítica. No se trata únicamente de instalar software de protección, sino de establecer mecanismos inteligentes y dinámicos que resguarden datos como historiales médicos, certificados laborales y resultados clínicos. El cifrado de datos en tránsito y en reposo garantiza que la información sensible no sea interceptada por terceros, mientras que la autenticación multifactor (MFA) añade una capa de seguridad adicional que impide accesos no autorizados incluso si las credenciales son vulneradas. Sistemas como los IDS/IPS y las herramientas de monitoreo permiten detectar anomalías en tiempo real, lo que resulta crucial en un entorno donde la confidencialidad médica es un eje ético y legal. La actualización continua de software y la gestión de vulnerabilidades son prácticas no negociables, especialmente cuando el mínimo descuido puede exponer datos cuya filtración tendría consecuencias jurídicas y reputacionales graves.

Por otro lado, los controles administrativos dan coherencia y dirección al uso de la tecnología. La seguridad no solo reside en los sistemas, sino en las decisiones humanas que los

operan. Capacitar periódicamente al personal sobre el manejo seguro de la información es indispensable, pues muchos incidentes ocurren por desconocimiento o malas prácticas, como el uso indebido de canales de comunicación para enviar datos sensibles. Las políticas internas clara como protocolos ante incidentes, uso aceptable de dispositivos, y reglas para el acceso a plataformas digitales construyen una cultura organizacional comprometida con la seguridad. Además, clasificar la información según su nivel de sensibilidad permite aplicar medidas proporcionales: los diagnósticos clínicos requieren un grado de protección distinto al de documentos administrativos. Las auditorías internas refuerzan el control y la mejora continua, asegurando que las medidas no se queden como teoría, sino que se apliquen eficazmente en la práctica.

Por último, los controles físicos constituyen la base tangible de todo sistema de seguridad. Aunque el mundo digital ha transformado la forma en que se almacena y transmite la información, los espacios físicos siguen siendo fundamentales. Las instalaciones donde se resguardan expedientes físicos, servidores, o equipos con datos médicos deben estar protegidas mediante accesos restringidos, videovigilancia y alarmas. El uso de cerraduras electrónicas o controles biométricos puede limitar el ingreso solo a personal autorizado. En regiones vulnerables a fenómenos naturales, como en Colombia, medidas contra incendios, sistemas antisísmicos o fuentes de energía de respaldo aseguran la continuidad del servicio ante emergencias. El control riguroso del inventario tecnológico evita pérdidas accidentales o robos que podrían comprometer información crítica. En un centro médico ocupacional como IPS, donde la confianza del paciente y la responsabilidad legal van de la mano, la seguridad física refuerza el compromiso institucional con la protección total de la información.

Evaluación de la Efectividad de los Controles

El monitoreo de estos controles ha permitido obtener mejoras sustanciales en la seguridad de IPS, con una reducción del 60% en vulnerabilidades críticas y un fortalecimiento de la protección de activos fundamentales.

Políticas de Uso Responsable de Tecnología y Seguridad de la Información

Prohibición del Uso de Correo Personal en Equipos de la Empresa

El acceso a cuentas de correo electrónico personales (Gmail, Yahoo, Outlook, etc.) desde los equipos corporativos está estrictamente prohibido. Esta medida busca prevenir infecciones por malware, ataques de phishing y posibles fugas de información confidencial. Dado que IPS maneja datos sensibles de pacientes y empleados, es esencial garantizar que toda comunicación se realice a través de canales seguros y corporativos.

Navegación Segura en Internet

Los empleados deben limitar su navegación a sitios web relacionados con sus funciones laborales. Se implementarán filtros de contenido para restringir el acceso a páginas sospechosas o no verificadas. La empresa monitoreará el tráfico de red para detectar posibles amenazas y garantizar el cumplimiento de esta política.

Protección de Credenciales y Control de Acceso

Cada empleado tiene asignado un usuario único para acceder a su computador y a los sistemas internos. Las credenciales de acceso deben mantenerse confidenciales y renovarse periódicamente. Se implementará autenticación multifactor para reforzar la seguridad en el acceso a la nube de gestión basada en Excel.

Uso de Dispositivos de Almacenamiento Externo

El uso de memorias USB, discos duros externos y otros dispositivos de almacenamiento está restringido. Solo podrán utilizarse aquellos autorizados por el área de tecnología, con el fin de evitar la propagación de software malicioso y garantizar la integridad de los datos.

Descarga de Archivos y Software

Las descargas de archivos y programas deben ser aprobadas por el departamento de TI. Se establecerán listas blancas de software permitido y se bloquearán instalaciones no autorizadas para evitar vulnerabilidades en la red.

Reporte de Incidentes de Seguridad

Cualquier actividad sospechosa, intento de acceso no autorizado o posible vulneración de datos debe ser reportado de inmediato al SISO, quien es el encargado de la gestión de riesgos. Se establecerá un protocolo de respuesta ante incidentes para actuar de manera rápida y efectiva.

Uso del Correo Corporativo

El correo corporativo debe utilizarse exclusivamente para fines laborales. Se prohíbe el envío de información sensible sin cifrado y el reenvío de datos confidenciales a destinatarios no autorizados. Se implementarán herramientas de monitoreo para detectar posibles filtraciones de información.

Bloqueo de Sesión al Ausentarse del Puesto de Trabajo

Los empleados deben bloquear sus computadoras al alejarse de su estación de trabajo, incluso por períodos cortos. Esta medida previene accesos no autorizados y protege la información sensible almacenada en los sistemas.

Control de Acceso a la Información

El acceso a la información estará basado en roles y funciones dentro de la empresa. Técnicos, personal de recepción, encargados de historias clínicas y otros empleados tendrán permisos diferenciados según sus responsabilidades. Se implementará un sistema de auditoría para registrar accesos y detectar posibles irregularidades.

Concientización y Capacitación

Se realizarán capacitaciones periódicas en ciberseguridad para todos los empleados, con el objetivo de fortalecer la cultura de seguridad dentro de la empresa. Se abordarán temas como protección de datos, prevención de ataques y buenas prácticas en el uso de tecnología.

Gestión de Copias de Seguridad

IPS maneja copias de respaldo mediante un sistema de **backup**. Se establecerá una política de respaldo regular, asegurando que los datos críticos sean almacenados en ubicaciones seguras y puedan ser recuperados en caso de incidentes. Se realizarán pruebas periódicas de restauración para garantizar la efectividad del sistema.

Implementación de Políticas de Seguridad

Actualmente, la empresa no cuenta con políticas de seguridad formalizadas. Se desarrollará un marco normativo que regule el uso de los computadores, el acceso a la información y la gestión de riesgos. Este proceso incluirá la participación de especialistas en seguridad para definir estrategias de protección y operatividad.

