Implementación de un plan director de seguridad para la protección de activos críticos de información en infraestructuras de salud

Dana Ximena Ayure Fula

Julio Cesar López Diaz

Asesor

Edgar Roberto Dulce Villarreal

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Agradecimientos

Agradezco a Dios por permitirme estar con vida, tener buena salud para seguir con el aprendizaje y plasmar los conocimientos adquiridos.

Agradezco a mi Familia y personas que siempre han estado presentes en los momentos más difíciles durante este proceso de aprendizaje.

Agradezco a los Tutores (Ingenieros), que se han esforzado por compartir su conocimiento y poder llevar a cabo este proceso de aprendizaje, a mis compañeros y la Universidad UNAD por darme apoyo para culminar esta Especialización.

Agradezco a la IPS por confiar en mi trabajo, permitirme realizar este proyecto, hacer estudios de posibles alteraciones, amenazas informáticas, poder intervenir en los hallazgos encontrados, buscar soluciones como la implementación de un sistema de seguridad de la Información, para ayudar en los procesos de mejora y seguridad en la empresa porque requiere manejar datos confidenciales y manejo de seguridad óptimo.

Agradezco a la vida y a todos los que me acompañaron en este proceso de aprendizaje.

Dedicatoria

Dedico este trabajo a Dios, por permitirme continuar con los procesos de conocimiento y crecimiento intelectual, por culminar mis estudios satisfactoriamente, a mi esposa Alexandra Cruz, mis Hijas Katherin López y Nataly López, mi familia, pilares de apoyo en cada paso de los procesos profesionales para ser siempre mejor persona e Ingeniero de sistemas, especialista en seguridad informática. Este logro, que con ayuda de ellos he podido llegar a culminar, es un paso más de los futuros logros por conseguir.

Resumen

La IPS es una institución prestadora de servicios en salud ocupacional con 18 años de experiencia legalmente constituida, con habilitaciones por los entes calificadores de Boyacá, institución privada, ubicada en Tunja (Boyacá), dentro de su actividad económica manejan atención de consultas médicas aproximadamente 100 pacientes diarios, de empresas como de usuarios particulares de todo el país. Hace 18 años el manejo de historias clínicas se manejaban en físico ,poca información se manejaba en medios magnéticos o archivos digitalizados ,en el año 2013 adquieren un software donde empiezan a manejar archivos digitales de las historias clínicas y manejo contable, siendo toda esta información base fundamental para su desarrollo económico y legal , realizando ocasionalmente alguna copia de seguridad en memorias externas, en el año 2020 por la ley 2015 donde regula la interoperabilidad integral de la historia clínica electrónica y digital, la Institución busca manejar un proceso de seguridad para la información ,viendo que la vulnerabilidad y los ataques informáticos pueden ser más accesible a los datos sensibles, empiezan a realizar copias de seguridad en memorias externas diariamente.

En Tunja, Boyacá, el aumento de ataques dirigidos a clínicas privadas ha generado una necesidad urgente de implementar sistemas de gestión de seguridad de la información (SGSI), y llegar como estudiante a la institución se empieza a identificar riesgos, falencias y vulnerabilidad en la IPS con los datos sensibles, haciendo estudios para fortalecer y proteger sus activos críticos de información.

Palabras clave: Análisis de Riesgos, Ciberseguridad, Controles de Seguridad, Datos Sensibles, Políticas de Seguridad, Salud Ocupacional, SGSI (Sistema de Gestión de Seguridad de la Información).

Abstract

This research analyzes the vulnerabilities of sensitive data managed within the health information systems of the company IPS. in Tunja, Boyacá. The study focuses on the challenges related to data privacy and security in the provision of healthcare services, highlighting the risks that arise from inadequate protection mechanisms. A qualitative approach was applied through document review and case analysis, identifying critical gaps in information management practices. The findings reveal the urgent need for robust security measures to safeguard patient data, ensure regulatory compliance, and strengthen trust in digital health systems. This work emphasizes the importance of implementing effective data protection strategies and establishes a framework that may guide healthcare organizations in mitigating vulnerabilities and enhancing information security.

Keywords: Risk Analysis, Cybersecurity, Security Controls, Sensitive Data, Security Policies, Occupational Health, ISMS (Information SecuriGGty Management System).

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista Apéndice

Glosario

Activo de Información: Recurso físico, lógico, documental o humano que tiene valor para la organización y requiere protección. Incluye historias clínicas, bases de datos, infraestructura de red, correos, servidores y respaldos.

Amenaza: Evento interno o externo con potencial de causar daño a los activos de información, como ataques informáticos, errores humanos, fallas tecnológicas o accesos no autorizados.

Análisis de Riesgos: Proceso sistemático para identificar, valorar y priorizar amenazas y vulnerabilidades que pueden comprometer la seguridad de los activos de información. En este trabajo se emplean principios de ISO/IEC 27005 y MAGERIT.

Autenticación Multifactor (MFA): Mecanismo de verificación que combina dos o más factores (contraseña, token, biometría) para reforzar la seguridad del acceso a sistemas y aplicaciones.

Backup (Copia de Seguridad): Proceso de duplicación y resguardo de información crítica con el fin de garantizar su recuperación en caso de incidentes como fallas, ransomware o borrado accidental.

Ciberataque: Intento malicioso de comprometer sistemas, redes o información mediante técnicas como malware, phishing, ransomware, ingeniería social o explotación de vulnerabilidades.

Ciberseguridad: Conjunto de medidas técnicas, administrativas y humanas orientadas a proteger sistemas y datos frente a ataques, accesos indebidos y amenazas digitales.

Ciberseguridad en Salud: Rama especializada de la seguridad informática que protege datos clínicos, registros médicos, dispositivos médicos electrónicos y sistemas hospitalarios que manejan información sensible.

Cifrado: Técnica que transforma la información mediante algoritmos (como AES256) para evitar que sea legible por usuarios no autorizados.

CIA (Confidentiality, Integrity, Availability): Modelo fundamental de la seguridad de la información:

Confidencialidad: acceso solo por personal autorizado.

Integridad: información completa y no alterada.

Disponibilidad: acceso oportuno a los datos cuando se requieren.

Control de Acceso: Conjunto de mecanismos que regulan quién puede ver, usar, modificar o eliminar un recurso, basado en criterios de autenticación, roles y privilegios mínimos.

Control de Seguridad: Medida técnica (software, firewall), administrativa (políticas) o física (acceso restringido) diseñada para reducir riesgos en los activos de información.

Datos Personales: Información que permite identificar a una persona. En salud ocupacional incluye nombres, documentos, firmas, historias ocupacionales, diagnósticos, resultados de laboratorio y registros clínicos.

Datos Sensibles: Categoría especial de datos cuyo tratamiento requiere protección reforzada. Incluye información médica, biométrica, diagnósticos, incapacidades, resultados de exámenes y datos de salud.

Disponibilidad: Capacidad de acceder a la información y los sistemas cuando se necesitan, evitando interrupciones mediante redundancia, respaldos y continuidad operativa.

Endpoint Security (Seguridad de Endpoints): Conjunto de políticas, herramientas y controles para proteger dispositivos finales como computadores, tablets o equipos médicos frente a amenazas.

Firewall / NGFW: Dispositivo o software que controla el tráfico de red para bloquear accesos indebidos y detectar amenazas. Los Next Generation Firewalls agregan análisis profundo, IDS/IPS y filtrado avanzado.

Gestión de Identidades (IAM): Sistema que administra usuarios, roles, permisos y autenticación centralizada, garantizando el principio de mínimo privilegio.

Gestión de Incidentes: Proceso para detectar, analizar, contener, erradicar y recuperar ante eventos que afectan la seguridad de la información. Se apoya en la norma ISO/IEC 27035.

Gestión de Riesgos: Metodología para valorar riesgos según probabilidad e impacto, permitiendo priorizar acciones de mitigación. En este trabajo se usa clasificación cualitativa y matrices MAGERIT.

Hardening (Endurecimiento de Sistemas): Proceso de reducir la superficie de ataque eliminando servicios innecesarios, reforzando configuraciones, aplicando parches y estableciendo políticas de seguridad estrictas.

Historia Clínica Electrónica (HCE): Documento digital que contiene datos sensibles del paciente, cuyo manejo debe garantizar estrictamente la confidencialidad, integridad y disponibilidad.

Indicador de Seguridad (KPI): Medida cuantitativa que permite evaluar la efectividad de políticas, controles y procedimientos implementados en el SGSI.

Ingeniería Social: Técnica de manipulación psicológica usada para obtener acceso a datos o sistemas mediante engaño. Incluye phishing, suplantación y fraude a usuarios.

Integridad: Propiedad que asegura que la información es exacta, confiable y no ha sido modificada sin autorización.

Internet seguro: uso de red de forma que se protejan datos, en dispositivos y privacidad de amenazas como el robo de identidad, el malware y el fraude, mediante el uso de protocolos (HTTPS con candado), contraseñas fuertes, software de seguridad (antivirus, firewall), configuración de privacidad y hábitos de navegación responsables, como no abrir enlaces sospechosos y verificar fuentes, protegiendo la seguridad informática.

IPS (Institución Prestadora de Salud): Entidad del sector salud encargada de prestar servicios médicos. Maneja grandes volúmenes de datos sensibles, por lo que requiere controles robustos de seguridad.

ISO/IEC 27001: Norma internacional para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en riesgos.

ISO/IEC 27032: Norma de referencia para la ciberseguridad colaborativa, orientada a la gestión de amenazas digitales, protección de datos e interacción segura entre usuarios y sistemas.

ISO/IEC 27799: Norma complementaria a ISO 27001 que define controles específicos de seguridad para el sector salud.

Logs: Registros generados por sistemas, aplicaciones y redes que documentan eventos relevantes para auditoría y seguridad.

MAGERIT: Metodología española para el análisis y gestión de riesgos de seguridad en sistemas de información, ampliamente usada en instituciones públicas y privadas.

Malware: Software malicioso diseñado para infectar sistemas, interceptar información o bloquear equipos (ransomware, troyanos, spyware).

Modelo NIST CSF: Marco del Instituto Nacional de Estándares y Tecnología (NIST) basado en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar, útil para mejorar la postura de ciberseguridad.

Phishing: Estrategia fraudulenta donde el atacante suplanta entidades legítimas para obtener contraseñas, datos personales o acceso a sistemas.

Plan Director de Seguridad: Documento estratégico que define políticas, controles, objetivos, responsables e indicadores para gestionar la seguridad de la información en la organización.

Política de Seguridad de la Información: Regla formal que establece directrices, responsabilidades y buenas prácticas para proteger la información de la organización.

RBAC (Role-Based Access Control): Modelo de autorización basado en roles que otorga permisos según funciones específicas dentro de la organización.

Respaldo y Recuperación (Backup & Restore): Prácticas orientadas a garantizar que la información pueda recuperarse en caso de pérdida, corrupción o ataque.

Riesgo Informático: Resultado de la combinación entre una amenaza, una vulnerabilidad y su impacto potencial sobre un activo.

SIEM (Security Information and Event Management): Sistema que centraliza, correlaciona y analiza registros (logs) en tiempo real para detectar anomalías y posibles incidentes de seguridad.

Sistema de Gestión de Seguridad de la Información (SGSI): Marco de trabajo estructurado para gestionar políticas, procedimientos, controles, riesgos e indicadores de seguridad en cumplimiento con ISO 27001.

Tokenización: Proceso que reemplaza datos sensibles con valores sustitutos (tokens) sin significado fuera del sistema, reduciendo su exposición.

Trazabilidad: Capacidad de registrar y auditar acciones realizadas por usuarios o sistemas, permitiendo reconstruir eventos ante incidentes.

Vulnerabilidad: Debilidad técnica, humana o procedimental que puede ser explotada por una amenaza para comprometer la seguridad de un activo.

Zero Trust (Modelo de Confianza Cero): Arquitectura de seguridad basada en el principio de “nunca confiar, siempre verificar”, donde cada solicitud de acceso debe autenticarse y autorizarse continuamente.

Introducción

Las instituciones médicas deben mantener y mejorar la salud de la población, estas deben proporcionar atención integral (promoción, prevención, tratamiento, rehabilitación de manera oportuna segura eficiente y equitativa debe minimizar riesgos y buscar resultados óptimos a través de innovación y mejora continua.

Una de las obligaciones que las rige por normativa legal según la ley 2015 del 2020 , resolución 839 del 2017,ley 1581 de 2012 ,establecen que las ips deben asegurar la guarda, custodia, integridad y acceso seguro de estos documentos por un mínimo de 20 años ,garantizando la privacidad y la reserva de la información, las instituciones que no cumplen con las normas pueden ingerir en efectos legales y mala reputación de las instituciones, siendo datos fundamentales en el pilar de una institución prestadora de servicios de Salud.

Hacia los últimos 5 años se ha evidenciado que las persona con grandes conocimientos de informática se dedican a hacer inclusiones de seguridad en sistemas informáticos para hacer estafas o daños que generen ganancias económicas o ciberataques y en las instituciones de salud en el último año se han incrementado en un 78%,es el caso que se reportó en Diciembre del año 2022 con la EPS sanitas, parte del grupo Keralty quien sufrió un grave ciberataque de ransomware que paralizó los sistemas digitales afectando millones de usuarios, impidiendo citas accesos a servicios, robos de datos personales de pacientes y empleados, así como muchas más instituciones de sector salud.

Estos ciberataques generaron que se empezaran a llevar solicitudes a defensoría del pueblo y super salud evidenciando que muchos hospitales e instituciones de salud no cuentan con un plan integral de seguridad informática.

En este contexto, la IPS de salud, ubicada en Tunja, atiende diariamente aproximadamente cien pacientes, ve la necesidad de mejorar o implementar seguridad informática ya que se enfrenta a desafíos derivados de nuevas amenazas cibernéticas y la ausencia de protocolos robustos genera vulnerabilidad y pone en riesgo la confidencialidad, integridad y disponibilidad de la información.

