Diseñar un Sistema de Gestión de Seguridad de la Información para el Hospital San Rafael de Pasto, Basado en la ISO 27001:2022

Sandra Jimena Burbano Meza

Asesor

Eduardo Antonio Mantilla Torres

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática Pasto

2025

Dedicatoria

Con amor dedico este trabajo a mi hija y esposo, que con su carisma y comprensión me acompañan en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones de madre y esposa, también lo dedico a mi mamá que, con su apoyo, consagración y paciencia disminuyo mis tareas en el hogar permitiéndome una entrega más tranquila en el estudio y trabajo.

Agradecimientos

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

Resumen

El proyecto plantea el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2022 para el Hospital San Rafael de Pasto, con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información. Esta iniciativa busca mitigar riesgos de seguridad, garantizar el cumplimiento de normativas internacionales y fortalecer la confianza de pacientes y colaboradores en los procesos del hospital.

Para su desarrollo, se emplea un enfoque sistemático basado en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar) y la metodología MAGERIT, la cual permite identificar, analizar y gestionar los riesgos asociados a los activos críticos del hospital, como sistemas de información, bases de datos, dispositivos de red y servidores. Se inicia con una auditoría inicial para evaluar el estado actual del SGSI, seguida por un análisis detallado de riesgos, la definición de políticas de seguridad y la elaboración de documentación clave.

Entre los hallazgos relevantes se identifican activos críticos cuya seguridad es prioritaria para garantizar la continuidad operativa. Las principales amenazas incluyen ciberataques, pérdida de información y vulnerabilidades en sistemas tecnológicos. Para mitigar estos riesgos, se proponen controles como la implementación de respaldos, políticas de acceso y mecanismos de monitoreo continuo.

La implementación del SGSI permitirá al hospital gestionar eficazmente los riesgos de seguridad, mejorar la resiliencia frente a incidentes y promover una cultura organizacional orientada a la ciberseguridad. Además, refuerza su posición como referente en seguridad de la información en el sector salud, garantizando la confianza de sus grupos de interés y la continuidad de los servicios médicos.

Palabras claves: Activos críticos, Análisis de riesgos, Auditoría inicial, Bases de datos, Ciberataques.

Abstract

The project proposes the design and implementation of an Information Security Management System (ISMS) based on the ISO 27001:2022 standard for the San Rafael Hospital in Pasto, with the objective of protecting the confidentiality, integrity, and availability of information. This initiative seeks to mitigate security risks, ensure compliance with international regulations, and strengthen patient and collaborator confidence in the hospital's processes.

For its development, a systematic approach is employed based on the PDCA cycle (Plan, Do, Check, Act) and the MAGERIT methodology, which allows for identifying, analyzing, and managing risks associated with the hospital's critical assets, such as information systems, databases, network devices, and servers. It begins with an initial audit to evaluate the current state of the ISMS, followed by a detailed risk analysis, definition of security policies, and preparation of key documentation.

Among the relevant findings, critical assets have been identified whose security is a priority to guarantee operational continuity. The main threats include cyberattacks, information loss, and vulnerabilities in technological systems. To mitigate these risks, controls are proposed such as the implementation of backups, access policies, and continuous monitoring mechanisms.

The implementation of the ISMS will allow the hospital to effectively manage security risks, improve resilience against incidents, and promote an organizational culture oriented towards cybersecurity. Additionally, it reinforces its position as a reference in information security in the healthcare sector, ensuring the trust of its stakeholders and the continuity of medical services.

Keywords: Critical assets, Risk analysis, Initial audit, Databases, Cyberattacks, Cybersecurity

Tabla de Contenido

Pág.

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

La seguridad de la información es un aspecto crítico en el sector de la salud, ya que impacta directamente la privacidad de los pacientes, la continuidad y eficiencia de los servicios médicos. En la era digital actual, donde la tecnología y los datos digitales desempeñan un papel cada vez más central, proteger la información confidencial se ha convertido en una prioridad estratégica para las organizaciones de salud. En este contexto, el Hospital San Rafael de Pasto ha reconocido la importancia de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2022. Esta norma internacional proporciona un marco sistemático y estructurado para la gestión de la seguridad de la información, permitiendo a las organizaciones identificar, gestionar y reducir los riesgos asociados a la información de manera efectiva.

El principal objetivo del SGSI es garantizar la protección de la información confidencial de los pacientes, y mejorar la continuidad de los servicios médicos. La norma ISO 27001:2022 establece los requisitos necesarios para la implementación de un SGSI efectivo, incluyendo la evaluación de riesgos, el establecimiento de políticas y controles de seguridad, y la mejora continua del sistema. Para su implementación, el Hospital utilizará la metodología Magerit, una herramienta ampliamente reconocida para el análisis y gestión de riesgos de seguridad de la información. Esta permitirá al hospital identificar y valorar los activos de información, analizar las amenazas y vulnerabilidades, y establecer las medidas de control adecuadas para mitigar los riesgos identificados. Además, el SGSI se desarrollará siguiendo el ciclo de mejora continua Planificar-Hacer-Verificar-Actuar (PHVA). Este enfoque sistemático garantizará que el sistema se planifique e implemente de manera efectiva, verificando su eficacia y realizando acciones correctivas y preventivas para lograr una mejora continua. La adopción de un SGSI basado en la norma ISO

27001:2022, utilizando la metodología Magerit y el ciclo PHVA, demuestra el compromiso del Hospital con la seguridad de la información y la protección de los datos sensibles de sus pacientes. Esta iniciativa permitirá al hospital fortalecer su posición y confianza en el sector de la salud, al tiempo que cumple con las regulaciones y estándares internacionales en materia de seguridad de la información.

Definición del Problema

La seguridad de la información en el sector salud ha cobrado importancia crucial en los últimos años, debido al aumento exponencial de la digitalización de registros médicos y la interconexión de sistemas. El Hospital como muchas instituciones de salud, enfrenta desafíos significativos para proteger la información confidencial de sus pacientes. Este problema puede analizarse desde tres contextos: el incremento de ciberataques, la evolución de normativas de seguridad y la necesidad de un enfoque sistemático en gestión de riesgos.

Aumento de los Ciberataques en el Sector Salud

En los últimos años, el sector salud se ha convertido en un blanco prioritario para los ciberataques. Los atacantes cibernéticos buscan información médica debido a su alto valor en el mercado negro y la posibilidad de extorsionar a las instituciones. En Colombia, los ciberataques a entidades de salud han mostrado un incremento notable. Según informe IBM (2024) *X-Force Threat Intelligence Index 2024*. IBM Security Intelligence, el país ha sido uno de los más afectados en Latinoamérica, con numerosos incidentes que han comprometido la seguridad de datos críticos y la operatividad de los servicios de salud.