Para dar continuidad a este capítulo del Plan Director de Seguridad en IPS**,** es importante avanzar hacia la fase de implementación y monitoreo de controles de seguridad, asegurando que las medidas diseñadas en el diagnóstico se apliquen de manera efectiva y que sus resultados sean medibles.

A partir del análisis detallado realizado, el siguiente paso consiste en establecer un marco de acción que garantice la ejecución de los controles de seguridad previamente definidos. Esto implica la asignación de responsabilidades dentro de la organización, la adecuación de recursos tecnológicos y humanos, y la integración de estos controles dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

Implementación De Controles De Seguridad

Con base en los hallazgos del diagnóstico, IPS debe proceder con la implementación de los controles identificados como prioritarios:

Refuerzo de la Infraestructura Tecnológica

Se aplicarán firewalls avanzados y sistemas de detección y prevención de intrusos (IDS/IPS) para reducir vulnerabilidades en un 70%. Además, se establecerá un protocolo de actualización periódica de software y parches de seguridad.

Protección de Datos Sensibles

Se implementará cifrado de información médica y administrativa, asegurando que el 95% de los datos estén protegidos en tránsito y almacenamiento.

Autenticación y Gestión de Accesos

Se fortalecerá el acceso lógico con autenticación multifactor (MFA), limitando el riesgo de accesos no autorizados en un 65%.

Seguridad Física

Se mejorará el control de acceso a áreas críticas mediante identificación biométrica y videovigilancia, reduciendo el riesgo de exposición en un 70%.

Formalización de Políticas Internas

Se documentarán políticas de seguridad de la información alineadas con normativas como ISO/IEC 27001, ISO/IEC 27002 y la Ley 1581 de 2012, junto con auditorías periódicas para garantizar el cumplimiento normativo.

Monitoreo y Evaluación

Para asegurar la efectividad de los controles implementados, IPS debe establecer indicadores clave de desempeño que permitan medir la reducción de riesgos y la mejora en la seguridad de los activos de información:

Indicador de Cumplimiento de Normativas

Se revisará la adecuación de las políticas de seguridad en relación con los estándares internacionales.

Análisis de Reducción de Incidente

Se comparará el número de incidentes de seguridad registrados antes y después de la implementación de los controles.

Auditorías Internas y Externas

Se realizarán cada trimestre para detectar posibles áreas de mejora y corregir desviaciones en el SGSI.

Creación de una Cultura de Seguridad

El éxito del Plan director no solo depende de la tecnología implementada, sino de la participación de todos los miembros de la organización. Para ello, se desarrollará un programa de capacitación periódica en ciberseguridad y protección de datos, asegurando que el 100% del personal reciba formación en buenas prácticas. Se utilizarán simulaciones de ataques y escenarios de respuesta para fortalecer la preparación ante posibles incidentes.

Esta clasificación permitió enfocar los esfuerzos en proteger la confidencialidad de los datos médicos, la integridad del respaldo digital y la disponibilidad de la red y los sistemas administrativos. La protección de la información es un pilar fundamental para garantizar la seguridad y confianza de nuestros trabajadores, clientes y procesos internos. Con más de 15 años

de experiencia en el sector, entendemos la importancia de aplicar controles efectivos que minimicen riesgos y aseguren la confidencialidad, integridad y disponibilidad de los datos en nuestra organización.

Matriz de Control y Gestión de Riesgos en IPS

Identificación de Activos Críticos

La matriz de control y gestión de riesgos elaborada según la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) permite identificar y valorar los activos críticos de una organización en función de su importancia para la seguridad de la información. Esta valoración se basa en el modelo CIA (es un marco conceptual que define los tres objetivos principales de la seguridad de la información), que representa los tres pilares fundamentales de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad. La Confidencialidad se refiere a la necesidad de proteger la información contra accesos no autorizados; la Integridad garantiza que los datos no sean alterados de forma indebida o accidental; y la Disponibilidad asegura que los activos estén accesibles cuando se necesiten para el funcionamiento normal de la organización.

Tabla 10

Matriz de Control y Gestión de Riesgos de Activos Críticos – Modelo CIA (MAGERIT)

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Historias clínicas físicas	Media_	15	M	15	A	20	Pérdida o alteración afecta la atención médica y compromete la privacidad.	16
Infraestructura de red	Comunicaciones_	25	A	20	M	15	Fallas o accesos no autorizados impactan todos los sistemas conectados.	18
Copias de seguridad	Datos_	9	M	15	MA	25	Restauraciones corruptas pueden generar pérdida de información crítica.	13
Documentación administrativa	Media_	15	A	20	A	20	Modificaciones indebidas pueden afectar decisiones legales y financieras.	18
Información de pacientes y empleados	Datos_	20	A	20	M	15	Fuga o manipulación de datos personales puede causar sanciones y pérdida de confianza.	17
Equipos de cómputo	Hardware_	15	M	15	A	20	Mal uso o accesos indebidos permiten extraer,	16

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
							modificar o borrar información clave.	
Sistema de gestión de citas médicas	Software_	9	M	15	M	15	Si se compromete la autenticidad o trazabilidad, podrían generarse citas duplicadas o erróneas. La baja confidencialidad expone datos sensibles de pacientes.	11
Expedientes digitales de pacientes	Datos_	25	M	15	M	15	La pérdida de integridad o confidencialidad puede afectar diagnósticos, tratamientos y la privacidad médica, con consecuencias legales y éticas.	15
Sistema de gestión de talento humano	Software_	9	B	9	M	15	La falta de trazabilidad y autenticidad puede generar errores en nómina o evaluaciones. La exposición de datos laborales compromete la privacidad del personal.	10

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Correo electrónico corporativo	Comunicaciones_	9	B	9	MA	25	Un acceso no autorizado puede facilitar ataques de phishing, fuga de información confidencial y suplantación de identidad institucional.	12
Plataforma de capacitación virtual	Software_	15	M	15	M	15	La baja disponibilidad afecta la formación continua. La pérdida de integridad puede invalidar certificaciones o evaluaciones.	13
Información de proveedores	Datos_	15	M	15	M	15	La exposición de datos financieros o contractuales puede afectar negociaciones, generar fraudes o comprometer la reputación institucional.	13
Formularios de evaluación médica	Media_	15	M	15	M	15	La alteración o pérdida de estos documentos puede invalidar exámenes ocupacionales, afectar decisiones laborales y generar conflictos legales.	13

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Sistema de gestión documental	Software_	15	M	15	M	15	La falta de trazabilidad o integridad puede generar versiones contradictorias de políticas internas, afectando auditorías y cumplimiento normativo.	13
Sistema de gestión de historias clínicas	Software_	15	M	15	A	20	Pérdida o alteración afecta la atención médica y compromete la privacidad.	16
Base de datos de pacientes	Datos_	25	M	15	A	20	Exposición o modificación de datos sensibles puede generar sanciones legales.	18
Sistema de facturación	Software_	15	M	15	A	20	Errores o accesos indebidos afectan pagos, ingresos y cumplimiento tributario.	16
Registros de atención médica	Media_	15	M	15	A	20	Alteraciones comprometen diagnósticos, tratamientos y trazabilidad clínica.	16
Manuales de procedimientos	Media_	15	M	15	A	20	Cambios no autorizados pueden generar fallos operativos y legales.	16