El manejo inadecuado de los datos sensibles en salud puede acarrear sanciones legales significativas, en concordancia con la normatividad vigente (Ley 1581 de 2012; Decreto 1377 de 2013). Por estas razones, resulta urgente identificar los riesgos y diseñar estrategias en este trabajo mitigación, prevención e implementación de un Plan Director de Seguridad Informática para la IPS, buscando establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que garantice la protección de los datos.

Planteamiento del Problema

Se presenta una pregunta a raíz de la investigación realizada teniendo en cuenta el mayor problema encontrado en la institución.

¿Cómo puede implementarse un Plan Director de Seguridad para la infraestructura de una IPS, que permita proteger los activos de información críticos relacionados con la historia clínica de los pacientes y garantizar el cumplimiento del marco ISO 27032: 2023.?

Después de plantear la pregunta evidenciamos que la institución de salud maneja diariamente información sensible de aproximadamente 100 pacientes ,procediendo a realizar un diagnóstico inicial (agosto 2025) que reveló la ausencia de controles técnicos y administrativos alineados con estándares internacionales como la norma ISO/IEC 27032, exponiendo a la organización a riesgos de fuga de datos, ransomware y sanciones por incumplimiento de la Ley 1581 de 2012 (Superintendencia de Industria y Comercio [SIC], 2021).

Es por eso que el análisis principal hace que se programe para la IPS sea una propuesta técnica que diseñe e implemente controles específicos, medibles y sostenibles, alineados con buenas prácticas internacionales (Superintendencia de Industria y Comercio, 2021).

Justificación

La protección de los datos sensibles en las instituciones prestadoras de servicios de salud, son muy importantes (historias clínicas, diagnósticos, datos personales) la confidencialidad, integridad y disponibilidad de datos, estas se ven expuestas a riesgos cibernéticos que pueden afectar credibilidad, calidad del servicio, consecuencias legales, reputacionales y económicas. Implementar un Plan Director de Seguridad alineado con el estándar ISO 27032:2023, la Ley 1581 de 2012, que exige adoptar "medidas de seguridad razonables" para datos sensibles es uno de los principales objetivos teniendo en cuenta , la Sentencia T-260 de 2021 de la Corte Constitucional que reafirma este derecho en el ámbito sanitario, la norma ISO/IEC 27032 (2012) proporciona un marco para la ciberseguridad colaborativa, permitirá establecer una hoja de ruta clara garantizando la confianza de usuarios, personal médico y entes reguladores para la salvaguarda de la información, fortaleciendo la infraestructura tecnológica y el cumplimiento normativo contribuyendo a la consolidación de mejores prácticas de ciberseguridad en el sector salud.

La realización de este trabajo de investigación sobre la implementación de un plan director de seguridad para la protección de activos críticos de información en infraestructuras de salud se sustenta en la creciente importancia que la ciberseguridad ha adquirido en el sector, donde la protección de la información clínica y administrativa constituye un eje fundamental para la prestación segura de los servicios médicos.

En el contexto nacional, la Ley 1581 de 2012 y el Decreto 1377 de 2013 obligan a las entidades del sector salud a garantizar medidas técnicas, administrativas y humanas adecuadas para la protección de los datos personales, especialmente aquellos clasificados como sensibles, la Sentencia T-260 de 2021 de la Corte Constitucional reafirma el deber de las IPS de implementar

medidas de seguridad que protejan los derechos fundamentales de los pacientes, lo que convierte la seguridad de la información en un compromiso legal, ético y social.

Desde una perspectiva técnica, este trabajo se enmarca en los lineamientos de las normas ISO/IEC 27032 (Ciberseguridad) e ISO 27799 (Seguridad de la Información en Salud), que orientan la gestión integral de los riesgos y la implementación de controles para asegurar la confidencialidad, integridad y disponibilidad de los datos clínicos. Estas normas no solo establecen los requisitos técnicos para la gestión de seguridad, sino que también promueven la formación continua del personal, la evaluación de amenazas emergentes y la adopción de prácticas de mejora continua.

El sector salud es actualmente uno de los más vulnerables ante ciberataques, informes de McAfee (2024) y de la Agencia de Ciberseguridad de la Unión Europea (ENISA) destacan que los incidentes de ransomware en instituciones sanitarias aumentaron más del 50 % en el último año, situando a los datos clínicos como uno de los activos más valiosos para los ciberdelincuentes. Es por esto por lo que la IPS necesita generar seguridad para evitar riesgos técnicos, evitar pérdidas financieras, sanciones legales y deterioro de la confianza institucional. De ahí que este estudio busque no solo identificar las debilidades actuales del sistema de seguridad de la información, sino también proponer e implementar un plan director de seguridad para la protección de activos críticos de información en infraestructuras de salud que sirva como base para la consolidación de un Sistema de Gestión de Seguridad de la Información (SGSI) sostenible y alineado con las normas internacionales.

Con este proyecto se contribuye a fortalecer la cultura organizacional de seguridad digital de la IPS, mediante la capacitación ,educación continua , sensibilización, toma de conciencia, conocimiento, difusión, información, comprensión y promoción del personal de la

organización ya que la seguridad informática no depende únicamente de la infraestructura tecnológica, sino también de las conductas y hábitos del recurso humano, previniendo incidentes derivados del de errores humanos o desconocimiento de políticas institucionales.

Finalmente, esta implementación no solo pretende resolver una necesidad inmediata, sino establecer un modelo estratégico de ciberseguridad adaptable y sostenible , y mejorar los procesos de gestión de información, garantizar la continuidad operativa y proyectar a la organización como un referente en buenas prácticas de protección de datos que permita a la IPS evolucionar dentro de un entorno digital en constante cambio y que los resultados de este trabajo puedan servir como base para futuras iniciativas de fortalecimiento tecnológico y de cumplimiento normativo tanto en la IPS como en otras instituciones del país que buscan consolidar su resiliencia digital.

Objetivos

Objetivo General

Implementar el Plan Director de Seguridad en una IPS para fortalecer las políticas, procedimientos y controles, así como evaluar su efectividad mediante indicadores de desempeño que garanticen la protección de los activos críticos de información y la continuidad segura en la atención de pacientes, en el marco de la norma ISO/IEC 27032.

Objetivos Específicos

Aplicar las políticas, procedimientos y controles de seguridad diseñados en el Plan Director de Seguridad verificando su alineación con las directrices de la norma ISO/IEC 27032 y su aplicación en las áreas críticas de la IPS.

Establecer un sistema de indicadores de desempeño que permita medir y controlar la efectividad de las políticas, procedimientos y controles.

Evaluar los resultados obtenidos a partir de los indicadores definidos, identificando las áreas de mejora.

Ejecutar un programa de seguimiento con asignación de funciones y responsabilidades, complementado con procesos de capacitación y sensibilización en ciberseguridad dirigidos al personal de la IPS.

Marco Referencial

Antecedentes

En los últimos años, la ciberseguridad ha adquirido una relevancia creciente en el sector salud, impulsada por la digitalización de los servicios médicos y el uso generalizado de las tecnologías de la información y las comunicaciones (TIC), estos avances han facilitado la gestión y el acceso a la información clínica, también han expuesto a las instituciones sanitarias a riesgos significativos en materia de protección de datos.

La Organización Mundial de la Salud (OMS) ha señalado que los datos médicos son considerados como uno de los activos más sensibles, dada la naturaleza crítica de la información que contienen, resulta indispensable la adopción de medidas eficaces para prevenir incidentes de seguridad que comprometan la confidencialidad y privacidad de los pacientes.

Estudios internacionales han evidenciado un aumento considerable en las violaciones de datos en el ámbito de la salud como el informe de Verizon (2020) revelando que el 34% de las brechas de seguridad en el sector involucraron la sustracción de información personal, con un impacto directo en la confianza de los usuarios y la estabilidad de las instituciones. De igual manera, el Informe sobre Ciberseguridad en el Sector Salud (CISA, 2022) reportó un incremento del 53% en los ataques de ransomware en comparación con el año anterior, consolidando al sector como uno de los principales objetivos de los ciberdelincuentes.

En Colombia, la Ley 1581 de 2012 establece la regulación sobre la protección de datos personales, imponiendo a las entidades de salud la obligación de garantizar altos estándares de seguridad en el tratamiento de la información, investigaciones académicas y profesionales han señalado que muchas instituciones, presentan limitaciones en la implementación de marcos proactivos de ciberseguridad, lo que aumenta su exposición a riesgos.

Pese a este panorama, existen experiencias positivas que sirven como referencia como el Hospital Universitario de Bellvitge (España) logró reducir un 40% sus brechas de seguridad en tres años mediante la adopción de la norma ISO/IEC 27001, Cleveland Clinic (EE. UU.) ha demostrado que la capacitación periódica del personal en ciberseguridad reduce significativamente la probabilidad de incidente, siendo estos evidencias donde la combinación de políticas sólidas, gestión de riesgos y formación continua constituye un modelo eficaz que puede ser replicado en organizaciones como en la IPS.

Vulnerabilidad de datos sensibles en sistemas de salud:

Repositorio desarrollado como proyecto de grado donde el objetivo es diseñar un plan director de seguridad para IPS que incluye políticas y procedimientos de seguridad informática, identificando riesgos y amenazas, para crear protección de los activos críticos de información, promoviendo un entorno seguro para la atención de pacientes.

Investigación implementación de un plan director de seguridad para la protección de activos críticos de información en infraestructura de salud que se empieza a realizar en el año 2024 la cual es base fundamental para realizar la implementación de las políticas de seguridad.

Marco Conceptual

Para el desarrollo de este estudio, es fundamental delimitar los conceptos clave:

Ciberseguridad: Conjunto de prácticas, procesos y tecnologías destinados a proteger redes, dispositivos y datos frente a accesos no autorizados, daños o ataques. En salud, se orienta a garantizar la confidencialidad, integridad y disponibilidad de la información clínica.

Datos Sensibles: Información personal que puede afectar la intimidad de los individuos si se expone de manera indebida. En el ámbito sanitario, incluye historias clínicas, diagnósticos, tratamientos y cualquier dato que permita identificar al paciente.

Vulnerabilidad: Debilidad en los sistemas de información que puede ser explotada por amenazas para comprometer los datos. Puede originarse en fallas de software, configuraciones inadecuadas o errores humanos.

Gestión de Riesgos: Proceso de identificar, evaluar y priorizar amenazas, implementando medidas para reducir su probabilidad e impacto.

Políticas de Seguridad Informática: Directrices institucionales que definen roles, responsabilidades y protocolos de actuación frente a incidentes de seguridad.

Respuesta a Incidentes (Incident Response): Conjunto de acciones planificadas para detectar, contener y mitigar incidentes de seguridad que afecten los datos o los sistemas.

Normativas de Protección de Datos: Marco legal que regula el tratamiento de la información personal. En Colombia, la Ley 1581 de 2012 y normas complementarias establecen los principios para garantizar la privacidad y la protección de los datos sensibles.

Marco Teórico

La ciberseguridad en el sector salud se enmarca en la necesidad de resguardar datos sensibles de pacientes frente a un ecosistema digital cada vez más complejo, investigaciones recientes subrayan que las amenazas no solo provienen de actores externos, sino también de errores internos y deficiencias en la cultura de seguridad organizacional.

Identificación del problema: En la IPS Se ha identificado una exposición a riesgos derivados de la ausencia de controles formales, la falta de capacitación y la carencia de un Sistema de Gestión de Seguridad de la Información (SGSI).

Análisis de riesgos: La materialización de estas vulnerabilidades podría traducirse en pérdida de información clínica, sanciones legales, disminución en la confianza de los pacientes y daños financieros.

Revisión de literatura: Autores como Whitman y Mattord (2022) destacan que la implementación de marcos normativos como ISO/IEC 27001 y NIST CSF permite mejorar la postura de seguridad de las organizaciones sanitarias.

Propuesta de soluciones: Se plantea la formulación de un Plan Director de Seguridad Informática para la IPS, basado en estándares internacionales, metodologías de gestión de riesgos y programas de capacitación continua.

Implementación y evaluación: La aplicación de controles de seguridad debe ir acompañada de auditorías periódicas y métricas de desempeño que permitan evaluar su efectividad y asegurar la mejora continua.

DIRECTRICES de ISO/IEC 27032 directrices y áreas de enfoque

Seguridad en Internet: Protección contra amenazas online como phishing, ransomware y malware.

Seguridad de la red: Protección de las comunicaciones (firewalls, encriptación) contra accesos no autorizados.

Seguridad de la información: Salvaguarda de datos (backups, políticas de gestión).

Protección del usuario final: Formación y concienciación para prevenir ataques de ingeniería social.

Seguridad de aplicaciones y software: Desarrollo de software seguro desde el diseño.

Protección de infraestructura crítica (CIIP): Especial atención a la protección de servicios esenciales en el entorno digital.

Gestión de Ciber incidentes: Preparación, detección y respuesta a incidentes cibernéticos.

Metodología MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es un marco estructurado del gobierno español para identificar, analizar y

gestionar riesgos en tecnologías de la información (TIC), ofreciendo un proceso sistemático y público que guía a organizaciones, especialmente administraciones públicas, a proteger sus activos digitales mediante la evaluación de amenazas, vulnerabilidades, impactos y la aplicación de salvaguardas, alineándose con normas como la ISO 31000 y el Esquema Nacional de Seguridad (ENS).

Marco Legal

El marco normativo en Colombia establece obligaciones claras para las instituciones de salud en materia de seguridad y protección de datos:

Ley 1581 de 2012: Regula la protección de datos personales y obliga a implementar medidas de seguridad para datos sensibles.

Decreto 1377 de 2013: Reglamenta la autorización y el tratamiento de datos personales recolectados antes de la Ley 1581.