Aquí algunos casos importantes que destacar:

Ataque al Instituto Nacional de Salud (INS)

El Instituto Nacional de Salud (INS) (2023) sufrió un ataque cibernético que comprometió varios de sus sistemas informáticos. Los atacantes accedieron a datos sensibles y afectaron la capacidad del INS para realizar algunas de sus funciones críticas, como el monitoreo epidemiológico y la gestión de información sobre la pandemia de COVID-19 (Sáenz, 2025).

La interrupción de los servicios y la posible exposición de datos confidenciales tuvieron un impacto significativo en la respuesta sanitaria del país. El incidente resaltó la necesidad de mejorar las defensas cibernéticas y la resiliencia de los sistemas de salud pública.

Incidente en la EPS Sura

En junio de 2022, EPS Sura, una de las principales Entidades Promotoras de Salud de Colombia, sufrió un ataque cibernético que afectó sus sistemas de TI. Los atacantes lograron acceder a datos personales y médicos de miles de afiliados, lo que provocó una crisis de confianza entre los usuarios (Hyperconectado, 2023).

La brecha de datos llevó a una investigación profunda y a la implementación de medidas adicionales de seguridad. EPS Sura tuvo que invertir significativamente en mejorar sus defensas cibernéticas y en ofrecer servicios de monitoreo de crédito a los afectados (Pinzón, 2022).

Ataque al Ministerio de Salud y Protección Social

En noviembre de 2023, el Ministerio de Salud y Protección Social de Colombia fue blanco de un ataque cibernético que resultó en la interrupción temporal de varios de sus servicios en línea. El ataque afectó la disponibilidad de sistemas utilizados para la gestión de datos de salud y la coordinación de servicios médicos a nivel nacional.

La interrupción de los servicios digitales del Ministerio causó retrasos en la atención sanitaria y dificultó la gestión de recursos en tiempo real. Este incidente destacó la importancia de tener planes de contingencia y sistemas de respaldo robustos para asegurar la continuidad operativa en el sector salud. (Revista Semana, 2023).

Ataque Cibernético a Sanitas en 2022

En noviembre de 2022, Sanitas sufrió un ataque cibernético significativo que afectó sus sistemas de información y comprometió datos sensibles de sus afiliados. Los atacantes lograron infiltrarse en la red de Sanitas, accediendo a información personal y médica de miles de pacientes.

El ataque provocó la interrupción temporal de varios servicios digitales de Sanitas, incluyendo la programación de citas, acceso a historiales médicos y la administración de tratamientos. Esto causó retrasos y complicaciones en la atención médica de los pacientes.

Se expusieron datos personales y médicos sensibles, como nombres, direcciones, números de identificación, y detalles de tratamientos médicos. Esta brecha de seguridad puso en riesgo la privacidad y seguridad de los pacientes.

Sanitas tuvo que activar planes de contingencia, utilizando métodos manuales y sistemas de respaldo para continuar operando. Además, la organización trabajó en colaboración con expertos en ciberseguridad y autoridades para contener el ataque y mitigar sus efectos.

La brecha de seguridad afectó la confianza de los pacientes en Sanitas, llevando a una pérdida de reputación. La organización también enfrentó posibles consecuencias legales y regulatorias debido a la exposición de datos sensibles.

Estos incidentes exponen la importancia de fortalecer las medidas de ciberseguridad en el sector de salud de Colombia. Implementar un SGSI (Sistema de Gestión de Seguridad de la Información)

bien diseñado es crucial para proteger la información sensible de los pacientes, garantizar la continuidad de los servicios médicos y mitigar los riesgos asociados con los ciberataques. Esto no solo protege a las instituciones y a los pacientes, sino que también

mantiene la confianza pública y cumple con las regulaciones y leyes aplicables (Intobae, 2023).

Evolución de Normativas y Estándares de Seguridad

Con la creciente amenaza de ciberataques, las normativas y estándares internacionales sobre la seguridad de la información han evolucionado para proporcionar guías más robustas y específicas. La ISO 27001:2022 es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Este estándar se ha convertido en una referencia fundamental para las organizaciones que buscan proteger sus activos de información de diversas amenazas, garantizando la confidencialidad, integridad y disponibilidad de los datos.

Necesidad de un Enfoque Sistemático en la Gestión de Riesgos

La gestión de la seguridad de la información en un hospital implica enfrentar una variedad de riesgos que van desde amenazas internas, como errores humanos y mal uso de sistemas, hasta amenazas externas, como ataques cibernéticos y desastres naturales. Para abordar estos riesgos de manera efectiva, es esencial adoptar un enfoque sistemático que permita identificar, evaluar y mitigar las amenazas de manera proactiva (Alvarado, sf).

El Hospital comprometido a implementar un SGSI que permita gestionar la seguridad de la información de manera integral, proporcionando un marco para la identificación de riesgos, la implementación de controles de seguridad, y la mejora continua a través de auditorías y revisiones periódicas, así se puede garantizar la protección de la información sensible de los pacientes y la continuidad de los servicios críticos (Ingenio Learnig, 2022).

Casos y Estudios Previos

Numerosos estudios y casos previos en el sector salud han demostrado la eficacia de implementar un SGSI basado en la ISO 27001. Instituciones que han adoptado estos sistemas han mostrado mejoras significativas en la protección de datos, reducción de incidentes de seguridad, y una mayor confianza por parte de los pacientes y partes interesadas. Estos ejemplos proporcionan una base sólida para el Hospital, que puede aprender de estas experiencias y adaptar las mejores prácticas a su propio contexto (Quodem, 2024).

Formulación del Problema

¿Cómo el diseño de un SGSI puede minimizar los riesgos de seguridad de la información en el Hospital San Rafael de Pasto?

Justificación

La Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el Hospital San Rafael de Pasto, constituye una medida clave para asegurar la confidencialidad, integridad y disponibilidad de la información, en concordancia con los lineamientos establecidos por la norma ISO/IEC 27001:2022. Este sistema no solo busca reforzar la seguridad de los activos de información, sino también responder de forma específica a los requerimientos del sector hospitalario en salud mental, donde la confidencial de la información exige un enfoque preventivo.

Con esta implementación, se prevé una disminución del 30% en eventos de seguridad relacionados con accesos indebidos durante el primer año, así como un mejoramiento del 40% en la implementación de controles establecidos en el anexo A de la norma ISO/IEC 27001:2022, conforme a los resultados de auditorías internas. Asimismo, se proyecta que el 100% del personal este debidamente capacitado en políticas de seguridad de información.