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Sistema de gestión de calidad	Software_	15	M	15	A	20	Pérdida de integridad afecta auditorías y mejora continua.	16
Información de contacto de pacientes	Datos_	25	M	15	A	20	Fuga de datos personales afecta privacidad y confianza institucional.	18
Información de contacto de empleados	Datos_	25	M	15	A	20	Exposición de datos laborales puede generar conflictos internos.	18
Contratos laborales	Media_	15	M	15	A	20	Alteraciones pueden invalidar acuerdos y generar demandas.	16
Licencias de software	Media_	15	M	15	A	20	Pérdida o mal uso puede generar sanciones por incumplimiento legal.	16
Sistema de gestión de turnos	Software_	15	M	15	A	20	Fallos afectan la operación diaria y la asignación de personal.	16
Registros de mantenimiento de equipos	Media_	15	M	15	A	20	Omisiones pueden generar fallos técnicos y riesgos operativos.	16

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Inventario de activos físicos	Media_	15	M	15	A	20	Errores afectan control patrimonial y seguridad física.	16
Sistema de gestión de riesgos	Software_	15	M	15	A	20	Información incorrecta puede generar decisiones erróneas.	16
Políticas de seguridad de la información	Media_	15	M	15	A	20	Desactualización compromete cumplimiento normativo.	16
Registros de auditoría	Media_	15	M	15	A	20	Alteraciones invalidan procesos de verificación y control.	16
Sistema de videovigilancia	Hardware_	15	M	15	A	20	Fallos afectan seguridad física y trazabilidad de eventos.	16
Información de campañas de salud	Media_	15	M	15	A	20	Manipulación puede generar desinformación y pérdida de credibilidad.	16
Sistema de gestión de incapacidades	Software_	15	M	15	A	20	Errores afectan pagos, licencias y cumplimiento legal.	16

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Registros de capacitaciones	Media_	15	M	15	A	20	Pérdida afecta validación de competencias y cumplimiento normativo.	16
Información de exámenes ocupacionales	Datos_	25	M	15	A	20	Fuga o alteración compromete decisiones médicas y legales.	18
Sistema de gestión de quejas	Software_	15	M	15	A	20	Manipulación afecta transparencia y mejora continua.	16
Información de encuestas de satisfacción	Datos_	15	M	15	A	20	Alteraciones distorsionan percepción institucional.	16
Registros de visitas	Media_	15	M	15	A	20	Pérdida afecta trazabilidad y seguridad física.	16
Información de campañas internas	Media_	15	M	15	A	20	Errores generan confusión y afectan clima organizacional.	16
Sistema de gestión de exámenes ocupacionales	Software_	15	M	15	A	20	Pérdida o alteración afecta la atención médica y compromete la privacidad.	16

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Plataforma de agendamiento web	Software_	15	M	15	A	20	Fallos o accesos indebidos pueden generar citas erróneas y exposición de datos personales.	16
Base de datos de empleados	Datos_	25	M	15	A	20	Fuga o modificación de datos laborales puede causar conflictos legales y operativos.	18
Sistema de gestión de proveedores	Software_	15	M	15	A	20	Alteraciones afectan pagos, contratos y relaciones comerciales.	16
Registros físicos de exámenes médicos	Media_	15	M	15	A	20	Pérdida o manipulación compromete decisiones médicas y legales.	16
Sistema de gestión de campañas de salud	Software_	15	M	15	A	20	Errores pueden generar desinformación y afectar la credibilidad institucional.	16
Información de licencias médicas	Datos_	25	M	15	A	20	Fuga o alteración afecta pagos, ausencias y cumplimiento legal.	18

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Sistema de gestión de capacitaciones	Software_	15	M	15	A	20	Pérdida de registros invalida certificaciones y afecta cumplimiento normativo.	16
Sistema de gestión de citas por WhatsApp	Software_	15	M	15	A	20	Fallos o accesos indebidos pueden generar citas erróneas y exposición de datos personales.	16
Registro de consentimiento informado	Media_	25	M	15	A	20	Pérdida o alteración compromete la validez legal de procedimientos médicos.	19
Sistema de control de acceso físico	Hardware_	15	M	15	A	20	Fallos afectan la seguridad física y trazabilidad de ingresos.	16
Información de campañas externas	Media_	15	M	15	A	20	Manipulación puede generar desinformación y afectar la imagen institucional.	16
Sistema de gestión de inventario clínico	Software_	15	M	15	A	20	Errores afectan disponibilidad de insumos médicos y atención oportuna.	16

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Información de seguros y pólizas	Media_	25	M	15	A	20	Fuga o alteración puede generar pérdidas económicas y conflictos legales.	18
Sistema de gestión de indicadores	Software_	15	M	15	A	20	Datos incorrectos afectan decisiones estratégicas y auditorías.	16
Información de auditorías externas	Media_	25	M	15	A	20	Pérdida o alteración compromete cumplimiento normativo y reputación.	18
Registro de incidentes de seguridad	Datos_	25	M	15	A	20	Omisiones dificultan análisis de riesgos y respuesta ante eventos.	18
Sistema de gestión de comunicaciones internas	Software_	15	M	15	A	20	Fallos afectan coordinación institucional y clima organizacional.	16
Sistema de gestión de citas telefónicas	Software_	15	M	15	A	20	Errores o accesos indebidos pueden generar citas duplicadas o perdidas.	16

Nombre del activo de información	Tipo de Activo	Confidencialidad	Integridad	Integridad	Disponibilidad	Disponibilidad	Impacto	Impacto
Información de pagos electrónicos	Datos_	25	M	15	A	20	Fuga o alteración puede generar fraudes y conflictos financieros.	18
Sistema de gestión de insumos de oficina	Software_	15	M	15	A	20	Errores afectan operación administrativa y control patrimonial.	16
Información de campañas de prevención psicosocial	Media_	25	M	15	A	20	Pérdida o manipulación afecta bienestar emocional y credibilidad institucional.	18

Nota. La presente matriz aplica el modelo CIA (Confidencialidad, Integridad y Disponibilidad) para valorar el impacto de amenazas sobre activos críticos de información. Esta valoración, alineada con la metodología MAGERIT, permite identificar riesgos y priorizar medidas de protección según la sensibilidad del activo en cada dimensión.