Ley Estatutaria 1266 de 2008: Regula la información financiera, crediticia y de servicios, vinculada también a la seguridad social.

Ley 1712 de 2014 (Transparencia y Acceso a la Información): Refuerza el deber de proteger la información personal en manos de entidades públicas y privadas.

Norma ISO/IEC 27001: Referente internacional para establecer un SGSI que garantice la seguridad de la información.

Jurisprudencia de la Corte Constitucional: Sentencias que han fortalecido el derecho a la privacidad y la obligación de las instituciones de proteger los datos personales.

Este marco normativo evidencia que la omisión en la implementación de controles de ciberseguridad no solo implica un riesgo técnico, sino también sanciones legales, pérdida de confianza institucional y afectación de los derechos fundamentales de los pacientes.

Marco Contextual

Introducción: Presenta el contexto general de la ciberseguridad en el sector de la salud, destacando la importancia de proteger los datos sensibles.

Definición de términos clave: Define conceptos como “datos sensibles”, “ciberseguridad”, “vulnerabilidad” etc., para asegurar que todos los lectores tengan una comprensión clara de estos términos.

Identificación del problema: Describe en detalle los problemas específicos de ciberseguridad que enfrenta la IPS, con un enfoque en la vulnerabilidad de los datos sensibles.

Análisis de riesgos y consecuencias: Analiza los posibles riesgos y consecuencias asociados con estos problemas de ciberseguridad, lo que puede generar impacto en la privacidad del paciente, la reputación de la empresa, y las posibles sanciones legales o financieras.

Revisión de literatura: Revisa la literatura existente sobre ciberseguridad en el sector de la salud, identificando las mejores prácticas y las soluciones propuestas por otros investigadores.

Propuesta de soluciones: Basándonos en el conocimiento adquirido en la especialización en Seguridad Informática, proponemos soluciones específicas para los problemas identificados en la IPS.

Implementación y evaluación: Describimos cómo se podrían implementar estas soluciones en la IPS, y cómo se evaluaría su efectividad.

Metodología

Para alcanzar los objetivos propuestos, el proyecto adoptará un enfoque metodológico mixto (cualitativo y cuantitativo) y se estructurará en fases secuenciales, siguiendo un ciclo de vida similar al propuesto por marcos de gestión de seguridad como el ciclo de Deming (PDCA: Planificar, Hacer, Verificar, Actuar).

Enfoque

Cualitativo. Se utilizará para comprender el contexto organizacional de IPS, identificar la cultura de seguridad y levantar los requerimientos a través de entrevistas y análisis documental de políticas existentes.

Cuantitativo. Se aplicará en la fase de análisis de riesgos para medir la probabilidad y el impacto de las amenazas, así como en la definición de indicadores de gestión (KPIs) para evaluar la eficacia del Plan Director de Seguridad.

Diseño Metodológico

Fases de la Metodología

Fase 1: Diagnóstico y Análisis. Técnicas: Entrevistas semiestructuradas con el personal clave (gerencia, personal de TIC, personal médico), revisión de la documentación existente (políticas, diagramas de red), y análisis técnico de la infraestructura.

Herramientas: Se utilizarán herramientas de escaneo de vulnerabilidades de código abierto (como Open VAS Nessus) para un análisis técnico no intrusivo, y se diseñarán matrices de identificación de activos y de análisis de riesgos basadas en metodologías como MAGERIT o la ISOIEC 27005.

Fase 2: Diseño Estratégico. Técnicas: Se empleará el análisis GAP para comparar el estado actual (obtenido en la Fase 1) con las directrices de la norma ISO 27032 y el marco NIST Cybersecurity Framework. Se realizarán sesiones de trabajo con la dirección para alinear los objetivos de seguridad con los objetivos estratégicos de IPS.

Fase 3: Desarrollo Táctico. Técnicas: Redacción técnica de documentos normativos utilizando plantillas y prácticas internacionales (ej. SANS Institute) para la creación de políticas y procedimientos, adaptándose al contexto y lenguaje de la organización.

Fase 4: Planificación Organizacional. Técnicas: Diseño organizacional y definición de roles utilizando matrices de asignación de responsabilidades (RACI) para clarificar las funciones, elaborando un presupuesto detallado y un cronograma de implementación para las iniciativas propuestas.

Diagnóstico de Vulnerabilidad y Riesgos de Seguridad que Afectan Activos de la IPS

Se realiza un diagnóstico inicial para determinar la situación de la IPS en cuanto riesgos de seguridad, que sea base para hacer aplicación e implementación del plan director de Seguridad.

Para iniciar el diagnóstico se debe organizar fases del proyecto que nos ayuden a generar secuencia para poder cumplir con el objetivo del diseño de SGSI, la cual se referencia en la tabla 1, un cronograma de actividades que se referencian en la tabla 2.

Tabla 1

Fases del Proyecto

Fase	Actividades	Responsable	Duración
1. Diagnóstico inicial	- Revisión de políticas y procedimientos de seguridad existentes. - Identificación de activos de información (servidores, bases de datos, equipos, etc.). - Entrevistas con personal del área TIC. - Definición del alcance del SGSI.	Dana Ximena Ayure Fula Julio César López	Agosto de 2025
2. Análisis de riesgos y GAP	- Aplicación de checklist basada en ISO/IEC 27001. - Identificación de amenazas y vulnerabilidades. - Elaboración de matriz de riesgos (probabilidad vs impacto). - Análisis GAP: Estado actual vs estándares de seguridad.	Dana Ximena Ayure Fula Julio César López	Septiembre de 2025

Fase	Actividades	Responsable	Duración
3. Diseño del SGSI	- Propuesta de controles de seguridad (acceso, cifrado, respaldos, monitoreo). - Redacción del Plan Estratégico de Seguridad de la Información. - Elaboración de políticas propuestas (uso de dispositivos, manejo de contraseñas, acceso remoto). - Propuesta de estructura del SGSI (roles, responsabilidades, comité de seguridad).	Dana Ximena Ayure Fula Julio César López	Octubre de 2025
4. Validación y ajustes	- Socialización del plan con el área TIC de la IPS - Recolección de retroalimentación. - Ajuste del documento según observaciones. - Validación de viabilidad técnica y operativa.	Dana Ximena Ayure Fula Julio César López (con apoyo del área TIC)	Noviembre de 2025
5.Documentación final	- Redacción del informe final del proyecto. - Consolidación de anexos (matriz de riesgos, checklist GAP, políticas propuestas). -Entrega formal del documento.	Dana Ximena Ayure Fula Julio César López	Diciembre de 2025

Nota. Este cuadro muestra las Fases del Proyecto y la duración de este.

Tabla 2

Cronograma de Actividades (Agosto – diciembre 2025)

Actividad	Agosto	Septiembre	Octubre	Noviembre	Diciembre
			3	4	5
1.1 Revisión documental y recolección de información	X				
1.2 Entrevistas con el área TIC	X				
1.3 Identificación de activos de información	X				
2.1 Aplicación de la lista de verificación ISO 27001		X			
2.2 Análisis GAP		X			
2.3 Evaluación de riesgos (matriz)		X			
3.1 Diseño de controles de seguridad			X		
3.2 Redacción del plan estratégico			X		
3.3 Propuesta de políticas de seguridad			X		
4.1 Socialización con área TIC				X	

4.2 Ajustes al plan estratégico	X	
5.1 Redacción del informe final		X
5.2 Preparación de anexos y referencias		X
5.3 Entrega final del proyecto		X

Nota. Esta tabla muestra el cronograma de actividades (Agosto – diciembre 2025)

Diagnóstico Inicial

Se realiza Revisión de políticas y procedimientos de seguridad existentes mediante entrevista con los profesionales TIC de la empresa haciendo una lista de chequeo desarrollados dentro del diagnóstico inicial encontrando:

Seguridad en Internet, Seguridad de la Red. (es el conjunto de tecnologías, políticas y prácticas diseñadas para proteger la infraestructura digital, datos, dispositivos y usuarios contra ciberataques, accesos no autorizados, robos o interrupciones), Dentro de la empresa el conjunto de políticas de seguridad encontradas es un contrato con una empresa acreditada que genera internet seguro. Apéndice 1.

Seguridad de la Información. (conjunto de medidas, políticas y tecnologías diseñadas para proteger la confidencialidad, integridad y disponibilidad de los datos, ya sean digitales o físicos), Dentro de las evidencias en la institución encontramos la Salvaguarda de datos (backups, creados por el personal autorizado líder TIC copias de seguridad en discos externos diariamente.

Protección del Usuario Final. (abarca herramientas y prácticas que defienden dispositivos individuales (portátiles, móviles, servidores) conectados a una red contra malware, ciberataques y robos de datos. Incluye antivirus, firewalls y políticas de seguridad, esenciales porque los usuarios finales suelen ser puntos vulnerables.) En la institución se realizan capacitaciones y auditorías, verificando accesos no permitidos en cada puesto de trabajo donde se pasa eventualmente para identificar que no estén usando USB, páginas no autorizadas, que estén incumplimiento las políticas de seguridad.

Seguridad de aplicaciones y software: (conjunto de prácticas, tecnologías y metodologías integradas en el ciclo de vida del desarrollo (diseño, codificación, pruebas y mantenimiento) para proteger los sistemas contra amenazas, vulnerabilidades y accesos no autorizados.) La IPS adquiere un software llamado SIGSO el cual maneja las historias clínicas, procesos de contabilidad y manejo de seguridad.

Protección de Infraestructura Crítica (CIIP). conjunto de medidas físicas y ciberseguridad diseñadas para salvaguardar activos, sistemas y redes —físicos o virtuales— cuyo fallo tendría efectos debilitantes en la seguridad nacional, economía, salud o bienestar público.) La institución se apoya por el Internet seguro.

Gestión de Ciber Incidentes:(proceso integral, técnico y organizativo diseñado para detectar, analizar, contener, erradicar y recuperarse de eventos adversos de seguridad, tales como ciberataques, brechas de datos o fallos críticos) la institución no presenta un proceso integral para detectar, analizar, contener, erradicar y recuperarse de eventos adversos de seguridad, tales como ciberataques, brechas de datos o fallos críticos.

Identificación de Activos de Información:

Para identificar los activos de la información se contactó con los administrativos de la institución, programando reunión para poder hacer la identificación de activos de información donde se relacionó un inventario detallado de todos los elementos físicos, digitales, software, los cuales se referencian así:

SERVIDORES: 1 SERVIDOR, Servidor encargado de alojar las bases de datos del sistema de historias clínicas de los pacientes atendidos.

EQUIPOS: Cuentan con 20 equipos de cómputo ubicados en el área administrativa y en el área asistencial.

REUNIÓN CON PERSONAL TIC: Manejan Manual de Políticas de Seguridad TIC vigente de la IPS (Código: TI-MA-0001, versión 3, 2025), lo que garantiza viabilidad operativa, su alineación directa con los principios de la norma ISO/IEC 27032.

Áreas Críticas Identificadas en la IPS.

Al realizar verificación hay controles faltantes que no se pudieron completar debido a limitaciones de recursos técnicos y humanos de la IPS, es importante informar que la priorización de áreas críticas (historias clínicas, respaldos, correo corporativo) son básicos para tener en cuenta a la seguridad informática, áreas críticas:

Sistema de gestión de historias clínicas electrónicas (base de datos MySQL con información sensible de pacientes).

Servidor de respaldo y archivo crítico (donde se almacenan copias diarias de bases de datos y documentos legales).

Estaciones de trabajo del personal médico y administrativo con acceso a datos sensibles.

Conectividad a Internet y correo corporativo, usados para intercambio de información con EPS, laboratorios y entidades reguladoras.

Políticas y Controles Aplicados y su Alineación con ISO /IEC 2732.

Para poder hacer verificación de políticas y controles Se revisó el Manual de Políticas de Seguridad TICs vigente en la IPS (Código: TI-MA-0001), se validó la aplicación de los siguientes controles, y de una vez se procedió a hacer la alineación con los principios de ISO/IEC 27032 donde los resultados se ven reflejados en la siguiente tabla (3).

Tabla 3

Políticas y controles aplicados y su alineación con ISO/IEC 27032

Control Aplicado	Artículo del Manual de Políticas de Seguridad	Alineación con ISO/IEC 27032
Restricción de acceso a Internet y prohibición de descargas no autorizadas	Art. 3, 4, 46–50	Sección 6.2: Gestión de riesgos en entornos colaborativos y uso seguro de redes públicas
Uso obligatorio de antivirus actualizado (ESET) y prohibición de software no licenciado	Art. 8, 32, 36–38	Sección 6.3: Protección contra malware y código malicioso
Gestión de identificadores únicos y contraseñas robustas	Art. 24–27	Sección 6.4: Autenticación y gestión de identidades en entornos digitales
Respaldo periódico de información crítica y almacenamiento en lugar seguro	Art. 2, 10, 16	Sección 7.1: Continuidad del negocio y recuperación ante incidentes
Prohibición de dispositivos personales y hardware no autorizado	Art. 22, 39–40	Sección 6.5: Seguridad perimetral y control de endpoints

Nota. Este cuadro muestra las Políticas y controles aplicados y su alineación con ISO/IEC 27032

La tabla referencia los controles ya existen en el manual, no se aplicaban de forma homogénea en todas las áreas, por ejemplo, en las estaciones del área de atención a pacientes se identificó el uso de memorias USB personales, para transferir documentos privados lo cual representa un riesgo de fuga de datos y posible introducción de malware, una brecha directa con la recomendación de ISO/IEC 27032 sobre “colaboración segura entre sistemas y usuarios”.

Adaptación a la realidad operativa de la IPS

Después de la aplicación de estos controles se analiza que la IPS requiere ajustes prácticos.