En el área académica, este proyecto ofrece la oportunidad de aplicar conocimientos importantes sobre cómo identificar y manejar riesgos, cumplir con las normas legales, y proteger la información digital, enfocados específicamente en el sector salud. La combinación de seguridad informática, principios éticos de la medicina y leyes actuales, como la Ley 1581 de 2012 sobre protección de datos personales, ayuda a fortalecer el manejo responsable de la información dentro de las instituciones.

Desde el punto de vista social, la implementación del sistema consolidará la confianza entre los pacientes y los profesionales de la salud, al garantizar que la información clínica, psicológica y personal sea manejada bajo estrictos estándares de

confidencialidad. Esta confianza es crítica para el desarrollo terapéutico y la eficacia de los procesos de recuperación.

Adicionalmente, la ubicación geográfica del hospital en Pasto, una ciudad intermedia con limitaciones en infraestructura tecnológica frente a los grandes centros urbanos agrega un valor diferencial al proyecto. La puesta en marcha del SGSI permitirá al Hospital posicionarse como un referente regional en gestión de la seguridad de la información en Colombia, especialmente considerando que, según el informe *IBM X-Force Threat Intelligence Index 2024,* Colombia ha sido uno de los países más vulnerables a ciberataques en América Latina.

Desde el punto de vista operativo, este sistema ayudará a prevenir y manejar situaciones que puedan interrumpir el funcionamiento del hospital, como la pérdida de acceso a las historias clínicas o fallas en los sistemas que apoyan la atención médica. Para esto, se implementarán medidas tecnológicas y normativas que aseguren que los servicios más importantes del hospital puedan continuar incluso en caso de incidentes o problemas de seguridad.

Por último, llevar a cabo este proyecto es una gran oportunidad de crecimiento profesional, ya que implica liderar un proceso que requiere conocimientos en seguridad de la información, manejo de normas internacionales actualizadas y experiencia en la gestión de proyectos tecnológicos que afectan directamente el funcionamiento del Hospital.

Figura 1

Partes Interesadas

GRUPO DE INTERÉS	PARTE INTERESADA
ORDEN HOSPITALARIA DE SAN JUAN DE DIOS	Comunidad de hermanos Hospitalarios
CURIA PROVINCIAL	Junta Directiva
COLABORADORES	Colaboradores y sus familias
USUARIOS	Pacientes
	Entidades Contratantes (EPS, subsidiado, contributivo, régimen especial / Cliente Institucional)
PROVEEDORES / CONTRATISTAS	Proveedores: Casas comerciales de materias primas, Proveedores insumos y suministros, dotación hospitalaria, medicamentos, Software, servicio (Recolección de residuos hospitalarios y peligrosos-laboratorios-Ambulancia urgencias, Mantenimiento y Calibración de equipos biomédicos, Aseguradoras
	Contratistas: Alimentación hospitalaria, Aseo, vigilancia, calibración y mantenimiento de equipos, dotación de personal
ENTIDADES REGULATORIAS	Entes de vigilancia y control: INVIMA, Superintendencia Nacional de Salud, Personería, Procuraduría, Contraloría, Ministerio de salud, Instituto departamental de Salud, secretaria de salud, secretaria de gestión ambiental, etc.
	Entidades y otros sectores: Cámara de comercio, DIAN, IDEAM, Autoridad Ambiental (CORPONARIÑO), Ministerio de Trabajo, Fondo de atención y prevención de emergencias, bomberos, entre otros
	Normas Técnicas Colombianas
COMUNIDAD LOCAL Y LOS VECINOS	Hospital San Pedro
	Barrio San Juan de Dios
	Barrio torres de Mariluz
	Corregimiento de Mapachico
	Bodegas de Puyo
	Universidad Mariana (campo Alvernia)
	Comunidad Hermanos Jesuitas
ONG O GRUPOS DE PRESIÓN	Red global de hospitales verdes y saludables
	Organizaciones de derechos humanos (víctimas del conflicto armado)
	Medios de comunicación
	Personería y defensoría del pueblo
COMPETENCIA	Hospital Perpetuo Socorro

Nota. Figura tomada del documento “Objetivos estratégicos”, elaborado por el Hospital San Rafael de Pasto, 2019.

Objetivos

Objetivos General

Diseñar un Sistema de Gestión de Seguridad de la Información, basado en ISO 27001 :2022, para proteger la confidencialidad, integridad y disponibilidad de la información de los pacientes, y dar continuidad a los servicios prestados.

Objetivos Específicos

Realizar una auditoría inicial, mediante la revisión documental, para identificar el estado actual de implementación del SGSI.

Evaluar los riesgos, mediante la metodológica MAGERIT para el Hospital San Rafael de Pasto

Proponer una política y objetivos de seguridad de la información, tomando como base la ISO27001 :2022.

Elaborar la documentación requerida para la implementación del SGSI

Marco Teórico

Antecedentes de la Investigación

Uno de los principales retos que siempre están presentes en el manejo de datos e información es el cumplimiento de tres pilares fundamentales que permiten la seguridad informática en un SGSI, garantizando el acceso a la información de los usuarios que se encuentran autorizados para este fin, preservando la información completa y exacta al igual que dar garantía de que el usuario posee la capacidad de acceder a la información que necesita en el momento preciso.

Diversos estudios recientes confirman la efectividad de estos sistemas. Por ejemplo, Díaz, M., Herrera, J., & López, R. (2021), en su estudio "Implementación De Un Sgsi En Instituciones Educativas: Análisis De Efectividad Y Desafíos En Entornos Académicos" demostraron que la implementación de un SGSI permitió mejorar los tiempos de respuesta ante incidentes y fortalecer la trazabilidad en el acceso a información crítica. No obstante, identificaron como debilidad la limitada adopción cultural entre el personal y la escasa integración con sistemas legados.

Asimismo, González, L., & Ramírez, P. (2022), en su investigación "Gestión De Riesgos En Hospitales Públicos: Evaluación Del Impacto Del Sgsi En Instituciones Del Sector Salud" evidenciaron en hospitales públicos una reducción del 28 % en incidentes de seguridad tras implementar un SGSI. Sin embargo, también reportaron la necesidad de fortalecer la formación continua y la gestión del cambio institucional.

Una observación crítica frecuente en la literatura especializada es el uso exclusivo del marco ISO/IEC 27001, sin considerar modelos complementarios. En este sentido, Lozano, S. & Restrepo, M. (2021), en su artículo "Comparación Entre Nist, Iso 27001 Y Octave: Análisis Metodológico Para Entornos Críticos" subrayan que el marco NIST SP

800-53 Rev. 5, desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), aporta un conjunto exhaustivo de controles técnicos y administrativos, aplicables principalmente en infraestructuras críticas.