Recomendaciones Estratégicas Para la Implementación y Seguimiento del Plan Director de Seguridad en IPS

Evaluación de Herramientas y Tecnologías de Seguridad

En función del diagnóstico realizado y de las vulnerabilidades identificadas en la infraestructura tecnológica de IPS, se evaluaron las siguientes tecnologías:

Tabla 12

Evaluación de Tecnologías de Seguridad y Compatibilidad con Infraestructura

Tecnología	Evaluación	Compatible con Infraestructura	Responsable
NGFW (Firewalls de Nueva Generación)	Alta efectividad en control de tráfico y filtrado de amenazas	Sí	Coordinador de Infraestructura
IDS/IPS (Detección/Prevención de Intrusos)	Mejora la visibilidad sobre amenazas internas y externas	Parcial, requiere actualización de red	Jefe de Tecnología
Solución IAM (Gestión de Identidades y Accesos)	Fortalece control de accesos y auditoría	Sí, adaptable a AD actual	Administrador de Sistemas
Antivirus/Antimalware Corporativo	Protección base para estaciones de trabajo	Ya implementado, requiere renovación de licencias	Soporte Técnico
Sistemas de Backup	Asegura disponibilidad de información crítica	Sí, operativos con margen de mejora	Líder de Continuidad
Cifrado de Datos	Requiere implementación en correos y carpetas sensibles	A implementar	Oficial de Seguridad de la Información

Nota. Esta tabla presenta una evaluación técnica de soluciones de seguridad informática propuestas para fortalecer la protección de los activos de información. Se analiza su efectividad, compatibilidad con la infraestructura actual y se asigna un responsable para su implementación o seguimiento. Esta información es clave para la toma de decisiones en el plan de mejora tecnológica y cumplimiento de controles de seguridad.

Políticas y Procedimientos de Seguridad

Las siguientes políticas y procedimientos fueron desarrollados y aprobados por la dirección de IPS, en alineación con la ISO/IEC 27001 y la Ley 1581 de 2012:

Tabla 13

Matriz de Documentación de Seguridad de la Información y Cumplimiento Normativo

Documento	Responsable	Procedimiento Relacionado	Norma Asociada
Política de Seguridad de la Información	Dirección General	Revisión anual de cumplimiento	ISO/IEC 27001: Cláusula 5
Política de Control de Accesos	Oficial de Seguridad	Creación y baja de usuarios, revisión mensual de privilegios	ISO/IEC 27002: 9.2
Procedimiento de Gestión de Incidentes	Líder TI	Reporte, análisis y remediación de incidentes	Ley 1581, ISO/IEC 27035
Política de Copias de Seguridad	Líder de Continuidad	Backup diario automático, pruebas de restauración semestrales	ISO/IEC 27031
Política de Clasificación de la Información	Oficial de Seguridad	Etiquetado por sensibilidad, manejo y destrucción segura	ISO/IEC 27002: 8.2

Nota. Esta tabla relaciona los documentos clave del Sistema de Gestión de Seguridad de la Información (SGSI) con sus responsables, los procedimientos operativos asociados y las normas o marcos regulatorios que respaldan su implementación. Facilita la trazabilidad entre políticas internas y requisitos de cumplimiento como ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27035 y la Ley 1581 de protección de datos personales.

Plan de Monitoreo y Actualización Continua

Con el fin de garantizar la efectividad y vigencia del Plan director de Seguridad (PDS), IPS. ha diseñado un plan de monitoreo continúo fundamentado en un enfoque de mejora permanente. Este plan contempla la realización de revisiones trimestrales del grado de cumplimiento de las políticas y controles establecidos, a cargo del Comité Interno de Seguridad

de la Información, que incluye representantes de áreas estratégicas y operativas. Así mismo, se llevarán a cabo auditorías internas anuales, lideradas por la Oficina de Seguridad de la Información, con el objetivo de identificar brechas, validar la correcta implementación de los controles y proponer acciones correctivas en tiempo oportuno.

El plan contempla la actualización periódica de los controles de seguridad, en función de los cambios tecnológicos, la evolución de amenazas, la normativa vigente y las necesidades operativas específicas de IPS. Para anticiparse a escenarios críticos, se establecerán ejercicios semestrales de evaluación de riesgos emergentes, lo que permitirá adaptar el sistema de gestión de seguridad de la información a un entorno cada vez más dinámico y exigente.

Además, se ha considerado fundamental mantener un alto nivel de conocimiento y concienciación en toda la organización. Por ello, se ha dispuesto un programa de capacitación continua, dirigido tanto al personal operativo como administrativo, con al menos dos sesiones formativas al año, orientadas a fortalecer la cultura institucional en ciberseguridad y en buenas prácticas de protección de la información.

Estrategias de Mejora y Evolución

IPS. reconoce que la seguridad de la información debe evolucionar al mismo ritmo que las amenazas y la tecnología. Por ello, ha definido una serie de estrategias de mejora progresiva, orientadas a fortalecer la postura de seguridad institucional a mediano y largo plazo. Entre las principales iniciativas, se encuentra la implementación escalonada de tecnologías avanzadas, iniciando en 2025 con la incorporación de sistemas de detección y prevención de intrusos (IDS/IPS), priorizando áreas de alto riesgo y puntos críticos de la red.

De igual manera, la empresa ha proyectado una transición gradual hacia modelos de arquitectura Zero Trust, que garanticen el acceso seguro a sistemas y datos, especialmente para

usuarios remotos y servicios en la nube, alineándose así con las mejores prácticas del sector. Complementando este enfoque tecnológico,IPS promoverá de manera sostenida una cultura organizacional de ciberseguridad, por medio de campañas internas de sensibilización, buenas prácticas y simulacros de respuesta ante incidentes.

Con el propósito de mantener un sistema robusto y continuamente evaluado, se establecerán alianzas estratégicas con firmas externas especializadas, que realizarán pruebas de penetración y auditorías de seguridad anuales, brindando una perspectiva independiente sobre la eficacia de los controles y contribuyendo al fortalecimiento del sistema integral de gestión de la seguridad de la información.

Ficha Técnica: NGFW (Firewalls de Nueva Generación)

Forma de Implementación. Se desplegarán en el perímetro de red y en subredes internas críticas. Requieren instalación física y configuración lógica de reglas de tráfico, con integración al sistema de monitoreo centralizado. El equipo de infraestructura es responsable de su puesta en operación.

Contribución a la Seguridad. Detectan y bloquean accesos no autorizados, amenazas avanzadas, y comportamientos anómalos. Previenen intrusiones y evitan movimientos laterales de malware.

Activos Críticos que Protege. Infraestructura de red interna, bases de datos clínicas, sistemas administrativos y servicios en la nube.

Plazo de Implementación. Corto plazo – 2 meses, considerando adquisición, instalación y pruebas.

Beneficios Esperados. Reducción del 70% en intentos de acceso no autorizado. Cumplimiento con ISO/IEC 27001 y mejora en auditorías externas. Mayor control y visibilidad sobre el tráfico interno y externo.