Capacitación rápida al personal médico: se diseñó una guía visual de “buenas prácticas en ciberseguridad” para personal no técnico, enfocada en el manejo seguro de historias clínicas y uso de correos enviada al grupo de la entidad. Apéndice 2.

Implementación de bloqueo de puertos USB en estaciones críticas, excepto en áreas autorizadas con justificación clínica.

Validación del cifrado en correos con datos sensibles (Art. 50), aunque actualmente no se cuenta con solución corporativa de cifrado, se estableció como medida transitoria el uso de contraseñas compartidas por canales seguros (ej. WhatsApp Business verificado).

Limitaciones encontradas

Durante la aplicación, se identificaron las siguientes limitaciones:

Falta de monitoreo continuo, no existe un SIEM ni registro centralizado de eventos de seguridad (logs), lo que dificulta la detección temprana de incidentes, contraviniendo la recomendación de ISO/IEC 27032 sobre “vigilancia colaborativa”.

Ausencia de un Comité de Ciberseguridad las decisiones de seguridad recaen únicamente en el Coordinador TIC, sin participación de áreas clínicas o legales.

Dependencia de proveedores externos, el hosting del sitio web y dominio de correo están gestionados por terceros sin cláusulas explícitas de ciberseguridad en los contratos.

Imagen 1 fuente https://impulso06.com/ciberseguridad-facil-la-guia-para-dummies-en-seguridad-2025/

Estas limitaciones evidencian que, las políticas les falta una implementación efectiva requiere recursos, gobernanza y cultura organizacional, aspectos que se abordarán en los objetivos posteriores mediante indicadores, seguimiento y capacitación.

Análisis de Riesgo y GAP

Realizar la Aplicación de checklist basada en ISO/IEC 27001.

La que cubre los pasos esenciales para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) la que define el contexto y alcance que está manejando la ips, se desarrolla con ayuda del supervisor de las TIC, está sirve para ayudar a obtener el compromiso de la dirección, realizar la evaluación de riesgos y aplicar controles, encontrando

Aplicación de checklist basada en ISO/IEC 27001. - Identificación de amenazas y vulnerabilidades.

Apéndice 3 Plantilla de Lista de Verificación de la Norma ISO 27001

En los resultados de la lista de chequeo se evidencia que presentan una política de seguridad que no se ha implementado ni se ha socializado de manera completa La entidad tiene una información básica de políticas de seguridad que necesitan ser modificadas y que generen mejora en los procesos.

Elaboración de matriz de riesgos (probabilidad vs impacto). - Análisis GAP:

Estado actual vs estándares de seguridad. Se hace diagnóstico iniciando con el estado de seguridad de la información identificando y clasificando Activos Críticos con la aplicación de la norma ISO/IEC ,27001:2022 y metodología MAGERIT.

Matriz de Levantamiento de Información de Activos Críticos

Identifica, clasifica y prioriza los recursos físicos, digitales y humanos esenciales para la operación y seguridad de una organización. Determina su nivel de riesgo, impacto ante fallas (confidencialidad, integridad, disponibilidad) y el valor estratégico que aportan al negocio, se referencia la tabla así:

Tabla 4

Clasificación de Activos críticos

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 tabla identifica que los activos críticos

La tabla identifica que los activos críticos de cómputo y entidad, tiene un nivel de riesgo medio alto , los activos de confiabilidad donde las historias clínicas ,copias de seguridad, información de pacientes empleados es de confiabilidad alta ,de confiabilidad media infraestructura de red ,documentación administrativa y equipos de cómputo ,Integridad confidencialidad alta ,infraestructura de red ,equipos de cómputo, integridad media historias clínicas y equipo de cómputo, en cuanto a disponibilidad Alta encontramos a historias clínicas ,infraestructura de red, documentación administrativa y equipos de cómputo y criticidad Alta asociado a diversos activos documentales, informáticos. Identifica que el nivel de criticidad de activos como historia clínica, infraestructura de red, copias de seguridad, información de

pacientes empleados es Crítica y la documentación administrativa y equipos de cómputo es de criticidad alta.

Amenazas y Vulnerabilidad según MAGERIT

Determinar qué eventos externos o internos pueden dañar los activos de información (amenazas) y qué debilidades permiten que los eventos ocurran (vulnerabilidades). Se analizan factores como fallos técnicos, errores humanos, acciones malintencionadas y desastres naturales para calcular el riesgo.

Tabla 5

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. En la tabla de amenaza y vulnerabilidad

En la tabla de amenaza y vulnerabilidad se evidencia que hay falencias en estos análisis en diferentes programas identificados en el impacto potencial, Fuga de información, violación de privacidad, perdida de datos de interrupción de servicios, hay deterioro posible pérdida de activos críticos, hay vulnerabilidad de secuestros de datos, puede encontrarse interrupción en servicios esenciales, robo de credenciales y violación de datos sensibles, y la exposición de amenazas conocidas ,datos que están en riesgo según el estudio, hay falta de procedimientos ante incidentes hay riesgo y falta de control contributivo hay riesgo de acceso no controlado, esta tabla identifica que la IPS presenta riesgo de seguridad informática.

Informe de Evaluación de Riesgo y Seguridad de la Información según MAGERIT.

Identifica activos de información, amenazas, vulnerabilidades, el impacto potencial y el nivel de riesgo residual. Este documento estructurado prioriza riesgos para implementar salvaguardas efectivas, permitiendo gestionar la seguridad de manera sistemática

Tabla 6

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. La tabla identifica que las historias clínicas y backaps necesitan ser intervenidas para la aumentar la seguridad.

La tabla identifica que se tiene que priorizar riesgos y salvaguardar las historias clínicas y backups necesitan ser intervenidas para aumentar la seguridad, de manera sistémica.

Acción Recomendada Activos con Riesgo Crítico

Esta acción debe implementar un mantenimiento proactivo, predictivo y preventivo intensivo, basado en controles críticos. Esto incluye monitoreo en tiempo real, gestión de repuestos y optimización de recursos.

Tabla 7

Acción recomendada 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	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. La tabla identifica acciones recomendadas en los activos de información clasificados en medio impacto y valores de riesgo y nivel de riesgo encontrando las muy altas para realizar intervenciones lo más urgente para mitigar los riesgos en la IPS.

Esta tabla determina que la acción debe implementar un mantenimiento proactivo, predictivo y preventivo intensivo, basado en controles críticos de manera urgente. Hay que incluir monitoreo en tiempo real, gestión de repuestos y optimización de recursos.

Acción Recomendada Activos con Riesgo Alto.

Esta Acción debe determinar altos rendimientos, la alta volatilidad e incertidumbre de la empresa.

Tabla 8

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. La tabla identifica los activos con riesgo alto los cuales se deben intervenir de maneja urgente es importante empezar la intervención una primera etapa para evitar riesgo de afectar la seguridad informática.

Esta tabla determina que la Acción se debe intervenir en todos los niveles de riesgo debe generar altos rendimientos, y evitar la volatilidad que en este momento tiene la empresa.

Acción Recomendada Activos con Riesgo Medio.

Los Activos que generalmente presentan: Volatilidad moderada: son menos propensos a subidas y bajadas dramáticas en comparación con las inversiones de alto riesgo.

Tabla 9

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	Medio	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. La tabla agrupa los activos de información presentando un nivel de riesgo medio, aunque la intervención no es urgente es importante tener en cuenta los ítems para intervenir.

Los Activos que generan Volatilidad moderada: son menos propensos a subidas y bajadas dramáticas en comparación con las inversiones de alto riesgo, las cuales según la tabla debe tener auditorias, controles, y respaldos de mantenimiento la empresa.

Activos de Riesgo Bajo

La volatilidad de su riesgo es cero, es decir, nula y por lo tanto su valor no cambiará con el tiempo.

Tabla 10

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. La tabla agrupa los activos de información presentando un nivel de riesgo bajo, aunque la intervención no es urgente es importante tener en cuenta los ítems para intervenir.

El hallazgo referencia un riesgo nulo en validaciones de datos controles y monitoreos que no necesitan intervención urgente paro requieren ser intervenidos.

Matriz de Levantamiento de Información de Activos Según Metodología MAGERIT.

Identifica y cataloga los recursos críticos de información, su interrelación, propietario, tipo (software, hardware, personas) y valoración en confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad

Apéndice 4. Matriz de Levantamiento de Información de Activos según Metodología MAGERIT en la IPS

En el análisis de la Matriz se identifica 61 activos en la empresa de salud catalogando los recursos críticos

Figura 1 *Matriz de Levantamiento de Información de Activos según Metodología MARGERT Y NORMA ISO 27001:2012*

MATRIZ DE LEVANTAMIENTO DE INFORMACION DE ACTIVOS SEGÚN METODOLOGIA MAGERIT Y NORMA ISO 27001:2012																					
Inventario de Activos de Información - Catalogación de Activos																					
Análisis de riesgos Número:		1		Fecha:																	
Empresa: IPS																					
No.		DATOS DEL ACTIVO DE INFORMACION				Valoración Cualitativa						Valoración Cuantitativa							Ubicación (marque con una X)		Responsable del Activo
Nro de activo	Nro de proceso	Nombre del activo de información	Descripción	Tipo de Activo	Epecificación según MAGERIT	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Descripción de impacto en dimesiones de la seguridad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Impacto	Evaluar Activo	Físico	Electrónico	
1	Pr 1	Historias clínicas físicas	Documentos médicos impresos que contienen información	Media_	[dbms] sistema de gestión de bases de datos	M	M	M	M	A	Pérdida o alteración afecta la atención médica y compro	15	15	15	15	20	16	SI	X		Área Médica

			sensible de los pacientes.								mete la privacidad.									
2	Pr 2	Infraestructura de red	Equipos, switches, routers y cableado que soportan la red interna.	Comunicaciones_	[int] datos de gestión interna	B	A	MA	A	M	Fallas o accesos no autorizados impactan todos los sistemas conectados.	9	20	25	20	15	18	SI	X		Área de Tecnología
3	Pr 3	Copias de seguridad	Respaldos digitales de los sistemas de información y base de datos.	Datos_	[int] interno (a usuarios de la propia organización)	B	B	B	M	MA		9	9	9	15	25	13	No	X	X	Área de Tecnología
4	Pr 4	Documentación administrativa	Contratos, informes, manuales y registro	Media_	[prp] desarrollo propio (in house)	M	A	M	A	A	Modificaciones indebidas pueden afectar decision	15	20	15	20	20	18	SI	X	X	Coordinación Administrativa

			s legales o financieros.								es legales y financieras.									
5	Pr 5	Información de pacientes y empleados	Datos personales, médicos, laborales y de contacto almacenados en sistemas.	Datos_	[int] datos de gestión interna	M	M	A	A	M	Fuga o manipulación de datos personales puede causar sanciones y pérdida de confianza.	15	15	20	20	15	17	SI	X	X	Talento Humano / Área Médica
6	Pr 6	Equipos de cómputo	Computadores utilizados por el personal para acceder a los sistemas.	Hardware_	[prp] desarrollo propio (in house)	M	M	M	M	A	Mal uso o accesos indebidos permiten extraer, modificar o borrar información clave.	15	15	15	15	20	16	SI	X	X	Área de Tecnología

7	Pr 7	Sistema de gestión de citas médicas	Plataforma digital para agendar, modificar y consultar citas de pacientes.	Software_	[prp] desarrollo propio (in house)	B	B	B	M	M	Si se compromete la autenticidad o trazabilidad, podrían generarse citas duplicadas o erróneas. La baja confidencialidad expone datos sensibles de pacientes.	9	9	9	15	15	11	No		X	Área Médica / Tecnología
8	Pr 8	Expedientes digitales de pacientes	Archivos electrónicos con historia clínica, diagnósticos y	Datos_	[int] datos de gestión interna	B	B	MA	M	M	La pérdida de integridad o confidencialidad puede	9	9	25	15	15	15	SI		X	Área Médica

			tratamientos.								afectar diagnósticos, tratamientos y la privacidad médica, con consecuencias legales y éticas.										
9	Pr 9	Sistema de gestión de talento humano	Software que administra información de empleados, nómina, capacitaciones y evaluaciones.	Software_	[prp] desarrollo propio (in house)	B	B	B	B	M	La falta de trazabilidad y autenticidad puede generar errores en nómina o evaluaciones. La exposición de datos laborale	9	9	9	9	15	10	No		X	Talento Humano

											s compromete la privacidad del personal.										
10	Pr 10	Correo electrónico corporativo	Cuentas institucionales utilizadas para comunicación interna y externa.	Comunicaciones_	[int] datos de gestión interna	B	B	B	B	MA	Un acceso no autorizado puede facilitar ataques de phishing, fuga de información confidencial y suplantación de identidad institucional.	9	9	9	9	25	12	No		X	Área de Tecnología
11	Pr 11	Plataforma de capacitación virtual	Sistema para formación	Software_	[prp] desarrollo propio	B	B	M	M	M	La baja disponibilidad	9	9	15	15	15	13	No		X	Talento Humano / Área Médica

			continua del personal en temas de salud ocupacional.		(in house)						afecta la formación continua. La pérdida de integridad puede invalidar certificaciones o evaluaciones.									
12	Pr 12	Información de proveedores	Datos contractuales, financieros y de contacto de empresas aliadas.	Datos_	[int] datos de gestión interna	B	B	M	M	M	La exposición de datos financieros o contractuales puede afectar negociaciones, generar fraudes o comprometer la	9	9	15	15	15	13	No		X	Coordinación Administrativa

											reputación institucional.										
13	Pr 13	Formularios de evaluación médica	Documentos físicos y digitales utilizados en exámenes ocupacionales.	Media_	[prp] desarrollo propio (in house)	B	B	M	M	M	La alteración o pérdida de estos documentos puede invalidar exámenes ocupacionales, afectar decisiones laborales y generar conflictos legales.	9	9	15	15	15	13	No	X	X	Área Médica
14	Pr 14	Sistema de gestión documental	Repositorio digital de políticas,	Software_	[prp] desarrollo propio (in house)	B	B	M	M	M	La falta de trazabilidad o integrid	9	9	15	15	15	13	No		X	Coordinación Administrativa

			procedimientos y registros institucionales.								ad puede generar versiones contradictorias de políticas internas, afectando auditorías y cumplimiento normativo.										
15	Pr 15	Sistema de gestión de historias clínicas	Software que almacena y gestiona expedientes médicos	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Pérdida o alteración afecta la atención médica y compromete la privacidad.	15	15	15	15	20	16	SI		X	Área Médica