Por su parte, Pérez, A. & Medina, F. (2022), en su trabajo de grado “Aplicación De Octave En Instituciones De Salud: Evaluación Participativa Del Riesgo En Entornos Clínicos”, Describen Cómo La Metodología Octave Allegro, desarrollada por Carnegie Mellon University, permite un análisis cualitativo del riesgo que involucra activamente a múltiples áreas organizacionales. Este enfoque facilita una comprensión más profunda de los impactos operativos, más allá de los aspectos puramente tecnológicos. Su enfoque organizacional permite comprender los impactos más allá del componente tecnológico.

En esta línea, Ramírez, J., Gutiérrez, C., & Paredes, D. (2021), en su estudio “Propuesta De Integración De Iso/Iec 27001 Y Nist Sp 800-53 En Entornos Hospitalarios” proponen una integración estratégica entre ISO 27001, NIST y OCTAVE, con el fin de optimizar la cobertura de controles, fomentar una cultura de seguridad y consolidar procesos sostenibles de gestión del riesgo

Bases Teóricas

Sistema de gestión de la seguridad de la información: Dentro de la norma ISO 27001 está estipulado que, un SGSI ayuda a establecer estas políticas y procedimientos en relación con los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente (Icontec, 27001).

Igualmente, para Doria, A. un SGSI es un marco de administración general a través del cual las organizaciones identifican, analizan y direccionan sus riesgos en la seguridad de la información. Su correcta implementación garantiza que los acuerdos de seguridad están afinados para mantenerse al ritmo constante con las amenazas de seguridad, vulnerabilidades e impactos en el negocio, el cual es un aspecto para considerar profundamente teniendo en cuenta la competitividad y cambios a los que enfrentan las organizaciones hoy en día.

Según la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC), la implementación de un SGSI brinda los siguientes beneficios a la organización:

Control interno: Existencia de Control Interno y dotar de un Marco de referencia con el objetivo de lograr mayor eficiencia en las operaciones; tener mayor confiabilidad de la Información Económico-Financiera, así como operativa; y adecuarse al cumplimiento de las normas y regulaciones aplicables.

Reducción de costos **:** La implantación de un SGSI incide directamente sobre los gastos económicos del Organismo en relación con una ineficiente gestión de la seguridad. En el corto plazo pueden existir costos vinculados a la implantación de controles, pero estos deben ser vistos como inversiones a mediano y largo plazo. Las implementaciones de dichos controles suelen redundar en mejoras.

Los beneficios surgen de, por ejemplo, la reducción de primas de seguros en algunas pólizas debido a la justificación de la protección de los activos asegurados, o evitando indemnizar a los usuarios por malas gestiones.

Continuidad del negocio **:** Con un SGSI en marcha se evitan interrupciones en los servicios ofrecidos, ya que se está asegurando de una manera eficaz la disponibilidad de los

activos de información y, por lo tanto, de los servicios que el organismo ofrece. Esto en cuanto a la actividad cotidiana, pero también se está preparado para recuperarse ante incidentes más o menos graves e incluso garantizar la continuidad del negocio, afrontando un desastre sin que peligre el mismo a largo plazo.

Mantener y mejorar la imagen: Los usuarios percibirán al organismo como una entidad responsable, comprometida con la mejora de sus procesos, productos y servicios. Debido a la exposición de cualquier organismo a un fallo de seguridad que pueda hacer pública información reservada o confidencial, un SGSI implantado coloca al Organismo en una posición de reconocimiento ante la ciudadanía y sus pares. Una imagen consolidada de confianza facilita la gestión general y habilita nuevas posibilidades para la toma de decisiones.

Cumplimiento legal y reglamentario**:** Día a día el marco normativo referido a seguridad de la información se afianza y consolida, en este contexto contamos con normas como: ley de protección de datos personales y acción de habeas data, y ley de acceso a la información pública. Un SGSI permite dar cumplimiento al marco normativo con mayor rapidez y eficiencia. Un logro importante para todo organismo (AGESIC, 2012).

La selección de una metodología adecuada para la gestión de la seguridad de la información debe basarse en las necesidades, el entorno regulatorio y el nivel de madurez de la organización. A continuación, se presenta una comparación estructurada entre tres enfoques ampliamente utilizados: ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5, y OCTAVE Allegro. Esta tabla analiza sus principales características, ventajas y limitaciones, con base en criterios técnicos y organizacionales relevantes

Comparación Metodológica

Figura 2

Cuadro Comparativo

Criterio	ISO/IEC 27001:2022	NIST SP 800-53 Rev. 5	OCTAVE Allegro
Enfoque	Gestión integral del riesgo basado en políticas, procedimientos y mejora continua	Basado en controles técnicos, dividido en familias de seguridad	Evaluación cualitativa del riesgo desde una perspectiva organizacional
Alcance	Aplicable a cualquier organización sin importar su tamaño o sector	Principalmente orientado a entidades gubernamentales y entornos críticos	Enfocado en organizaciones con múltiples procesos y gestión descentralizada
Participació	Alta dirección, TI y responsables de seguridad	Especialistas en ciberseguridad y equipos de cumplimiento normativo	Equipos multidisciplinarios (administración, TI, áreas operativas)
Ciclo de mej	Basado en el modelo PDCA (Planificar-Hacer-Verificar-Actuar)	Sigue el Risk Management Framework (RMF) con fases bien estructuradas	Iterativo, participativo y centrado en la evaluación de impacto de activos
Fortalezas	Reconocida internacionalmente, adaptable, permite certificación	Detallado, técnico, alineado con regulaciones de EE.UU.	Alto grado de contextualización y compromiso organizacional
Limitaciones	Puede ser generalista sin ajustes específicos si no se adapta bien	Complejo de implementar sin recursos técnicos robustos	Requiere madurez organizacional y liderazgo fuerte para ser eficaz
Enfoque	Gestión integral del riesgo	Controles técnicos y administrativos	Evaluación cualitativa del riesgo
Alcance	Multisectorial	Sector gubernamental e infraestructura crítica	Entornos con alta participación organizacional
Participació	Alta dirección y TI	Equipos especializados de seguridad	Grupos multidisciplinarios
Ciclo de mej	PDCA	RMF (Risk Management Framework)	Enfoque iterativo y colaborativo

Nota. Adaptado de “Comparativo de metodologías de análisis de riesgos”, por Pérez Gómez, 2021.