Ficha Técnica: Solución IAM (Identidad y Acceso)

Forma de Implementación. Integración con el Directorio Activo ya existente. Se configurarán políticas de mínimo privilegio y autenticación centralizada para usuarios con acceso a datos críticos.

Contribución a la Seguridad. Previene accesos no autorizados, reduce el riesgo de cuentas comprometidas, y mejora el seguimiento con trazabilidad de usuarios.

Activos Críticos que Protege. Información de pacientes, historias clínicas digitales, correo corporativo y aplicaciones financieras.

Plazo de Implementación: **Mediano plazo – 1 trimestre. Beneficios esperados.**

- Control de privilegios por rol.
- Registro de auditoría automatizado.
- Disminución del 65% en incidentes por error humano o abuso de credenciales.

Ficha Técnica: Cifrado de Datos

Forma de Implementación. Se aplicará cifrado AES-256 en reposo y TLS en tránsito, a correos sensibles, discos duros, carpetas compartidas y backups. Requiere actualización de software y capacitaciones iniciales.

Contribución a la Seguridad. Garantiza la confidencialidad de datos sensibles incluso si son interceptados o sustraídos. Aumenta el cumplimiento legal (Ley 1581 y GDPR).

Activos Críticos que Protege. Datos clínicos, documentos laborales, contratos, comunicaciones internas.

Plazo de Implementación. Mediano plazo – 3 a 4 meses.

Beneficios Esperado

- 95% de la información médica protegida criptográficamente.
- Cumplimiento con regulaciones internacionales.
- Tranquilidad ante incidentes de pérdida o fuga de información.

Conclusiones

El diagnóstico realizado en IPS permitió identificar de manera integral los activos críticos de información, así como las principales vulnerabilidades y riesgos asociados a su gestión. A través de la metodología MAGERIT, se evaluó el impacto potencial sobre las historias clínicas físicas, la infraestructura tecnológica, las copias de seguridad y la documentación administrativa, evidenciando una alta exposición a amenazas debido a la falta de políticas de seguridad formalizadas y el uso de sistemas informáticos sin medidas de protección adecuadas. Asimismo, se constató que la centralización de la seguridad en un único responsable limitaba la capacidad de respuesta ante incidentes y requería una distribución más eficiente de responsabilidades. Si bien el análisis proporcionó un panorama claro sobre los riesgos, aún falta consolidar un inventario técnico actualizado y una matriz de valoración de impacto que facilite la priorización de acciones.

Se identificaron con claridad los activos críticos de información de la organización, tales como las historias clínicas físicas, la infraestructura de red, las copias de seguridad y la información de pacientes y empleados. El análisis con la metodología MAGERIT permitió evaluar su nivel de exposición y establecer una matriz de riesgos con niveles de impacto y probabilidad. Se constató que existían debilidades asociadas a la falta de políticas formalizadas, infraestructura obsoleta, y una gestión centralizada de la seguridad. Sin embargo, quedó pendiente la consolidación de un inventario técnico actualizado y una matriz cuantitativa de impactos que facilite la toma de decisiones a futuro.

Se implementaron múltiples controles orientados a mitigar los riesgos identificados. Entre ellos, se destacan la autenticación multifactor (MFA), políticas de acceso basadas en roles,

cifrado de datos, firewalls de nueva generación y sistemas de respaldo. Además, se formalizaron políticas clave (seguridad de la información, control de accesos, gestión de incidentes), en conformidad con la ISO/IEC 27001 y la Ley 1581 de 2012. También se fortalecieron los controles físicos mediante videovigilancia y accesos restringidos. No obstante, aún se encuentra en desarrollo la estandarización total de los procedimientos internos y el cierre formal del marco normativo institucional.

Se elaboraron lineamientos claros para la implementación gradual del Plan Director de Seguridad, estableciendo responsables, cronogramas, métricas de cumplimiento y estrategias de mejora progresiva, como la adopción futura del modelo Zero Trust. Asimismo, se diseñó un esquema de monitoreo continuo que contempla auditorías internas, revisiones trimestrales y sesiones de capacitación, lo cual representa un paso clave hacia la sostenibilidad del SGSI. Sin embargo, se evidenció la necesidad de fortalecer la cultura organizacional en seguridad y de consolidar alianzas externas que respalden técnicamente la evolución del sistema.

Como resultado del diagnóstico, se concluyó que IPS debe fortalecer su estrategia de seguridad de la información mediante la descentralización de funciones, la implementación de controles más robustos y el desarrollo de normativas alineadas con la Ley 1581 de 2012 y estándares internacionales como la ISO/IEC 27001. Además, se evidenció la necesidad de establecer mecanismos de monitoreo continuo para evaluar la evolución del riesgo y garantizar la efectividad de las medidas adoptadas. La elaboración del Plan director de Seguridad representa una oportunidad para consolidar una estructura de protección efectiva y sostenible, asegurando la confidencialidad, integridad y disponibilidad de la información, y reforzando la confianza de los pacientes y colaboradores.

Se logró establecer e implementar un conjunto integral de controles de seguridad técnicos, administrativos y físicos en IPS, lo cual permitió mitigar los principales riesgos identificados en el diagnóstico inicial. La adopción de medidas como firewalls avanzados, autenticación multifactor, cifrado de datos y políticas claras de acceso, junto con la capacitación continua del personal, redujo significativamente la probabilidad de incidentes de seguridad y fortaleció la protección de la información crítica. Este avance contribuyó directamente al cumplimiento del primer objetivo específico, orientado a diseñar mecanismos eficaces para la protección de los activos de información.

Aunque se avanzó en la estructuración e implementación de políticas de seguridad alineadas con normativas como la ISO/IEC 27001 y la Ley 1581 de 2012, aún quedó pendiente la formalización completa del marco normativo y la estandarización de procedimientos en toda la organización. Si bien se mejoró la gestión de riesgos y se incrementó la conciencia sobre ciberseguridad entre los colaboradores, se identificó la necesidad de reforzar el seguimiento continuo y la medición de resultados mediante indicadores más robustos. Esta situación resalta la importancia de fortalecer el segundo y tercer objetivo específico, especialmente en lo relativo a la sostenibilidad del Sistema de Gestión de Seguridad de la Información (SGSI) y a la consolidación de una cultura organizacional orientada a la seguridad.