16	Pr 16	Base de datos de pacientes	Información médica y personal	Datos_	[int] datos de gestión interna	M	M	MA	M	A	Exposición o modificación de datos sensibles puede generar sanciones legales.	15	15	25	15	20	18	SI		X	Área Médica
17	Pr 17	Sistema de facturación	Gestión de pagos, cobros y cuentas	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Errores o accesos indebidos afectan pagos, ingresos y cumplimiento tributario.	15	15	15	15	20	16	SI		X	Coordinación Administrativa
18	Pr 18	Registros de atención médica	Documentos físicos de consultas	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Alteraciones comprometen diagnósticos, tratamientos y	15	15	15	15	20	16	SI	X		Área Médica

											trazabilidad clínica.									
19	Pr 19	Manuales de procedimientos	Documentación interna de procesos	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Cambios no autorizados pueden generar fallos operativos y legales.	15	15	15	15	20	16	SI	X	X	Coordinación Administrativa
20	Pr 20	Sistema de gestión de calidad	Software para auditorías y control	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Pérdida de integridad afecta auditorías y mejora continua.	15	15	15	15	20	16	SI		X	Área Médica
21	Pr 21	Información de contacto de pacientes	Teléfonos, correos, direcciones	Datos_	[int] datos de gestión interna	M	M	MA	M	A	Fuga de datos personales afecta privacidad y confian	15	15	25	15	20	18	SI		X	Talento Humano

											za institucional.										
22	Pr 22	Información de contacto de empleados	Datos personales y laborales	Datos_	[int] datos de gestión interna	M	M	MA	M	A	Exposición de datos laborales puede generar conflictos internos.	15	15	25	15	20	18	SI	X	X	Talento Humano
23	Pr 23	Contratos laborales	Documentos legales de vinculación	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Alteraciones pueden invalidar acuerdos y generar demandas.	15	15	15	15	20	16	SI		X	Área de Tecnología
24	Pr 24	Licencias de software	Documentos de propiedad y uso	Media_	[int] datos de gestión interna	M	M	M	M	A	Pérdida o mal uso puede generar sanciones por incumpl	15	15	15	15	20	16	SI		X	Talento Humano

											imiento legal.									
25	Pr 25	Sistema de gestión de turnos	Software para asignación de horarios	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Fallos afectan la operación diaria y la asignación de personal.	15	15	15	15	20	16	SI		X	Coordinación Administrativa
26	Pr 26	Registros de mantenimiento de equipos	Historial de revisiones técnicas	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Omisiones pueden generar fallos técnicos y riesgos operativos.	15	15	15	15	20	16	SI	X	X	Área de Tecnología
27	Pr 27	Inventario de activos físicos	Listado de equipos y dispositivos	Media_	[int] datos de gestión interna	M	M	M	M	A	Errores afectan control patrimonial y seguridad	15	15	15	15	20	16	SI		X	Área de Tecnología

											física.										
28	Pr 28	Sistema de gestión de riesgos	Software para análisis de amenazas	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Información incorrecta puede generar decisiones erróneas.	15	15	15	15	20	16	SI		X	Coordinación Administrativa
29	Pr 29	Políticas de seguridad de la información	Documentos normativos internos	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Desactualización compromete cumplimiento normativo.	15	15	15	15	20	16	SI		X	Coordinación Administrativa
30	Pr 30	Registros de auditoría	Evidencias de revisiones internas	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Alteraciones invalidan procesos de verificación y control.	15	15	15	15	20	16	SI		X	Coordinación Administrativa

31	Pr 31	Sistema de videovigilancia	Cámaras y grabaciones	Hardware_	[int] datos de gestión interna	M	M	M	M	A	Fallos afectan seguridad física y trazabilidad de eventos.	15	15	15	15	20	16	SI		X	Área de Seguridad
32	Pr 32	Información de campañas de salud	Materiales y registros de actividades	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Manipulación puede generar desinformación y pérdida de credibilidad.	15	15	15	15	20	16	SI	X	X	Área Médica
33	Pr 33	Sistema de gestión de incapacidades	Software para control de ausencias	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Errores afectan pagos, licencias y cumplimiento legal.	15	15	15	15	20	16	SI		X	Talento Humano
34	Pr 34	Registros de capacitaciones	Listado de cursos y	Media_	[prp] desarrollo propio	M	M	M	M	A	Pérdida afecta validación de	15	15	15	15	20	16	SI		X	Talento Humano

			asistentes		(in house)						competencias y cumplimiento normativo.									
35	Pr 35	Información de exámenes ocupacionales	Resultados médicos laborales	Datos_	[int] datos de gestión interna	M	M	MA	M	A	Fuga o alteración compromete decisiones médicas y legales.	15	15	25	15	20	18	SI		X	Área Médica
36	Pr 36	Sistema de gestión de quejas	Plataforma para reportes de usuarios	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Manipulación afecta transparencia y mejora continua.	15	15	15	15	20	16	SI		X	Coordinación Administrativa
37	Pr 37	Información de encuestas de satisfacción	Resultados y análisis	Datos_	[int] datos de gestión interna	M	M	M	M	A	Alteraciones distorsionan percepción instituci	15	15	15	15	20	16	SI		X	Coordinación Administrativa

											onal.									
38	Pr 38	Registros de visitas	Control de ingreso de personas	Media_	[int] datos de gestión interna	M	M	M	M	A	Pérdida afecta trazabilidad y seguridad física.	15	15	15	15	20	16	SI	X	X	Área de Seguridad
39	Pr 39	Información de campañas internas	Comunicaciones institucionales	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Errores generan confusión y afectan clima organizacional.	15	15	15	15	20	16	SI		X	Talento Humano
40	Pr 40	Sistema de gestión de exámenes ocupacionales	Software que administra resultados médicos laborales	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Pérdida o alteración afecta la atención médica y compromete la privacidad.	15	15	15	15	20	16			X	Área Médica

41	Pr 41	Plataforma de agendamiento web	Portal en línea para que los pacientes soliciten citas	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Fallos o accesos indebidos pueden generar citas erróneas y exposición de datos personales.	15	15	15	15	20	16			X	Área Médica / Tecnología
42	Pr 42	Base de datos de empleados	Información laboral, médica y de contacto del personal	Datos_	[int] datos de gestión interna	M	M	MA	M	A	Fuga o modificación de datos laborales puede causar conflictos legales y operativos.	15	15	25	15	20	18			X	Talento Humano
43	Pr 43	Sistema de gestión de proveedores	Software que administra contratos, pagos	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Alteraciones afectan pagos, contratos y	15	15	15	15	20	16			X	Coordinación Administrativa

			y evaluaciones								relaciones comerciales.									
44	Pr 44	Registros físicos de exámenes médicos	Documentos impresos con resultados ocupacionales	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Pérdida o manipulación compromete decisiones médicas y legales.	15	15	15	15	20	16		X		Área Médica
45	Pr 45	Sistema de gestión de campañas de salud	Software que organiza actividades preventivas y educativas	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Errores pueden generar desinformación y afectar la credibilidad institucional.	15	15	15	15	20	16			X	Área Médica
46	Pr 46	Información de licencias médicas	Registros de incapacidades	Datos_	[int] datos de gestió	M	M	MA	M	A	Fuga o alteración afecta	15	15	25	15	20	18			X	Talento Humano

			y ausencias laborales		n interna						pagos, ausencias y cumplimiento legal.									
47	Pr 47	Sistema de gestión de capacitaciones	Plataforma para cursos, evaluaciones y certificados	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Pérdida de registros invalida certificaciones y afecta cumplimiento normativo.	15	15	15	15	20	16			X	Talento Humano
48	Pr 48	Sistema de gestión de citas por WhatsApp	Canal alternativo para agendamiento y comunicación con pacientes	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Fallos o accesos indebidos pueden generar citas erróneas y exposición de datos persona	15	15	15	15	20	16			X	Área Médica / Tecnología

											les.									
49	Pr 49	Registro de consentimiento informado	Documentos físicos o digitales firmados por pacientes antes de procedimientos	Media_	[prp] desarrollo propio (in house)	M	M	MA	M	A	Pérdida o alteración compromete la validez legal de procedimientos médicos.	15	25	15	20	19		X	X	Área Médica
50	Pr 50	Sistema de control de acceso físico	Software y dispositivos que regulan el ingreso a áreas restringidas	Hardware_	[int] datos de gestión interna	M	M	M	M	A	Fallos afectan la seguridad física y trazabilidad de ingresos.	15	15	15	15	20	16			X	Área de Seguridad
51	Pr 51	Información de campañas externas	Materiales y registros de actividades	Media_	[prp] desarrollo propio (in house)	M	M	M	M	A	Manipulación puede generar desinformación	15	15	15	15	20	16		X	X	Área Médica / Comuni

			realizadas fuera de la sede								y afectar la imagen institucional.									caciones
52	Pr 52	Sistema de gestión de inventario clínico	Software que controla insumos médicos, reactivos y equipos	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Errores afectan disponibilidad de insumos médicos y atención oportuna.	15	15	15	15	20	16			X	Área Médica / Logística
53	Pr 53	Información de seguros y pólizas	Documentación relacionada con seguros institucionales y de empleados	Media_	[int] datos de gestión interna	M	M	MA	M	A	Fuga o alteración puede generar pérdidas económicas y conflictos legales.	15	15	25	15	20	18			X	Coordinación Administrativa
54	Pr 54	Sistema de gestión de	Plataforma que consoli	Software_	[prp] desarrollo	M	M	M	M	A	Datos incorrectos	15	15	15	15	20	16			X	Coordinación

		indicadores	da métrica s de desemp eño y calidad		propio (in house)						afectan decision es estratég icas y auditorí as.									Admini strativa
55	Pr 55	Informació n de auditorías externas	Informe s y hallazg os de revision es por entes regulad ores	Media_	[int] datos de gestió n intern a	M	M	M A	M	A	Pérdida o alteraci ón compro mete cumpli miento normati vo y reputaci ón.	15	15	25	15	20	18			X	Coordin ación Admini strativa
56	Pr 56	Registro de incidentes de seguridad	Base de datos con eventos relacion ados con ciberse guridad o segurid ad	Datos_	[int] datos de gestió n intern a	M	M	M A	M	A	Omisio nes dificulta n análisis de riesgos y respuest a ante eventos.	15	15	25	15	20	18			X	Área de Tecnolo gía / Segurid ad

			física																	
57	Pr 57	Sistema de gestión de comunicaciones internas	Plataforma para boletines, anuncios y mensajes institucionales	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Fallos afectan coordinación institucional y clima organizacional.	15	15	15	15	20	16			X	Talento Humano / Comunicaciones
58	Pr 58	Sistema de gestión de citas telefónicas	Registro y control de citas agendadas por llamada	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Errores o accesos indebidos pueden generar citas duplicadas o perdidas.	15	15	15	15	20	16			X	Área Médica / Recepción
59	Pr 59	Información de pagos electrónicos	Datos de transacciones realizadas por medios digitale	Datos_	[int] datos de gestión interna	M	M	MA	M	A	Fuga o alteración puede generar fraudes y conflict	15	15	25	15	20	18			X	Coordinación Administrativa

			s								os financieros.									
60	Pr 60	Sistema de gestión de insumos de oficina	Control de papelería, mobiliario y recursos administrativos	Software_	[prp] desarrollo propio (in house)	M	M	M	M	A	Errores afectan operación administrativa y control patrimonial.	15	15	15	15	20	16		X		Coordinación Administrativa
61	Pr 61	Información de campañas de prevención psicosocial	Materiales y registros de actividades de bienestar emocional	Media_	[prp] desarrollo propio (in house)	M	M	MA	M	A	Pérdida o manipulación afecta bienestar emocional y credibilidad institucional.	15	15	25	15	20	18		X	X	Talento Humano / Área Médica

Matriz de Levantamiento de Información de Activos según Metodología MAGERIT Y Norma ISO 27001_2012 en la IPS.

Control de Seguridad según Norma ISO/IEC 27032.

Se realizan verificaciones de controles de seguridad analizando las directrices de la norma ISO/IEC 27032.

Identifica controles de seguridad enfocados en la ciberseguridad para proteger la información en el ciberespacio. Abarca seguridad de redes, aplicaciones, usuarios y protección de infraestructuras críticas, enfocándose en la detección, prevención y respuesta a ciberataques como phishing, malware y ransomware.