Amenaza: Evento o condición que tiene el potencial de explotar una vulnerabilidad y causar daño a los activos de información. Puede tener origen humano (errores, negligencia, ataques deliberados), natural (inundaciones, terremotos) o tecnológico (fallas en sistemas, software malicioso). Según Tarazona (2021), la identificación sistemática de amenazas permite priorizar esfuerzos de mitigación con base en su recurrencia y criticidad.

Riesgo: Combinación de la probabilidad de ocurrencia de una amenaza y el impacto que esta puede generar sobre los activos. La gestión de riesgos no elimina completamente el peligro, pero permite tomar decisiones informadas sobre su aceptación, mitigación, transferencia o evitación. UNESCO (2021) plantea que el riesgo es dinámico y debe revisarse continuamente ante cambios internos o del entorno.

Vulnerabilidad: Debilidad o fallo en el diseño, implementación o gestión de los sistemas de información que puede ser explotada por una amenaza. Estas pueden ser técnicas (puertos abiertos, software sin parches) u organizacionales (falta de capacitación, políticas inadecuadas). Fundación Carlos Slim (2021) recomienda realizar pruebas periódicas como análisis de vulnerabilidades o test de penetración para su identificación temprana.

Gestión: Conjunto de actividades planificadas para alcanzar objetivos específicos mediante el uso eficiente de recursos. En el contexto de seguridad de la información, implica coordinar controles, asignar responsabilidades y evaluar continuamente el desempeño del SGSI. Salgueiro (2021) define la gestión como el medio para asegurar que las políticas de seguridad sean aplicadas de manera eficaz y coherente.

Información: Recurso estratégico compuesto por datos estructurados que tienen valor para la organización. Es el activo central de un SGSI y puede encontrarse en múltiples formatos (digital, físico, oral). Según Chiavenato (2021), la información reduce la incertidumbre, permite la toma de decisiones acertadas y debe ser protegida conforme a su nivel de criticidad y confidencialidad.

Control: Mecanismo técnico, administrativo o físico diseñado para prevenir, detectar o responder ante incidentes de seguridad. Los controles deben seleccionarse con base en los resultados del análisis de riesgos, y pueden clasificarse en preventivos, detectivos o correctivos. La norma ISO/IEC 27002:2022 establece buenas prácticas para su aplicación efectiva en entornos organizacionales.

Continuidad del negocio: Capacidad de una organización para mantener operaciones críticas durante y después de un incidente. Un SGSI debe integrarse con planes de continuidad y recuperación ante desastres, asegurando la disponibilidad de la

información en situaciones adversas. AGESIC (2021) recomienda realizar pruebas regulares de estos planes para garantizar su eficacia operativa.

Cumplimiento normativo: Conjunto de obligaciones legales, contractuales y regulatorias que una organización debe observar respecto al tratamiento de la información. El SGSI debe facilitar el cumplimiento de leyes como la Ley 1581 de 2012 (protección de datos personales) y normas técnicas como la ISO 27001. Su observancia contribuye a evitar sanciones, preservar la reputación institucional y fomentar la confianza de los stakeholders.

Definición de Términos Básicos

Para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) se utilizan conceptos referentes a la seguridad que aplican a cualquier tipo de entidad, ya sean públicas o privadas, con o sin fines de lucro, grandes o pequeñas.

Sistema de Gestión de la Seguridad de la Información: es un conjunto de políticas, procedimientos, guías, recursos y herramientas organizadas, cuyo objetivo principal es establecer un enfoque sistemático y proactivo para gestionar y proteger la información y los activos de información de una organización.

La información se refiere a cualquier conjunto de datos organizados que posean valor para la entidad, independientemente de su forma de almacenamiento, transmisión, origen o fecha de elaboración, puede estar en formato físico (impreso, en imágenes, oral) o digital (almacenada electrónicamente, transmitida por correo electrónico, mensajería, etc.).

Según la norma ISO 27001, la seguridad de la información consiste en preservar tres principios fundamentales: la confidencialidad, la integridad y la disponibilidad, tanto de la información como de los sistemas y procesos que la manejan. Estos tres principios son la base sobre la que se sustenta la seguridad de la información:

Confidencialidad: Asegurar que la información no sea accedida, divulgada o revelada a individuos, entidades o procesos no autorizados.

Integridad: Mantener la exactitud, completitud y estado inmodificable de la información y sus métodos de procesamiento.

Disponibilidad: Garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los usuarios, entidades o procesos autorizados cuando lo requieran.

La norma ISO 27001: es un estándar internacional emitido por la Organización Internacional de Normalización (ISO) que proporciona un marco de trabajo y una metodología para implementar y gestionar un SGSI en cualquier organización, independientemente de su tamaño, sector o naturaleza. Está basada en la norma británica BS 7799-2 y su versión más reciente fue publicada en 2022 con el nombre ISO/IEC 27001:2022. Esta norma también permite que una organización obtenga una certificación formal de su SGSI por parte de una entidad de certificación independiente.

Análisis de riesgos: es un proceso fundamental dentro del SGSI, ya sea de manera cuantitativa o cualitativa, que permite evaluar e identificar los riesgos a los que están expuestos los activos de información de la organización, es el primer paso para identificar y valorar los activos a proteger.

La evaluación de riesgos implica comparar el nivel de riesgo detectado con los criterios de riesgo previamente establecidos y alcanzar un consenso sobre los objetivos y niveles de riesgo aceptables, los resultados del análisis de riesgos permiten aplicar métodos para el tratamiento de los riesgos identificados, como mitigarlos, transferirlos, aceptarlos o evitarlos.

Durante el análisis de riesgos, se deben tener en cuenta cinco elementos clave: la probabilidad de ocurrencia de un evento, las amenazas potenciales, las vulnerabilidades existentes, los activos a proteger y el impacto que tendría la materialización de un riesgo.

MAGERIT: (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) es una metodología elaborada por el Consejo Superior de Administración Electrónica de España que permite:

Estudiar y analizar los riesgos que enfrenta un sistema de información y su entorno asociado, propone realizar un análisis de riesgos que implica evaluar el impacto que una violación de seguridad tendría en la organización, identificar las amenazas presentes, determinar la vulnerabilidad del sistema ante esas amenazas y obtener resultados precisos.

Basándose en los resultados del análisis de riesgos, la gestión de riesgos puede recomendar e implementar las medidas apropiadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados, minimizando su potencial impacto y posibles daños.

La norma ISO/IEC 27001:2022 establece un ciclo de mejora continua conocido como "Planificar-Hacer-Verificar-Actuar" para la gestión efectiva de un SGSI.