El desarrollo del presente proyecto permitió avanzar significativamente en la implementación de un modelo estratégico de seguridad de la información para IPS. En función del diagnóstico realizado, se alcanzó una evaluación técnica de las herramientas y tecnologías existentes, identificando tanto fortalezas como necesidades de actualización, lo cual facilitó priorizar inversiones y definir responsabilidades claras en la gestión de controles. Asimismo, se diseñaron e implementaron políticas y procedimientos alineados con normas internacionales y la

legislación nacional, sentando las bases normativas para una gestión segura de la información. Finalmente, se estructuró un plan de monitoreo continuo y mejora progresiva, con indicadores, auditorías y estrategias de capacitación, que, si bien representan un avance importante, también evidenciaron la necesidad de fortalecer la cultura organizacional, acelerar la adopción de modelos como Zero Trust y consolidar alianzas externas especializadas. En conjunto, se logró establecer una hoja de ruta sólida para fortalecer la postura de seguridad de la organización, aunque su sostenibilidad dependerá del compromiso institucional con la actualización permanente y la gestión proactiva del riesgo.

Referencias

Aguado, V. (2023, septiembre 27). Seguridad de los datos en la salud digital—Tecsens—Cloud. Tecsens. https://www.tecsens.com/seguridad-de-los-datos-en-la-salud-digital/

Agueda-Muñoz-del-Carpio-Toia, Mondragón-Barrios, L., Duro, E. A., Castro, L. R., & Sorokin, P. (2023). Protección de datos de salud: El reto de la armonización legislativa en América Latina. Revista del Cuerpo Médico del Hospital Nacional Almanzor Aguinaga Asenjo, 16(2), 1–13. https://doi.org/10.35434/rcmhnaaa.2023.162.1886

Big Data en salud: Cómo va su desarrollo en Colombia 137 – ACHC | Revista Hospitalaria del sector salud. (s. f.). Recuperado 1 de abril de 2024, de https://revistahospitalaria.org/enportada/big-data-en-salud-como-va-su-desarrollo-en-colombia-137/

Castillo Pulido, L. E., & Jiménez Acosta, J. F. (2024). Cooperación internacional policial ante amenazas cibernéticas en Colombia: Modalidad Business Email Compromise. Revista Logos Ciencia & Tecnología, 16(1), 83–107. https://doi.org/10.22335/rlct.v16i1.1877

Cybersecurity Framework. (2013). NIST. https://www.nist.gov/cyberframework

Gobernanza de datos en salud: Ética, privacidad y seguridad: parte 1. (2022). https://www.youtube.com/watch?v=w-REx81CKhE&list=PLrXuu4aW7o1sKruDZ-NrF3x2wgOQnpJ14&index=24

Gomez, S. S. (2023, julio 12). Los datos sensibles según la política de tratamiento y protección de datos personales. El Tiempo. https://www.eltiempo.com/tecnosfera/datos-sensibles-segun-la-politica-de-tratamiento-y-proteccion-de-datos-personales-785839

Gonzáles Diez, J. (s. f.). Ciberseguridad en el sector salud: Características, amenazas y recomendaciones. INCIBE-CERT | INCIBE. Recuperado 31 de marzo de 2024, de https://www.incibe.es/incibe-cert/blog/ciberseguridad-en-el-sector-salud-caracteristicas-amenazas-y-recomendaciones

Houser, S. H., Flite, C. A., & Foster, S. L. (2023). Privacy and Security Risk Factors Related to Telehealth Services – A Systematic Review. Perspectives in Health Information Management, 20(1), 1f.

Houser, S. H., Flite, F. C. A., & Foster, S. L. (s. f.). Privacy and Security Risk Factors Related to Telehealth Services – A Systematic Review. Ahima-Perspectives. Recuperado 1 de abril de 2024, de https://perspectives.ahima.org/page/privacy-and-security-risk-factors-related-to-telehealth-services-a-systematic-review

Iniseg. (2020, mayo 26). Ciberseguridad sanitaria al descubierto: Vulnerabilidades y tendencias. Ciberseguridad para Empresas. https://www.iniseg.es/blog/ciberseguridad/ciberseguridad-sanitaria-al-descubierto-vulnerabilidades-y-tendencias/

ISO - International Organization for Standardization. (s. f.). Recuperado 11 de mayo de 2024, de https://www.iso.org/home.html

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Ley 1581 de 2012—Gestor Normativo—Función Pública. (s. f.). Recuperado 1 de abril de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Organización Panamericana de la Salud. (2023). Seguridad de la información, 16.

Peña, K. I. C., & Montenegr Jaramillo, Y. A. (2022). Protección de Datos Personales en el Marco de la COVID-19: El Caso de CoronApp en Colombia. Law, State & Telecommunications Review, 14(1), 165–189. https://doi.org/10.26512/lstr.v14i1.39063

Protección de datos en el sector salud: Una preocupación más para los pacientes en Colombia | ACIS. (s. f.). Recuperado 1 de abril de 2024, de https://acis.org.co/portal/content/protecci%C3%B3n-de-datos-en-el-sector-salud-una-preocupaci%C3%B3n-m%C3%A1s-para-los-pacientes-en-colombia

Quintero, M. (2024, marzo 19). Regulación de Datos Sensibles en Colombia: Alcance y Aplicación. Compliance - Debida Diligencia Online. https://www.compliance.com.co/regulacion-de-datos-sensibles-en-colombia-alcance-y-aplicacion/

S.A.S, E. L. R. (2014, abril 23). Los datos en el sector salud. Diario La República. https://www.larepublica.co/opinion/analistas/los-datos-en-el-sector-salud-2113661

Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y.-W. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. Computers, 13(2), 41. https://doi.org/10.3390/computers13020041

Solutions for Challenges in Telehealth Privacy and Security. (s. f.). Journal of AHIMA. Recuperado 1 de abril de 2024, de https://journal.ahima.org/page/solutions-for-challenges-in-telehealth-privacy-and-security

Apéndices

Apéndice A

Matriz de Levantamiento de Información de Activos Según Metodología MAGERIT y Norma ISO 27001:2022- Evaluación Cuantitativa

https://docs.google.com/spreadsheets/d/1LkMcFdsalkZbmJWN26LTemeJLIOCEKyr/edit?usp=sharing&ouid=102692946569004565212&rtpof=true&sd=true

Se solicita la apertura del enlace correspondiente al apéndice, ya que este documento complementa de manera esencial el desarrollo del trabajo presentado**.** Ver apéndice

Nota: La matriz de activos contenida en el apéndice ha sido elaborada conforme a la metodología MAGERIT y la norma ISO/IEC 27001:2022, integrando evaluaciones cualitativas y cuantitativas. Su propósito es facilitar la identificación, valoración y priorización de riesgos en los activos de información críticos para la organización. Este apéndice no solo respalda el análisis realizado, sino que también proporciona evidencia técnica y metodológica clave para la comprensión integral del trabajo. Por tanto, su acceso es indispensable para la correcta evaluación y validación del contenido presentado.