Tabla 11. ***Alineación de controles de seguridad con ISO/IEC 27032 en la IPS***

Control aplicado	**Artículo del manual de políticas de seguridad**	**Alineacion con iso/iec 27032**	**Requisito iso/iec 27032**	**Estado de implementación en la IPS**
Restricción de acceso a Internet y prohibición de descargas no autorizadas	Art. 3, 4, 46–50	Sección 6.2: Gestión segura del uso de redes públicas y colaboración en entornos abiertos	Parcial– Se permite acceso a Internet sin filtrado de contenido ni monitoreo de navegación	Implementar solución de filtrado web (URL categorizado) y registrar accesos mediante proxy o firewall con logs
Uso obligatorio de antivirus actualizado y prohibición de software no licenciado	Art. 8, 32, 36–38	Sección 6.3: Protección contra malware y código malicioso en entornos colaborativos	Cumple– Se utiliza ESET Smart Security en todos los equipos	Mantener actualizaciones automáticas y auditar mensualmente el estado de protección
Gestión de identificadores	Art. 24–27	Sección 6.4: Autenticación	Parcial– No se exige cambio	Establecer política de contraseñas (mín. 8

únicos y contraseñas robustas		segura y gestión de identidades en entornos digitales	periódico ni complejidad mínima en contraseñas	caracteres, mayúsculas, números, cambio cada 90 días) y activar bloqueo tras intentos fallidos
Respaldo periódico de información crítica y almacenamiento en lugar seguro	Art. 2, 10, 16	Sección 7.1: Continuidad del negocio y recuperación ante incidentes cibernéticos	Parcial– Se realizan respaldos, pero no hay verificación de integridad ni plan de recuperación documentado	Documentar procedimiento de respaldo/restauración, probar restauraciones trimestrales y cifrar copias críticas
Prohibición de dispositivos personales y hardware no autorizado (USB, discos externos)	Art. 22, 39–40	Sección 6.5: Control de endpoints y prevención de fugas de datos en entornos colaborativos	No cumple– Uso frecuente de memorias USB personales en áreas clínicas	Bloquear puertos USB mediante GPO o solución de control de dispositivos; autorizar excepciones solo con justificación clínica y registro
Cifrado en transmisión de datos sensibles (correo, archivos)	Art. 50	Sección 6.6: Comunicación segura y protección de datos en tránsito	No cumple– No se cuenta con mecanismos de cifrado corporativo	Implementar cifrado TLS en correo saliente y usar plataformas seguras (ej. enlaces cifrados con contraseña) para compartir archivos sensibles
Monitoreo y registro de eventos de seguridad (logs)	No explícito en el manual	Sección 8.1: Vigilancia colaborativa y detección	No cumple– No existe centralización ni revisión de logs	Implementar servidor de logs (SIEM básico o herramienta open-source como Wazuh) y definir alertas críticas

temprana de incidentes

Nota. La tabla referencia el Control aplicado a los diferentes estudios de seguridad informática de la IPS, basándose en artículos y políticas de seguridad alineado con la norma referenciando los requisitos y los ítems para implementar en la entidad los cuales deben tenerse en cuenta para implementar el plan director de seguridad.

Se identifican controles de seguridad enfocados en la ciberseguridad basándose en artículos y políticas de seguridad para proteger la información. Abarca seguridad de redes, aplicaciones, usuarios y protección de infraestructuras críticas, se debe Implementar solución de filtrado web (URL categorizado) y registrar accesos mediante proxy o firewall enfocándose en la detección, estableciendo políticas de contraseñas, documentar procedimientos de bloqueos de puertos USB, implementando cifrados, hay que tener prevención y respuesta a ciberataques como phishing, malware y ransomware.

Arquitectura de la Información

Identifica la estructura, organización, etiquetado y navegación de contenidos en entornos digitales (webs, apps, intranets) para asegurar que sean intuitivos, útiles y fáciles de usar.

Se verifica la implementación el diseño el marco integral del sistema de la organización contra amenazas cibernéticas, esto para realizar controles identificar, prevenir y detectar incidentes para asegurar la continuidad del negocio y poder implementar y mejorar posibles falencias. Capítulo

Tabla 12. ***Arquitectura de la información***

Componente	**Propósito Principal**	**Configuración y Controles Clave**	**Relación con el Plan Director de Seguridad**
Firewall de Nueva Generación (NGFW)	Proteger el perímetro de la red, controlar el tráfico y prevenir accesos no autorizados.	• Filtrado de contenido web (URL Filtering): Bloqueo de acceso a sitios maliciosos o no autorizados. • Sistema de Prevención de Intrusiones (IPS): Detectar y bloquear patrones de ataque conocidos. • Reglas de acceso inter-VLAN: Controlar estrictamente la comunicación entre segmentos de red.	Aplica directamente el control de "Restricción de acceso a Internet" y fortalece la seguridad perimetral.
Segmentación de Red (VLANs)	Aislar sistemas críticos para limitar la propagación de amenazas y proteger los datos sensibles.	• VLAN 10 – Servidores: Aloja la BD MySQL y el servidor de archivos. Solo accesible desde VLANs autorizadas.	Reduce el riesgo de movimiento lateral de un atacante, protegiendo los activos de información críticos identificados.

Componente	Propósito Principal	Configuración y Controles Clave	Relación con el Plan Director de Seguridad
Servidor SIEM (Security Information and Event Management)	Centralizar, monitorear y analizar los registros (logs) de seguridad de toda la red para una detección temprana de incidentes.	• VLAN 20 – Clínica: Para estaciones de trabajo del personal médico que accede a historias clínicas. • VLAN 30 – Administrativa: Para equipos del área administrativa. • Agentes en Endpoints y Servidores: Recolectan logs de eventos de seguridad. • Correlación de Eventos: Define alertas por actividades sospechosas (ej. intentos de acceso fallidos repetidos). • Plataforma: Wazuh (Open-Source).	Aborda directamente la debilidad crítica de la “Falta de monitoreo continuo” y la ausencia de revisión de logs, alineándose con la norma ISO/IEC 27032.
Servidor de Directorio Activo (o similar)	Centralizar la gestión de usuarios, autenticación y la aplicación de políticas de seguridad en los equipos.	• Políticas de Grupo (GPO):1. Bloqueo de puertos USB en equipos no autorizados.2. Políticas de contraseñas robustas (complejidad, longitud, rotación). • Gestión centralizada de identidades y permisos de acceso.	Implementa los controles de “Prohibición de dispositivos personales” y “Gestión de identificadores únicos y contraseñas” de manera sistematizada y escalable.

Componente	Propósito Principal	Configuración y Controles Clave	Relación con el Plan Director de Seguridad
Endpoints (Estaciones de trabajo)	Puntos finales donde los usuarios interactúan con los datos. Son la primera línea de defensa.	• Software Antivirus gestionado centralmente (ESET Smart Security). • Sistema Operativo actualizado y con parches de seguridad. • Cifrado de disco (opcional): Protege la información en caso de robo del equipo.	Asegura el cumplimiento de la política de "Uso obligatorio de antivirus actualizado" y reduce la superficie de ataque general.
Servidor de Respaldos (Backup Server)	Garantizar la continuidad del negocio y la recuperación de datos ante un incidente (ej. Ransomware).	• Almacenamiento en un segmento de red seguro y aislado. • Cifrado de las copias de seguridad. • Pruebas de restauración periódicas para validar la integridad de los respaldos.	Materializa la política de "Respaldo periódico de información crítica" y es un control fundamental para la recuperación ante incidentes cibernéticos, como indica la norma ISO/IEC 27032.

Nota. La arquitectura propuesta integra controles preventivos (NGFW, segmentación), detectivos (SIEM) y correctivos (respaldos).

La arquitectura propuesta integra controles preventivos (NGFW, segmentación), detectivos (SIEM) y correctivos (respaldos), complementados por la gestión centralizada de identidades y el endurecimiento de endpoints. Este enfoque contribuye a reducir riesgos como accesos no autorizados, propagación lateral y pérdida de información, fortaleciendo el cumplimiento de políticas internas y buenas prácticas de ciberseguridad.

Desarrollo Sistema de Indicadores de Desempeño y Efectividad de Políticas Procedimientos y Controles

Se elabora un Sistema de Indicadores para la IPS, de acuerdo con el diagnóstico inicial enfocado en el ámbito de seguridad informática, orientado a medir y controlar la efectividad de las políticas, procedimientos y controles antes, durante y después de su implementación.

Este sistema aplica a IPS que manejan datos sensibles, historias clínicas, resultados ocupacionales, exámenes médicos, bases de datos de empresas clientes y servicios digitales, cumpliendo estándares como:

ISO 27001 / 27002

Ley de protección de datos personales (Habeas Data)

Buenas prácticas de ciberseguridad en salud.

Controles internos administrativos y técnicos.

Se presentan indicadores por áreas: políticas, procedimientos, controles técnicos, controles administrativos, respuesta a incidentes, continuidad del negocio y concientización del personal todo que permita medir y controlar la efectividad de las políticas, procedimientos y controles de seguridad implementados en la IPS, en coherencia con los principios de mejora continua propios de un Sistema de Gestión de Seguridad de la Información (SGSI).

Sistema de Indicadores de Desempeño para la Seguridad Informática de la IPS

Identificar los indicadores que maneja la IPS, la efectividad, eficiencia y madurez de los controles de seguridad, haciendo que se monitoree e identifique la vulnerabilidad y la postura de riesgo en tiempo real de la institución.

Indicadores de Cumplimiento de Políticas de Seguridad Informática

Cumplimiento de políticas de seguridad

Objetivo: Medir qué tan implementadas y aplicadas están las políticas (accesos, contraseñas, backups, privacidad, etc.).

Fórmula: (Políticas implementadas y operativas / Políticas aprobadas) × 100.

Meta: ≥ 95%.

Frecuencia: Semestral

Responsable: Oficial de seguridad / Coordinador TIC.

Fuente: Auditoría de controles, revisión documental.

Porcentaje de áreas alineadas al marco de seguridad

Objetivo: Verificar cumplimiento de políticas por áreas: medicina laboral, laboratorio, psicología, audiometría, talento humano, facturación.

Fórmula: (Áreas que cumplen / Áreas evaluadas) × 100.

Meta: ≥ 90%.

Frecuencia: Semestral.

Fuente: Evaluación por área.

Responsable: Seguridad TIC – Calidad.

Indicadores sobre Procedimientos de Seguridad

Cumplimiento de procedimientos críticos de TI (gestión de accesos, actualización de software, backups, protección de datos).

Fórmula: (Procedimientos ejecutados conforme / Total de procedimientos establecidos) × 100.

Meta: ≥ 95%.

Frecuencia: Mensual.

Responsable: TIC – Control interno.

Fuente: Registros de ejecución.

Tiempo de actualización de sistemas

Objetivo: Verificar la efectividad del procedimiento de actualización y parcheo.

Fórmula: Tiempo promedio entre lanzamiento de parche y aplicación internamente

Meta: menor de 14 días

Frecuencia: Mensual

Cumplimiento de procedimiento de respaldo

Fórmula: (Respaldos realizados / Respaldos programados) × 100.

Meta: 100%.

Frecuencia: Semanal.

Fuente: Logs de backup.

Responsable: TIC.

Indicadores de Controles de Seguridad Informática

Índice de dispositivos protegidos

Objetivo: Medir eficacia del control técnico de antivirus, firewall y antimalware.

Fórmula: (Dispositivos con protección activa / Total de dispositivos) × 100

Meta: ≥ 98%.

Frecuencia: Mensual.

Fuente: Consola de seguridad TIC.

Porcentaje de accesos con autenticación segura

Objetivo: Confirmar uso de contraseñas robustas y doble factor (2FA).

Fórmula: (Usuarios con autenticación segura activa / Total de usuarios) × 100.

Meta: 100% áreas clínicas; 95% administrativos.

Frecuencia: Mensual

Porcentaje de vulnerabilidades corregidas

Objetivo: Medir eficacia de los controles de detección y eliminación de riesgos técnicos.

Fórmula: (Vulnerabilidades corregidas / Vulnerabilidades detectadas) × 100

Meta: ≥ 90%.

Frecuencia: Mensual.

Fuente: Escáner de vulnerabilidades.

Indicadores de Riesgo y Gestión de Incidentes

Tasa de incidentes de seguridad

Objetivo: Evaluar la efectividad de los controles preventivos.

Fórmula: (Incidentes registrados / Total de usuarios internos) × 100

Meta: Tendencia a la baja.

Frecuencia: Mensual.

Fuente: Registro de incidentes – Mesa de ayuda TIC.

Tiempo de respuesta a incidentes

Fórmula: (Tiempo promedio desde detección hasta mitigación)

Meta: < 4 horas críticos

Frecuencia: Mensual

Responsable: Equipo de respuesta

Incidentes asociados a errores humanos

Objetivo: Medir efectividad de capacitación y cultura de seguridad.

Fórmula: (Incidentes por error humano / Total incidentes) × 100.

Meta: ≤ 20%.

Frecuencia: Mensual.

Indicadores de Protección de Datos (Habeas Data)

Cumplimiento de medidas de protección de datos sensibles

Fórmula: (Procesos que cumplen protección de datos / Procesos evaluados) × 100.

Meta: 100%.

Fuente: Auditoría de datos personales.

Responsable: Oficial de Privacidad.

Porcentaje de contratos con cláusulas de seguridad (con proveedores, médicos externos, laboratorios aliados, empresas clientes)

Fórmula: (Contratos con cláusula de protección / Total contratos activos) × 100.

Meta: 100%.

Frecuencia: Anual.

Gestión de solicitudes de titulares de datos

Fórmula: (Solicitudes atendidas a tiempo / Total solicitudes) × 100

Meta: ≥ 95% en 10 días hábiles

Frecuencia: Mensual

Indicadores de Concientización y Capacitación en Seguridad

Cobertura de capacitación en seguridad informática

Fórmula: (Trabajadores capacitados / Total trabajadores) × 100

Meta: 100%.

Frecuencia: Semestral.

Índice de phishing simulado

Objetivo: Medir preparación del personal ante ciberataques reales.

Fórmula: (Usuarios que cayeron en simulación / Total usuarios) × 100.

Meta: ≤ 10%.

Frecuencia: Trimestral

Uso adecuado de dispositivos y sistemas

Fórmula: (Cumplimiento de normas de uso de TI / Usuarios evaluados) × 100.

Meta: ≥ 95%.

Indicadores de Continuidad del Negocio y Resiliencia

Pruebas de recuperación ante desastres

Fórmula: (Pruebas ejecutadas exitosamente / Pruebas programadas) × 100.

Meta: 100%.

Frecuencia: Anual.