Este ciclo implica las siguientes etapas:

Planificar: Consiste en planificar acciones para abordar los riesgos e identificar oportunidades de mejora, lo que incluye:

Definir las políticas de seguridad de la información

Establecer el alcance del SGSI

Realizar el análisis de riesgos

Seleccionar los controles de seguridad adecuados

Definir las competencias y responsabilidades necesarias

Establecer un mapa de riesgos

Hacer: Implica disponer de los recursos necesarios para establecer, implementar y mantener el SGSI, así como comunicar las políticas de seguridad de la información. Esto incluye:

Poner en marcha el plan de gestión de riesgos establecido

Implementar el SGSI

Establecer los controles de seguridad seleccionados

Verificar: Consiste en realizar revisiones y auditorías internas para monitorear y evaluar el desempeño del SGSI, lo que implica:

Revisar internamente el SGSI

Realizar auditorías periódicas

Revisar los indicadores y métricas de seguridad

Actuar: Basándose en los resultados de la etapa de verificación, se deben tomar acciones correctivas y preventivas para mejorar continuamente el SGSI, incluyendo:

Realizar las acciones correctivas necesarias

Implementar acciones preventivas para abordar riesgos potenciales

Este ciclo de mejora continua permite a las organizaciones adaptar y optimizar constantemente su SGSI para responder a los cambios en los riesgos, las amenazas y las necesidades de seguridad de la información.

Diseño Metodológico

La metodología formulada busca cumplir los objetivos específicos definidos, con el fin de lograr el objetivo general del trabajo de grado, teniendo en cuenta el marco de referencia de la norma NTC-ISO-IEC 27001:2022. El proyecto de diseño del SGSI se desarrollará en fases estructuradas, garantizando un enfoque sistemático y definido.

La metodología seguirá un cronograma establecido para evaluar el progreso del proyecto. Las fases principales del proyecto son: auditoría inicial, evaluación de riesgos, desarrollo de políticas y objetivos, y elaboración de la documentación necesaria.

Para la auditoria inicial, se emplearán los siguientes recursos para la recolección de datos:

Entrevistas

Revisión de la documentación existente

Observación

Las encuestas se analizarán utilizando herramientas estadísticas como y tablas que resuman los resultados.

Estos métodos permitirán obtener una visión integral y detallada de la situación actual en materia de seguridad de la información

Para la evaluación de riesgos, se aplicará la metodología MAGERIT, utilizando sus herramientas específicas para identificar y analizar activos, amenazas y vulnerabilidades.

Las mejoras propuestas al diseño del SGSI se enfocarán en establecer un sistema integral que contemple:

Políticas y Procedimientos: Se desarrollarán políticas específicas de seguridad de la información basadas en los hallazgos de la auditoría inicial y la evaluación de riesgos, alineadas con la norma ISO 27001:2022.

Capacitación y Sensibilización: Se implementará un programa de formación para el personal, asegurando que todos comprendan las nuevas políticas y procedimientos, y su importancia para la seguridad de la información.

Sistema de Monitoreo y Revisión: Se establecerá un mecanismo para la revisión continua del SGSI, asegurando que se adapte a nuevas amenazas y cambios en el entorno operativo.

Auditoria Inicial

Objetivo

Realizar una evaluación detallada del nivel de cumplimiento del proceso de Gerencia de la Información respecto a los requisitos definidos en la norma NTC-ISO-IEC 27001:2022, con el fin de, identificar el estado actual del Sistema de Gestión de Seguridad de la Información (SGSI) en el proceso de Gerencia de la Información.

Alcance

El alcance de la auditoría se aplicará al proceso de Gerencia de la Información, y se enfoca en realizar entrevista con los miembros del equipo involucrados, para evaluar el nivel de cumplimiento de la norma NTC-ISO-IEC 27001:2022 y controles según anexo A de la NTC-IEC 27001:2022

Metodología

Para evaluar el nivel de cumplimiento, se adoptará un enfoque estructurado que combina herramientas de diagnóstico, revisión documental y entrevistas con los responsables**.**

Herramientas de Evaluación

Instrumento de Evaluación de los Requisitos de la Norma

NTC-ISO-IEC 27001:2022**:** Esta herramienta mide la conformidad con los requisitos obligatorios del SGSI, aplicando una escala de madurez que permite clasificar el estado de cada control o requisito evaluado así:

Tabla 1

Instrumento de Evaluación de los Requisitos de la Norma

Estado	Significado
Desconocido	No se ha verificado el cumplimiento ni la existencia del control.
Inexistente	El control de seguridad no se lleva a cabo; no existe evidencia de su implementación.
Inicial	El control existe, pero no se gestiona formalmente ni se apoya en procesos establecidos. Depende del esfuerzo individual o de personal altamente calificado.
Repetible	Se realiza de manera informal, sin documentación oficial; la responsabilidad es individual y no hay evidencia de capacitación estructurada.
Definido	El control se aplica de acuerdo con un procedimiento documentado, aunque este no está formalizado ni aprobado oficialmente.
Administrado	El control sigue un procedimiento documentado y formalizado, aprobado por las autoridades correspondientes.
Optimizado	El control está formalizado y se mide su efectividad periódicamente mediante indicadores clave de desempeño (KPIs).
No Aplicable	En casos específicos, los requisitos principales son obligatorios; sin embargo, ciertos controles pueden ser ignorados bajo justificación administrativa.

Nota. Adaptado de "ISO/IEC 27001:2013 ISMS Status, Statement of Applicability (SoA) and Controls Status (gap analysis) workbook", 2019.

Los ítems evaluados de los requisitos de la norma se presentan en el anexo 1.

Evaluación de cumplimiento de controles, según anexo A de la NTC-IEC 27001:2022

Instrumento que evalúa el nivel de cumplimiento de los controles, del anexo A de la NTC-ISO-IEC 27001:2022, cada ítem se evaluará de la siguiente manera.

Tabla 2

Evaluación de cumplimiento de controles, según anexo A de la NTC-IEC 27001:2022

Estado	Significado

Desconocido	No se ha verificado el cumplimiento ni la existencia del control.
Inexistente	El control de seguridad no se lleva a cabo; no existe evidencia de su implementación.
Inicial	El control existe, pero no se gestiona formalmente ni se apoya en procesos establecidos. Depende del esfuerzo individual o de personal altamente calificado.
Repetible	Se realiza de manera informal, sin documentación oficial; la responsabilidad es individual y no hay evidencia de capacitación estructurada.
Definido	El control se aplica de acuerdo con un procedimiento documentado, aunque este no está formalizado ni aprobado oficialmente.
Administrado	El control sigue un procedimiento documentado y formalizado, aprobado por las autoridades correspondientes.
Optimizado	El control está formalizado y se mide su efectividad periódicamente mediante indicadores clave de desempeño (KPIs).
No Aplicable	En casos específicos, los requisitos principales son obligatorios; sin embargo, ciertos controles pueden ser ignorados bajo justificación administrativa.