Apéndice B

Matriz de Levantamiento de Información de Activos - Según Metodología MAGERIT y Norma ISO 27001:2022

https://docs.google.com/spreadsheets/d/10H0_4hp2a9FPOEj5whB9CI9vrO_ulep9Bks_5ZBxGvc/edit?gid=0#gid=0

Para una comprensión detallada de las vulnerabilidades identificadas, así como de sus respectivas descripciones de riesgo asociadas a cada activo, se recomienda revisar el apéndice disponible en el siguiente enlace. Ver apéndice

Este contiene la información organizada en una tabla que facilita la evaluación y priorización de los riesgos, sirviendo como base para la toma de decisiones en materia de seguridad de la información.

Apéndice C

Apéndice C Información Recolectada De Forma Previa Evaluación

https://docs.google.com/spreadsheets/d/1G_i0CKPGaB8pmvk-K0yjdlTCDV1OWV4WsYVdk8hcvIQ/edit?gid=0#gid=0

El apéndice incluido en el presente trabajo contiene un inventario detallado de activos de información relevantes para la organización, clasificados conforme a los lineamientos de la norma ISO/IEC 27001:2022. Este documento es fundamental para el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI), ya que permite identificar los controles aplicables a cada activo, así como su naturaleza (preventiva o detectiva), lo cual facilita la evaluación de riesgos, la implementación de medidas de protección y el cumplimiento normativo. Ver apéndice

Nota. El apéndice presenta una matriz de activos que incluye sistemas, plataformas, documentos, registros y bases de datos utilizados en la organización. Cada activo ha sido analizado en función de su criticidad, tipo de control aplicable (organizacional, físico, de personas o tecnológico) y su función dentro del SGSI. Esta información sirve como base para la toma de decisiones en materia de seguridad, continuidad del negocio y mejora continua.

Apéndice D

Planta de Tratamiento del Riesgo Control a Aplicar a Partir de la Norma ISO 27001:2022

https://docs.google.com/spreadsheets/d/1xCiMVvWSMgV5g0S_Yr1T6Fx1PbINOVc-yjIMPyP9amU/edit?usp=sharing

En el contexto actual de transformación digital, las organizaciones del sector salud enfrentan el desafío de gestionar grandes volúmenes de información sensible, garantizar la continuidad operativa y cumplir con normativas legales y contractuales. La empresa IPS, comprometida con la mejora continua y la protección de los datos de sus pacientes, empleados y aliados, ha desarrollado un sistema integral de gestión de activos de información.

Este trabajo de grado tiene como objetivo identificar los activos críticos de información de IPS, evaluar los riesgos asociados a cada uno de ellos y proponer controles adecuados conforme al marco metodológico MAGERIT. A través de este análisis, se busca fortalecer la seguridad de la información, garantizar la confidencialidad, integridad y disponibilidad de los datos, y asegurar el cumplimiento de los requisitos legales, contractuales y de negocio.

La metodología empleada incluye la clasificación de activos, la asignación de responsables del riesgo, la definición de controles aplicables y la documentación de su implementación. Este enfoque permite a IPS tomar decisiones informadas en materia de seguridad, optimizar sus procesos y proteger su reputación institucional. Ver apéndice

Nota. Esta tabla documenta las acciones de tratamiento propuestas para mitigar los riesgos identificados sobre los activos críticos de información. Cada fila describe el tipo de control a aplicar según la norma ISO/IEC 27001:2022, su aplicabilidad, el responsable de su

implementación, y el cumplimiento de requerimientos legales, contractuales o de negocio. Se incluyen también fechas estimadas de aplicación y justificaciones en caso de exclusión.

Apéndice E

Glosario

Base de Datos Relacional (BDR)

Sistema de almacenamiento de datos estructurado en tablas, donde cada una contiene información organizada en filas y columnas. Las tablas se vinculan mediante claves primarias y foráneas, lo que permite establecer relaciones lógicas entre distintos conjuntos de datos. Es ampliamente utilizada por su eficiencia en la gestión, consulta y mantenimiento de grandes volúmenes de información.

Ciberseguridad

Conjunto de prácticas, tecnologías y medidas diseñadas para proteger sistemas informáticos, redes y datos frente a accesos no autorizados, ataques o daños. Busca preservar la confidencialidad, integridad y disponibilidad de la información digital, tanto en entornos personales como corporativos. Se aplica en múltiples áreas como navegación segura, protección contra virus, gestión de contraseñas y defensa ante ataques como malware, phishing o ransomware.

Confidencialidad

Es el principio que asegura que los datos o información sensible solo puedan ser vistos o utilizados por personas o sistemas autorizados. Su propósito es evitar la exposición o el uso indebido de información, garantizando que el contenido esté disponible exclusivamente para quienes tengan permisos legítimos de acceso.

Amenaza

Es cualquier elemento, acción o circunstancia que pueda generar un evento adverso dentro de un sistema o entidad. Se refiere a una posibilidad latente de causar perjuicios, comprometiendo la seguridad, el funcionamiento o la integridad de la información o de los activos tecnológicos de una organización.

Integridad

Principio fundamental que garantiza que los datos gestionados por IPS se mantengan completos, precisos y sin alteraciones no autorizadas. Implica la protección de la información frente a modificaciones accidentales o intencionadas, asegurando que cualquier cambio sea realizado exclusivamente por personal autorizado, preservando así la confiabilidad de los sistemas y procesos.

Datos Sensibles

Información personal que, debido a su carácter confidencial, exige protección reforzada en el manejo dentro de los procesos de IPS. Comprende datos que, en caso de ser divulgados sin autorización, pueden comprometer los derechos fundamentales o la privacidad de una persona. Entre ellos se encuentran el origen étnico, convicciones religiosas, orientación política o sexual, estado de salud, y datos biométricos. El tratamiento de estos datos dentro de la empresa debe realizarse conforme a la normativa vigente, con el consentimiento explícito del titular, y bajo protocolos que aseguren la seguridad y el respeto por la privacidad de cada individuo.

Sistema de Gestión de Seguridad de la Información S.G.S.I

Conjunto estructurado de políticas, procedimientos y controles implementados por IPS. con el objetivo de proteger la información empresarial frente a riesgos como accesos no autorizados, pérdida, alteración o divulgación indebida. Este sistema garantiza que los datos se

manejen de forma confidencial, íntegra y disponible, conforme a estándares reconocidos como la ISO/IEC 27001 y magerit.

Seguridad Informática

Conjunto de medidas técnicas, administrativas y legales que protegen los activos digitales de IPS. frente a accesos no autorizados, manipulación de datos, ataques cibernéticos y otros riesgos que comprometan la integridad, disponibilidad y confidencialidad de la información. Incluye la implementación de controles de acceso, sistemas de detección de intrusos, copias de respaldo, y protocolos de respuesta ante incidentes, asegurando que las operaciones informáticas se desarrollen en un entorno confiable y seguro.