Tiempo de recuperación (bgvhnnn bb/RPO)

Objetivo: Verificar que la IPS puede recuperar servicios tras caída.

Fórmula: Tiempo real de recuperación vs. RTO establecido

Meta: Cumplimiento ≥ 90%

Frecuencia: Semestral

Disponibilidad de sistemas críticos

Fórmula: (Horas de servicio disponible / Horas planificadas) × 100.

Meta: ≥ 99%.

Frecuencia: Mensual.

La ausencia de medidas previas dificultaba evaluar si la seguridad estaba generando el impacto esperado, sé diseñó un conjunto de indicadores clave de seguridad (KPI), alineados con las áreas críticas identificadas y con los controles del Manual de Políticas TIC. Estos indicadores fueron validados con el Coordinador TIC de la IPS, quien confirmó su viabilidad técnica y operativa con los recursos actuales. Se acordó registrarlos en una hoja de control mensual que servirá como insumo para las reuniones de seguimiento del SGSI.

Avance concreto: Se logró definir un sistema de indicadores cuantificables, priorizando simplicidad, relevancia y factibilidad. Esto representa un avance significativo frente al estado inicial, donde no existía ningún mecanismo de medición de la seguridad informática.

Evaluación de conocimiento sobre políticas de seguridad en IPS

Por medio de encuestas de conocimiento al talento humano de la institución se identificó que no tienen conocimiento claro sobre políticas o manejo de seguridad informática. Apendice 5.

¿Usted sabe o tiene conocimiento sobre qué es seguridad de la información?

¿Conoce las políticas de seguridad de la información de la entidad?

Escriba su concepto de seguridad de la información

¿Qué entiende por confidencialidad de la información?

¿Qué entiende por Disponibilidad de la información?

¿Qué entiende por integridad de la información?

¿Cuál es la información, datos o archivo digital o físico que considera más importante en su área?

¿Cuáles han sido los problemas en cuanto a seguridad de la información en la entidad o en su puesto de trabajo?

Evaluación de Resultados Obtenidos a Partir de Indicadores Definidos.

Al realizar el análisis inicial de la IPS e identificando áreas de mejora y utilizando como referencia los estándares internacionales ISO/IEC 27032, ISO/IEC 27001, ISO/IEC 27001:2022, la metodología de análisis y gestión de riesgos MAGERIT, se identifican múltiples vulnerabilidades en los procesos de cifrado, en el control de accesos, en el manejo de historias clínicas electrónicas, bases de datos de pacientes, políticas internas de seguridad, infraestructura de red y equipos de cómputo.

Los hallazgos evidencian que la organización carece de un Sistema de Gestión de Seguridad de la Información (SGSI) formalizado, lo cual incrementa significativamente la exposición a incidentes de ciberseguridad, accesos no autorizados, fuga de datos y fallas operativas que comprometen la confidencialidad, integridad y disponibilidad de la información crítica.

Mediante la aplicación de MAGERIT se determinaron los riesgos más relevantes, sus impactos y probabilidades, permitiendo priorizar activos esenciales para la operación clínica, requiere adoptar un enfoque estratégico de seguridad, actualizado y alineado con buenas prácticas internacionales.

Como resultado de este estudio se plantea la implementación de un Plan Director de Seguridad, que servirá como hoja de ruta para establecer políticas, controles técnicos, procedimientos, monitoreo y un marco de mejora continua que fortalezca la protección de los activos críticos de la organización. Este plan busca no solo mitigar los riesgos identificados, sino también avanzar hacia un SGSI maduro que incremente la confiabilidad institucional, para que se cumplan las normativas vigentes y garantizar la protección adecuada de los datos de los pacientes.

Resultados clave

Antivirus: El 100% de las estaciones tienen DEFENDER instalado, pero el 30% no tenía actualizaciones en los últimos 15 días debido a desconexiones de Internet no reportadas.

Contraseñas: Solo el 45% de los usuarios cumplía con complejidad mínima (más de 6 caracteres, sin nombres propios). El resto usaba contraseñas como “123456” o “empresa2025”.

Capacitación: Solo 2 de 20 empleados completaron la guía de buenas prácticas en ciberseguridad, lo que refleja baja priorización del tema por parte del personal clínico.

Respaldos: Se verificó que se realizan copias diarias, pero ninguna restauración ha sido probada en los últimos 6 meses, lo que pone en riesgo la disponibilidad real de la información.

Áreas de mejora prioritarias

Con base en estos resultados, se identificaron tres áreas críticas para intervenir:

Gestión de identidades y accesos: Implementar política de contraseñas robustas y capacitación específica sobre su importancia.

Pruebas de recuperación: Programar simulacros trimestrales de restauración de bases de datos y documentos críticos.

Cultura de seguridad: Diseñar estrategias de sensibilización breves, visuales y repetidas (afiches, recordatorios en correo, micro capacitaciones).

La evaluación permitió pasar de una percepción subjetiva (“creemos que estamos seguros”) a una visión objetiva basada en datos. Esto confirma que la medición es el primer paso hacia la mejora real.

Ejecución de un Programa de Seguimiento

Ejecutar un programa de seguimiento con asignación de funciones y responsabilidades, complementado con procesos de capacitación y sensibilización en ciberseguridad dirigidos al personal de la IPS elaborando un plan director el cual debe contener:

Objetivo: establecer un plan integral de seguridad que fortalezca la protección de la información clínica, administrativa y operativa de la IPS mediante la definición de funciones claras, responsabilidades específicas y procesos de capacitación y sensibilización continua para todo el personal.

Aplica a:

Personal asistencial (médicos, enfermeros, auxiliares).

Personal administrativo.

Personal de TIC.

Directivos.

Personal de servicios generales (seguridad física, mantenimiento).

Contratistas y proveedores externos que manejan información.

Responsabilidades:

Aprobar políticas y lineamientos de ciberseguridad

Priorizar riesgos y asignar presupuesto

Revisar reportes mensuales e incidentes críticos

Integrantes sugeridos:

Director General.

Director de TIC.

Oficial de Seguridad de la Información (OSI).

Líder de Talento Humano.

Representante médico-asistencial.

Roles y Responsabilidades Detalladas

Oficial de Seguridad de la Información (OSI)

Responsabilidades:

Liderar el Plan Director de Ciberseguridad.

Definir políticas, estándares y procedimientos.

Gestionar incidentes de seguridad.

Supervisar el cumplimiento normativo (Habeas Data, sistemas de historia clínica, etc.).

Coordinar auditorías internas y externas.

Diseñar e impartir programas de capacitación.

Departamento de TI

Responsabilidades:

Implementar controles técnicos (antivirus, firewalls, backups, actualizaciones).

Administrar accesos y permisos.

Ejecutar planes de continuidad y recuperación ante desastres.

Monitoreo constante de la red.

Reportar incidentes al OSI.

Talento Humano

Responsabilidades:

Registrar y verificar la participación en las capacitaciones.

Incluir ciberseguridad en la inducción y reinducción.

Aplicar medidas disciplinarias en caso de incumplimientos.

Generar campañas internas de sensibilización.

Personal Asistencial

Responsabilidades:

Cumplir las políticas de acceso seguro a la historia clínica.

No compartir usuarios ni contraseñas.

Reportar incidentes o comportamientos sospechosos.

Proteger dispositivos móviles con información sensible.

Personal Administrativo

Responsabilidades:

Manejar información de pacientes con confidencialidad.

Verificar la autenticidad de correos y documentos.

Evitar el uso de dispositivos externos no autorizados.

Cumplir políticas de escritorio limpio y pantalla bloqueada.

Proveedores y Contratistas

Responsabilidades:

Firmar acuerdos de confidencialidad.

Cumplir normas de seguridad de la IPS.

Notificar incidentes relacionados con servicios prestados.

Procesos de Capacitación y Sensibilización en Ciberseguridad

Capacitación Inicial (Inducción)

Duración: 2 horas

Responsable:

OSI + Talento Humano

Temas:

- Políticas de Seguridad de la IPS
- Manejo seguro de la historia clínica electrónica
- Uso seguro del correo corporativo
- Identificación de phishing
- Procedimiento para reportar incidentes

Capacitación Periódica (Trimestral)

- Modalidad:

Presencial o virtual

Temas:

- Nuevas amenazas y casos reales en el sector salud
- Ingeniería social en IPS
- Gestión segura de contraseñas
- Seguridad en telemedicina
- Buenas prácticas en dispositivos móviles

Campañas de Sensibilización

Frecuencia: Mensual

Canales: Carteleras, correo interno, WhatsApp corporativo

Ejemplos:

- Semana "Cuidado con el Phishing"
- Concurso “Contraseña más segura”
- Infografías sobre uso seguro de la historia clínica

Recordatorios de bloqueo de pantalla

Simulacros de Phishing

Frecuencia: Bimensual

Objetivos:

Medir el nivel de riesgo por ingeniería social

Identificar usuarios vulnerables

Redirigir a capacitaciones correctivas

Capacitación Técnica (para TIC)

Frecuencia: Semestral

Temas:

Forensia digital

Gestión de incidentes

Hardening de servidores y redes

Seguridad en nube

Gestión de parches y vulnerabilidades

Procesos Operativos del Plan Director

Gestión de Incidentes

Identificación

Contención

Erradicación

Recuperación

Lecciones aprendidas

Tiempo máximo de reporte: 30 minutos

Gestión de Accesos

Alta de usuarios: 24 horas

Baja inmediata al retiro

Revisión de permisos cada 3 meses

Prohibición de cuentas compartidas

Respaldo y Recuperación

Copias de seguridad diarias

Verificación semanal de integridad

Pruebas de restauración trimestrales

Actualización y Parches

Actualizaciones críticas en menos de 72 horas

Registro documentado de versiones del sistema

Formato de reporte de incidentes

Política de contraseñas

Procedimiento de acceso a historia clínica

Acuerdo de confidencialidad para personal y contratistas

Manual Institucional de Ciberseguridad de la IPS

Plan Director – Roles, Responsabilidades, Procesos y Capacitación

Presentación del Manual

La IPS, como Institución Prestadora de Servicios de Salud, reconoce la importancia de proteger la información clínica, administrativa y operativa, así como la responsabilidad de garantizar la disponibilidad, integridad, confidencialidad y trazabilidad de los datos.

El presente Manual Institucional de Ciberseguridad establece las directrices, funciones y procesos necesarios para la operación segura y cumplimiento normativo.

Objetivo General

Implementar un programa institucional de ciberseguridad que permita gestionar los riesgos tecnológicos, fortalecer la cultura de seguridad y proteger los activos de información de la IPS mediante controles organizacionales, tecnológicos y de capacitación continua.

Alcance

El manual aplica a todos los colaboradores, contratistas, estudiantes en práctica, proveedores, aliados estratégicos y cualquier persona que maneje información o sistemas pertenecientes a la IPS.

Principios Rectores de Ciberseguridad en la IPS

Confidencialidad: La información solo puede ser accedida por personal autorizado.

Integridad: La información debe permanecer completa, sin alteraciones no autorizadas.

Disponibilidad: La información y sistemas deben estar accesibles para quienes lo requieran.

Trazabilidad: Toda acción debe poder ser auditada.

Legalidad: Cumplimiento de la Ley 1581 de 2012, Decreto 1377 de 2013 y normatividad del sector salud.

Responsabilidad: Cada colaborador es parte activa de la seguridad institucional.

Estructura de Gobierno de Ciberseguridad

Comité de Ciberseguridad de la IPS

Oficial de Seguridad de la Información (OSI)

Área de Tecnología e Infraestructura

Talento Humano

Personal Asistencial y Administrativo

Política Institucional de Ciberseguridad

La IPS adopta una política basada en los siguientes pilares:

1. Protección de activos de información

2. Gestión de riesgos tecnológicos

3. Educación y cultura organizacional

4. Respuesta y recuperación ante incidentes

5. Mejora continua

El incumplimiento de la política será sujeto a acciones disciplinarias internas y/o responsabilidades legales. Incorpora un plan de seguimiento trimestral y estrategia de sensibilización: “Se desarrollarán campañas trimestrales de capacitación en temas de ciberseguridad, buenas prácticas de uso de contraseñas y prevención de phishing.”

MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA

MA-Políticas Seguridad TICs IPS.docx

Conclusiones

Identificación integral de vulnerabilidades

El análisis realizado con base en los estándares ISO/IEC 27032, ISO/IEC 27001, ISO/IEC 27001:2022 y la metodología MAGERIT permitió identificar de manera precisa múltiples fallas en la seguridad informática de la IPS, especialmente en los procesos de cifrado, control de accesos, manejo de historias clínicas, administración de bases de datos, políticas internas de seguridad, infraestructura de red y equipos de cómputo, estas brechas representan riesgos significativos para la confidencialidad, integridad y disponibilidad de los activos críticos.

Insuficiencia de controles y ausencia de un marco de gestión

El estudio evidenció que la organización no cuenta con controles formalizados ni suficientemente robustos para proteger la información sensible de los pacientes, la ausencia de políticas claras, protocolos de acceso y mecanismos de monitoreo demuestra la necesidad de establecer un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con estándares internacionales.

Exposición de datos sensibles y riesgos operativos

Las deficiencias encontradas en las historias clínicas electrónicas, bases de datos y equipos de cómputo incrementan el riesgo de accesos no autorizados, pérdida o manipulación de información y posibles incidentes de ciberseguridad compromete no solo la continuidad del servicio, sino también la privacidad de los pacientes y la responsabilidad legal de la IPS.

Necesidad de fortalecer la ciberseguridad organizacional

Al confrontar el estado actual de la IPS con las buenas prácticas planteadas por la ISO/IEC 27032 y el marco de riesgos definido por MAGERIT, se concluye que es imprescindible adoptar

un enfoque más maduro y estructurado de la ciberseguridad, orientado a la gestión de amenazas modernas y la protección de la infraestructura tecnológica crítica.