Nota. Adaptado de “ISO/IEC 27001:2013 ISMS Status, Statement of Applicability (SoA) and Controls Status (gap analysis) workbook”, 2019.

Los ítems evaluados de los requisitos de la norma se presentan en el anexo 2.

Informe de la Auditoria Inicial

Al finalizar la auditoría, se elabora y entrega un informe de diagnóstico en el que se detallan los niveles de cumplimiento e incumplimiento frente a los requisitos y controles establecidos por la norma aplicable. Este informe incluye un desglose porcentual que facilita la visualización del grado de conformidad alcanzado durante el proceso. Además, los resultados específicos, junto con las observaciones y evidencias recopiladas, se presentan en el Anexo 3, el cual ofrece una visión estructurada y detallada de los hallazgos

identificados.

Evaluacion de Riesgos

Metodología MAGERIT

Se ha optado por la metodología MAGERIT debido a que ofrece un marco estructurado y confiable para la gestión de riesgos, facilitando que la alta dirección tome decisiones fundamentadas frente a los riesgos inherentes al uso de tecnologías de la información. Su principal fortaleza radica en el análisis profundo que propone, eliminando la improvisación y minimizando la subjetividad del evaluador, al apoyarse en procedimientos sistemáticos, claros y bien definidos.

Inicia con la identificación de activos, el cual es un paso fundamental para garantizar una gestión adecuada y eficiente de los recursos tecnológicos y de información en cualquier organización. En este caso, se llevó a cabo mediante entrevistas estructuradas al personal del área de sistemas, quienes, debido a su conocimiento y experiencia, se logró la recopilación de información detallada sobre los activos críticos vinculados al proceso de Gerencia de la Información. Como resultado de este proceso, se identificaron 10 activos críticos de gran relevancia, los cuales fueron considerados esenciales para garantizar la continuidad de las operaciones, la protección de la información y la prestación de servicios, estos fueron clasificados y evaluados así:

Figura 3

Valoración de los Activos de Información

DATOS DEL ACTIVO DE INFORMACION			IMENSION				
Nombre del activo de información	**Proceso propietario del activo**	**Tipo de Activo**	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad
SISTEMA DE INFORMACION DINAMICA GERENCIAL	GERENCIA DE LA INFORMACION	SOFTWARE	MA	MA	MA	MA	MA
SISTEMA DE INFORMACION COMPUCONTA	GERENCIA DE LA INFORMACION	SOFTWARE	A	A	A	A	A
MOTOR SQL COMPUCONTA	GERENCIA DE LA INFORMACION	DATOS	A	A	A	A	A
CORREO ELECTRONICO ESTADISTICA	GERENCIA DE LA INFORMACION	COMUNICACIONES	M	A	A	A	M
SERVIDOR COMPUCONTA	GERENCIA DE LA INFORMACION	HARDWARE	A	A	A	A	A
DISPOSITIVO INTERMEDIO DE RED (SWITCH CORE)	GERENCIA DE LA INFORMACION	HARDWARE	A	A	B	A	MA
FIREWALL DE NUEVA GENERACION	GERENCIA DE LA INFORMACION	HARDWARE	A	A	A	A	A
SERVIDOR NEXTCLOUD	GERENCIA DE LA INFORMACION	SOFTWARE	A	A	A	MA	A
DISOS DUROS COPIAS DE SEGURIDAD EQUPOS DE COMPUTO	GERENCIA DE LA INFORMACION	HARDWARE	A	A	A	MA	A
EQUIPO DE COMPUTO ESTADISTICA	GERENCIA DE LA INFORMACION	HARDWARE	A	A	A	A	B

Nota. Tomado del documento “Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

La información contenida en la tabla es la siguiente:

Datos del activo de la Información

Nombre del Activo de Información. Cada fila identifica un activo específico utilizado por el proceso de Gerencia de la Información. Estos activos comprenden sistemas, hardware y datos esenciales para las operaciones del Hospital, estos son:

Sistema de información dinámica gerencial

Sistema de información compuconta

Motor SQL compuconta

Correo electrónico estadística

Servidor compuconta

Dispositivo intermedio de red (Switch core)

Firewall de nueva generación

Servidor nextcloud

Discos duros copias de seguridad

Todos los activos listados son gestionados por el proceso de Gerencia de la Información, lo que indica que esta área es responsable de su operación, mantenimiento, monitoreo y cumplimiento de las políticas de seguridad asociadas.

Tipo de Activo. Los activos están clasificados en distintas categorías según su naturaleza:

Software: Programas y sistemas operativos que gestionan información.

Hardware: Equipos físicos, como servidores, dispositivos de red y unidades de almacenamiento.

Datos: Información almacenada y procesada por los sistemas.

Comunicaciones: Herramientas que facilitan el intercambio de información, como los sistemas de correo electrónico.

Dimensiones de seguridad.

Cada activo ha sido evaluado bajo cinco dimensiones críticas de seguridad de la información:

Autenticidad: Verifica que los activos y la información sean genuinos y confiables.

Trazabilidad: Asegura la capacidad de rastrear el uso y las modificaciones realizadas en los activos.

Confidencialidad: Protege la información frente a accesos no autorizados.

Integridad: Garantiza que la información y los sistemas no sean alterados de manera no autorizada.

Disponibilidad: Asegura que los activos estén accesibles cuando sean necesarios.

Cada dimensión se califica con niveles como "A" (Alto) o "MA" (Medio Alto), lo que permite identificar las prioridades de seguridad para cada activo. Por ejemplo, los sistemas de información como el *Compucounta* presentan un nivel Medio Alto (MA) en todas las dimensiones, mientras que dispositivos de hardware como los servidores de copia de seguridad también son altamente críticos para garantizar la disponibilidad y confidencialidad.