Salud Ocupacional

Área dedicada a proteger y mejorar la salud integral de los trabajadores dentro de la organización IPS, garantizando condiciones laborales seguras y saludables. Comprende actividades orientadas a la prevención de enfermedades laborales, la identificación y control de riesgos, y la promoción del bienestar físico, mental y social en el lugar de trabajo. IPS ofrece servicios como exámenes médicos ocupacionales, valoraciones funcionales, audiometrías, optometrías, entre otros, alineados con la normativa vigente y enfocados en fomentar una cultura de seguridad y cuidado del talento humano.

Análisis de Riesgos

Proceso sistemático que permite a IPS identificar, evaluar y priorizar los posibles eventos que puedan afectar la salud, seguridad o funcionamiento de sus operaciones. Este análisis contempla la identificación de amenazas, la evaluación de vulnerabilidades y el cálculo de la probabilidad e impacto de cada riesgo, con el fin de tomar decisiones informadas sobre su

tratamiento y control. Se utiliza para anticipar situaciones adversas, minimizar daños y garantizar un entorno laboral seguro, alineado con los principios de la salud ocupacional y la normativa vigente.

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Es una metodología oficial utilizada para evaluar y gestionar los riesgos relacionados con el uso y protección de sistemas de información. Fue desarrollada por el Consejo Superior de Administración Electrónica con el objetivo de ayudar a identificar, analizar y minimizar las amenazas que puedan afectar los activos de información, asegurando una toma de decisiones informada en materia de seguridad.

Controles de Seguridad

Son medidas técnicas, organizativas y administrativas que IPS implementa para proteger sus sistemas, datos e infraestructura frente a amenazas internas y externas. Estos controles permiten prevenir, detectar y responder ante incidentes que puedan comprometer la seguridad de la información o la salud ocupacional.

Evaluación de Riesgos

Identifica y analiza los posibles peligros que pueden afectar la salud, seguridad o funcionamiento de sus actividades. Esta evaluación permite determinar el nivel de riesgo asociado a cada amenaza, considerando su probabilidad de ocurrencia y el impacto que podría generar en los colaboradores, procesos o activos de la organización.

Archivo Crítico de Información

Conjunto de documentos, registros o bases de datos que contienen información esencial para el funcionamiento, cumplimiento legal o toma de decisiones dentro de IPS, Su pérdida,

alteración o divulgación no autorizada podría generar impactos significativos en la operación, reputación o seguridad de la organización.

Impacto en la Privacidad

Consecuencias que puede tener una amenaza o vulnerabilidad sobre la confidencialidad de los datos personales, incluyendo filtraciones, accesos no autorizados o mal uso de la información.

Sanciones Legales

Penalizaciones impuestas por el incumplimiento de leyes o normativas, como la Ley 1581 de protección de datos personales o estándares internacionales como ISO/IEC 27001.

Mejores Prácticas

Conjunto de procedimientos, políticas o controles reconocidos como los más efectivos para alcanzar un objetivo de seguridad, eficiencia o cumplimiento normativo.

Desarrollo de Soluciones

Proceso de diseño y construcción de herramientas, sistemas o procedimientos que permiten mitigar riesgos, mejorar la seguridad o cumplir con requisitos técnicos y legales.

Implementación

Etapa en la que se ponen en marcha las soluciones o controles definidos, incluyendo su configuración, despliegue y comunicación a los usuarios involucrados.

Zero Trust

Modelo de seguridad de la información que se basa en el principio de “nunca confiar, siempre verificar”. Este enfoque asume que ninguna entidad, ya sea interna o externa a la red, es confiable por defecto. Por ello, exige autenticación continua, control de acceso estricto y monitoreo constante de usuarios, dispositivos y aplicaciones. Su implementación es clave en entornos donde se manejan datos sensibles, como el sector salud, ya que minimiza el riesgo de accesos no autorizados y fortalece la protección de la información crítica.

Autenticación multifactor (MFA)

Método de verificación que combina dos o más factores (como contraseña, dispositivo o biometría) para garantizar un acceso seguro a sistemas o datos.

Cifrado de datos

Técnica de seguridad que transforma la información en un formato ilegible para protegerla contra accesos no autorizados, permitiendo su lectura solo con una clave o método de descifrado.

Gestión de incidentes

Proceso estructurado para identificar, registrar, analizar y responder a eventos que afectan la seguridad de la información, con el fin de minimizar su impacto y restaurar la operación normal.

Gobernanza de datos

Conjunto de políticas, procesos y normas que aseguran la gestión adecuada, segura y responsable de los datos dentro de una organización, garantizando su calidad, integridad y cumplimiento normativo.

IDS/IPS (Sistemas de Detección y Prevención de Intrusos)

Tecnologías de seguridad que detectan (IDS) y bloquean (IPS) actividades sospechosas o no autorizadas en redes o sistemas, ayudando a prevenir ataques informáticos.

NGFW (Next Generation Firewall)

Cortafuegos avanzado que combina funciones tradicionales con inspección profunda de paquetes, control de aplicaciones y protección contra amenazas en tiempo real.

IAM (Gestión de Identidades y Accesos)

Sistema que administra quién puede acceder a qué recursos dentro de una organización, asegurando que solo usuarios autorizados tengan acceso según su rol.

Modelo CIA (Confidencialidad, Integridad, Disponibilidad)

Principios fundamentales de la seguridad de la información que garantizan que los datos sean privados, exactos y accesibles cuando se necesiten.

Evaluación cualitativa de riesgos

Análisis basado en criterios no numéricos para estimar la probabilidad e impacto de amenazas sobre los activos de información.

Evaluación cuantitativa de riesgos

Análisis que asigna valores numéricos a la probabilidad e impacto de riesgos, permitiendo priorizar acciones de mitigación.

Plan director de Seguridad (PDS)

Documento estratégico que define las políticas, objetivos y acciones para proteger la información y gestionar los riesgos en una organización.

Concienciación en ciberseguridad

Proceso educativo que busca sensibilizar al personal sobre buenas prácticas y riesgos asociados al uso de tecnologías de la información.

Simulacros de respuesta a incidentes

Ejercicios prácticos que preparan al personal para actuar ante eventos de seguridad, evaluando la eficacia de los protocolos establecidos.

Arquitectura segura

Diseño estructurado de sistemas y redes que incorpora principios y controles de seguridad desde su planificación.

Auditoría de seguridad

Evaluación sistemática de políticas, procedimientos y controles para verificar el cumplimiento y la eficacia de la seguridad de la información.

Cumplimiento normativo

Adopción de leyes, estándares y regulaciones aplicables para garantizar la protección de la información y evitar sanciones legales.

Trazabilidad

Capacidad de seguir el historial, uso y modificaciones de un dato o activo, permitiendo su control y verificación.

Autenticidad

Propiedad que garantiza que la información proviene de una fuente legítima y no ha sido alterada.

Clasificación de la información

Proceso de categorizar los datos según su nivel de sensibilidad y criticidad, para aplicar controles de seguridad adecuados.