Pertinencia y urgencia de un Plan Director de Seguridad

Los resultados demuestran que la implementación de un Plan Director de Seguridad es esencial para la IPS, ya que permitirá establecer una hoja de ruta estratégica que priorice los activos críticos, defina controles técnicos y administrativos, asigne responsabilidades y garantice un proceso de mejora continúa alineado con ISO/IEC 27001:2022.

Alineación futura con estándares internacionales

La adopción de un Plan Director de Seguridad basado en los estándares ISO no solo mitigará los riesgos identificados, sino que también facilitará la futura certificación del SGSI, mejorará la cultura organizacional respecto a la seguridad de la información y fortalecerá la confianza de los usuarios y entidades regulatorias.

Impacto positivo esperado

Implementar un marco sólido de seguridad permitirá optimizar la protección de datos personales, garantizar la trazabilidad de los accesos a la información clínica, reducir la probabilidad de incidentes de ciberseguridad y asegurar la continuidad de los servicios asistenciales, generando un impacto directo en la calidad y seguridad del servicio prestado por la IPS.

Recomendaciones

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022

Establecer políticas, procedimientos, roles y responsabilidades que permitan gestionar la seguridad de la información bajo un enfoque sistemático y auditable con seguimiento constante.

Poner en marcha el Plan Director de Seguridad, debe incluir prioridades, cronogramas, recursos, indicadores y mecanismos de seguimiento para asegurar la mejora continua y la reducción progresiva de brechas.

Fortalecer los mecanismos de control de acceso

Implementar autenticación multifactorial (MFA).

Definir perfiles de acceso según roles (RBAC).

Garantizar el registro y monitoreo de accesos a sistemas críticos.

Mejorar los procesos de cifrado y protección de datos

Utilizar estándares robustos de cifrado para bases de datos, respaldos y comunicaciones.

Cifrar obligatoriamente la información sensible en tránsito y en reposo.

Actualizar y formalizar políticas internas de seguridad

Crear o reforzar políticas como:

Política de uso aceptable.

Política de contraseñas.

Política de gestión de incidentes.

Política de continuidad del negocio y respaldo de información.

Optimizar la seguridad de las historias clínicas electrónicas y bases de datos

Implementar auditorías periódicas de integridad.

Garantizar la trazabilidad completa de modificaciones.

Restringir estrictamente el acceso según funciones.

Fortalecer la infraestructura de red

Segmentar la red para aislar sistemas críticos.

Utilizar firewalls, IDS/IPS y herramientas de monitoreo continuo.

Actualizar equipos de red y aplicar parches de seguridad regularmente.

Renovar y asegurar los equipos de cómputo

Establecer un inventario actualizado.

Aplicar políticas de protección de endpoints, antivirus/EDR y parches automáticos.

Sustituir equipos obsoletos o sin soporte.

Capacitar al personal en seguridad de la información

Realizar programas de formación continua sobre buenas prácticas, phishing, manejo seguro de datos y protocolos de incidentes.

Referencias Bibliográficas

ACHC. (2023). Big data en salud: Cómo va su desarrollo en Colombia. Revista Hospitalaria del Sector Salud. https://revistahospitalaria.org/ ...Aguado, V. (2023, 27 de septiembre). Seguridad de los datos en la salud digital. Tecsens. https://www.tecsens.com/seguridad-de-los-datos-en-la-salud-digital/

Agueda-Muñoz-del-Carpio-Toia, R., 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. (s. f.). Revista Hospitalaria del Sector Salud. 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). National Institute of Standards and Technology. https://www.nist.gov/cyberframework

Gobernanza de datos en salud: Ética, privacidad y seguridad: Parte 1. (2022). [Video]. YouTube. https://www.youtube.com/watch?v=w-REx81CKhE

Gómez, S. S. (2023, 12 de julio). 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. 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.

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

ISO - International Organization for Standardization. (s. f.). 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. (2012). Diario Oficial de la República de Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Organización Panamericana de la Salud. (2023). Seguridad de la información (OPS/OMS).

Peña, K. I. C., & Montenegro 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 / Revista de Direito, Estado e Telecomunicações, 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. (s. f.). Asociación Colombiana de Instituciones de Salud (ACIS). 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, 19 de marzo). 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, 23 de abril). Los datos en el sector salud. 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. https://journal.ahima.org/page/solutions-for-challenges-in-telehealth-privacy-and-security

Apéndice

Apéndice A

Contrato Empresa de Internet Seguro

CONTRATO PARA LA PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES Y SERVICIOS CONEXOS CELEBRADO ENTRE COLOMBIA TELECOMUNICACIONES S.A. ESP Y ASOCIACION DE SERVICIOS EN SALUD OCUPACIONAL ASSOC SAS

No: 00142344

Contrato con la empresa Telefónica con tráfico seguro. Fuente propia

Apéndice B

5 Claves para Mejorar tu Ciberseguridad

5 claves de ciberseguridad que nos servirán para nuestra vida.

Apéndice C

Plantilla de Lista de Verificación de la Norma ISO 27001

PLANTILLA DE LISTA DE VERIFICACIÓN DE LA ISO 27001

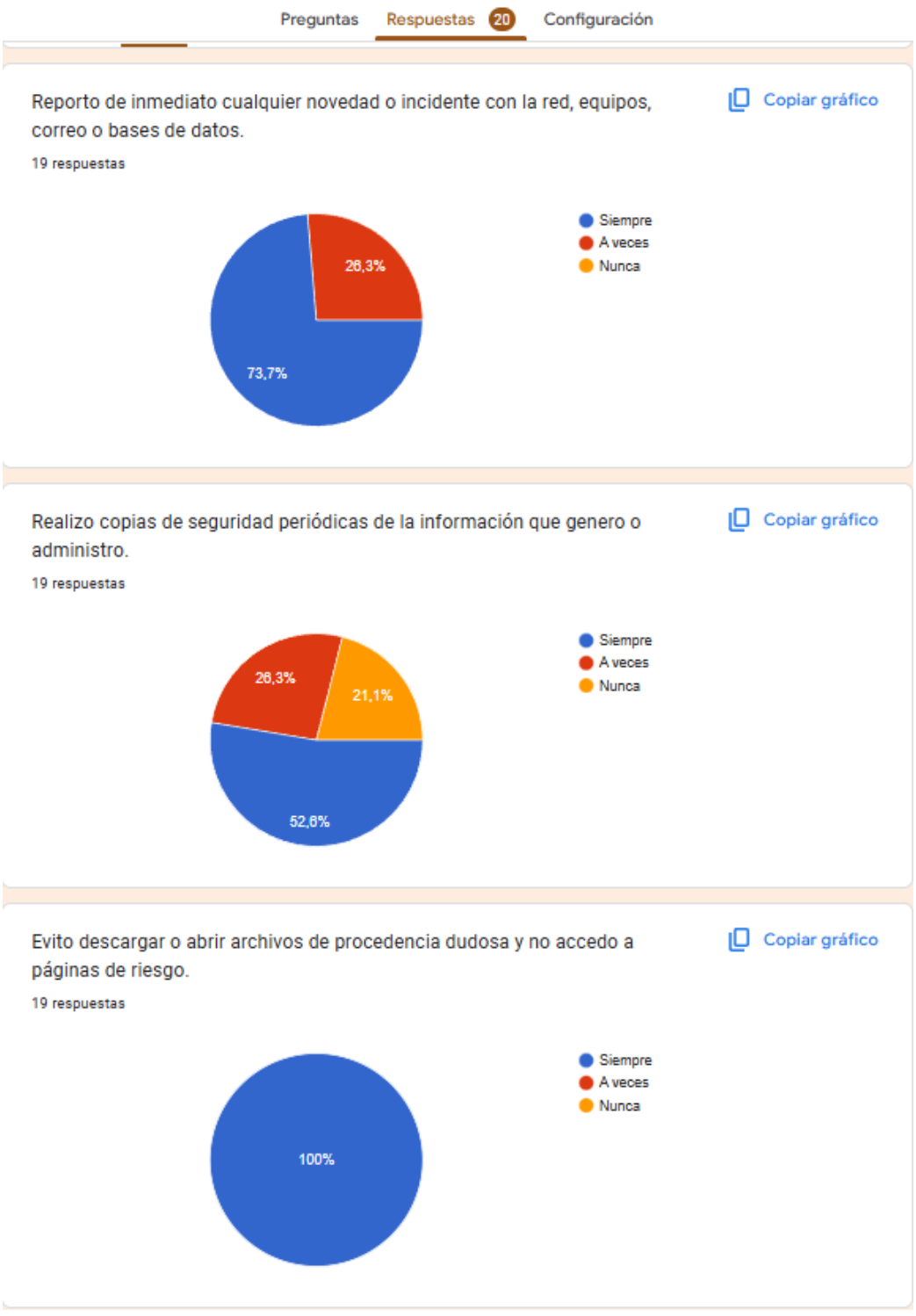
Pruebe smartsheet gratis

CONTROL DE LA ISO 27001	FASES DE IMPLEMENTACIÓN	TAREAS	¿CONFORME?	NOTAS
5	*Políticas de seguridad de la información*			
5.1	**Dirección de gestión para la seguridad de la información**			
5.1.1	Políticas de seguridad de la información	¿Existen políticas de seguridad?		
		¿Todas las políticas están aprobadas por el equipo directivo?		
		¿Prueba del cumplimiento?		
6	*Organización de seguridad de la información*			
6.1	**Roles y responsabilidades de seguridad de la información**			

Lista de verificación de las normas ISO 27001.

Apéndice D

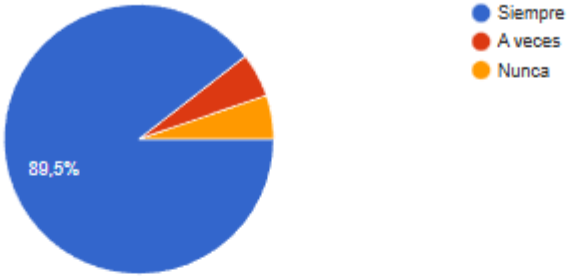
Resultados Encuestas



Solicito el aval del Coordinador TICs antes de adquirir o instalar hardware o software.

Copiar gráfico

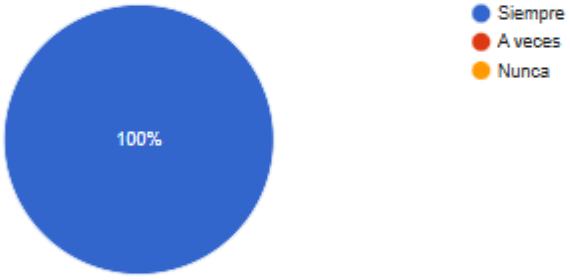
19 respuestas



Uso únicamente software con licencia entregado/validado por la empresa y no instalo software personal.

Copiar gráfico

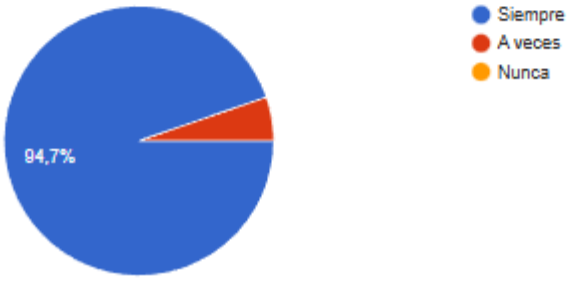
19 respuestas



Protejo mis credenciales (usuario y contraseña): no las comparto y mantengo una identidad única de acceso.

Copiar gráfico

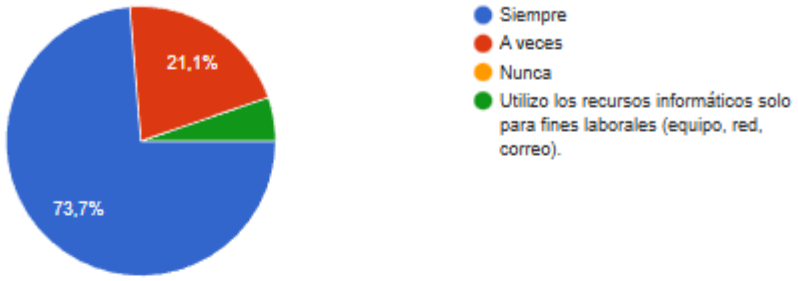
19 respuestas



Utilizo los recursos informáticos solo para fines laborales (equipo, red, correo).

Copiar gráfico

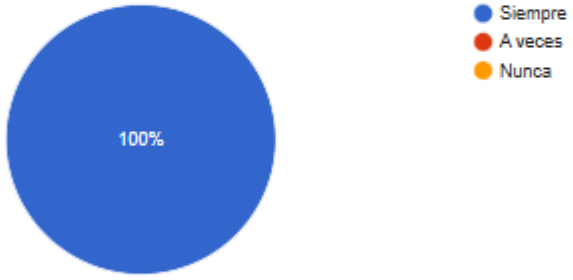
19 respuestas



No conecto equipos o módems no autorizados y me conecto solo por los medios definidos por la organización.

Copiar gráfico

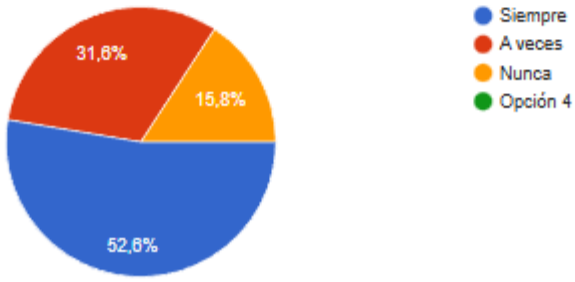
19 respuestas



No almaceno datos personales o sensibles en el disco local de mi computador de trabajo.

Copiar gráfico

19 respuestas



Resumen de encuesta interna en la IPS. Fuente propia