Figura 4

Información de los Activos

INFORMACIÓN DE LOS ACTIVOS														
No.	DATOS DEL ACTIVO DE INFORMACION	ATRIBUTOS											UBICACIÓN	
	Nombre del activo de información	¿Es activo de información de terceros o de	Sistema expuesto en internet	¿Activo de información que debe ser restringido a un	Activo de información que debe ser	Activo de información que puede ser alterado o	Activo de información que es muy	Activo de información que es muy	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la			Físico	Electrónico
									Leve	Importante	Grave		
1	SISTEMA DE INFORMACION DINAMICA GERENCIAL	SI	SI	NO	SI	SI	SI	SI			X		X
2	SISTEMA DE INFORMACION COMPUCONTA	SI	SI	NO	SI	SI	SI	SI			X	X	
3	MOTOR SQL COMPUCONTA	SI	SI	SI	SI	SI	SI	SI			X	X	
4	CORREO ELECTRONICO ESTADISTICA	NO	NO	NO	NO	SI	NO	NO		X			X
5	SERVIDOR COMPUCONTA	SI	NO	SI	SI	SI	SI	SI			X	X	
6	DISPOSITIVO INTERMEDIO DE RED (SWITCH CORE)	SI	NO	SI	SI	SI	SI	SI			X	X	
7	FIREWALL DE NUEVA GENERACION	NO	SI	SI	SI	SI	SI	SI			X		X
8	SERVIDOR NEXTCLOUD	SI	SI	NO	SI	NO	NO	SI		X			X
9	DISOS DUROS COPIAS DE SEGURIDAD EQUPOS DE COMPUTO	NO		SI	SI	SI	SI	SI			X	X	
10	EQUIPO DE COMPUTO ESTADISTICA	NO		SI	SI	SI	SI	SI			X	X	

Nota. Tomado del documento "Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Atributos Evaluados. Los atributos evaluados corresponden a características específicas consideradas fundamentales para cumplir con los requisitos Estos atributos se analizan en función de su relevancia para la gestión efectiva de la seguridad de la información y su alineación con los objetivos organizacionales

¿Es activo de información de terceros o de clientes que debe protegerse?

Descripción: Evalúa si el activo contiene datos sensibles o confidenciales de terceros o clientes que requieren medidas específicas de protección.

Análisis: Los activos con "SI" en esta columna son críticos porque comprometer esta información podría afectar la confianza y la relación contractual con terceros.

Sistema expuesto en internet

Descripción: Indica si el activo está accesible desde internet, lo que lo hace más vulnerable a ataques externos, como hacking o accesos no autorizados.

Análisis: Aquellos activos con "SI" aquí necesitan estrictas medidas de seguridad, como firewalls, autenticación y cifrado.

¿Activo de información que debe ser restringido a un número limitado de empleados?

Descripción: Determina si el acceso al activo debe ser limitado solo a empleados esenciales.

Análisis: Los activos restringidos son aquellos que manejan información sensible o crítica para las operaciones internas.

Activo de información que debe ser restringido a personas externas

Descripción: Evalúa si el activo debe estar completamente inaccesible para personas externas a la organización.

Análisis: Los activos marcados con "SI" aquí requieren políticas estrictas de acceso y monitoreo.

Activo de información que puede ser alterado o comprometido para fraudes o corrupción

Descripción: Indica si el activo es susceptible a manipulaciones que puedan dar lugar a fraudes, corrupción o uso indebido.

Análisis: Los activos con "SI" necesitan controles de integridad, como auditorías regulares y sistemas de registro de cambios.

Activo de información que es muy crítico para las operaciones internas

Descripción: Define si el activo es fundamental para el funcionamiento interno de la organización.

Análisis: Estos activos son esenciales para la continuidad operativa y requieren estrategias robustas de respaldo y recuperación.

Activo de información que es muy crítico para el servicio hacia terceros

Descripción: Indica si el activo afecta directamente la capacidad de brindar servicios a clientes o socios externos.

Análisis: Los activos identificados aquí tienen un impacto directo en la percepción y la reputación de la empresa.

Impacto del Activo. El impacto se clasifica según la gravedad de las consecuencias que tendría el acceso, uso o modificación no autorizada del activo:

Leve: El impacto sería mínimo, sin interrupciones significativas.

Importante: El impacto sería moderado, afectando parcialmente los procesos o servicios.

Grave: El impacto sería crítico, causando interrupciones mayores o daños severos.

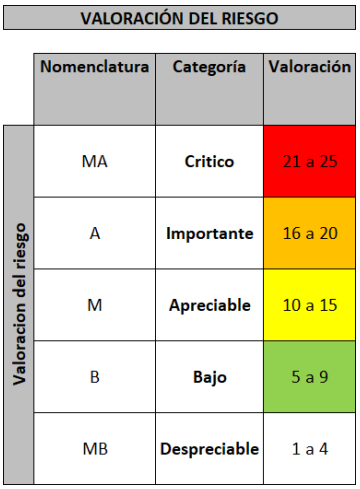
Ubicación de los Activos. Físico: Incluye hardware como servidores, equipos de almacenamiento y otros componentes tangibles.

Electrónico: Incluye sistemas, bases de datos, aplicaciones y cualquier recurso intangible que requiera seguridad cibernética.

Valoración del Riesgo de Activos de la Información. Una vez evaluados los activos, genera la valoración del riesgo según la siguiente tabla, en la cual se clasifican los niveles de riesgo de acuerdo con su puntuación final. Esta valoración permite priorizar la atención a cada activo, dependiendo de su impacto y criticidad.

Figura 5

Valoración del Riesgo



VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Nota. Tomado del documento "Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Crítico (MA): Valoración entre 21 y 25, indicando un nivel de riesgo severo que requiere atención inmediata.

Importante (A): Valoración entre 16 y 20, señalando un nivel de riesgo alto que necesita medidas correctivas a corto plazo.

Apreciable (M): Valoración entre 10 y 15, reflejando un riesgo moderado que puede gestionarse a mediano plazo.

Bajo (B): Valoración entre 5 y 9, representando un riesgo bajo que solo requiere monitoreo ocasional.

Despreciable (MB): Valoración entre 1 y 4, indicando un nivel de riesgo mínimo sin necesidad de acciones inmediatas.

Esta clasificación es fundamental para asignar los recursos de manera eficiente y garantizar que los activos más críticos sean protegidos adecuadamente.

Figura 6 Riesgos Evaluados

Riesgos Evaluados

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILI	VALOR
SISTEMA DE INFORMACION DINAMICA GERENCIAL	CRITICO	25	25	25	25	25	25
SISTEMA DE INFORMACION COMPUCONTA	IMPORTANTE	20	20	20	20	20	20
MOTOR SQL COMPUCONTA	IMPORTANTE	20	20	20	20	20	20
CORREO ELECTRONICO ESTADISTICA	IMPORTANTE	15	20	20	20	15	18
SERVIDOR COMPUCONTA	IMPORTANTE	20	20	20	20	20	20
DISPOSITIVO INTERMEDIO DE RED (SWITCH CORE)	IMPORTANTE	20	20	9	20	25	19
FIREWALL DE NUEVA GENERACION	IMPORTANTE	20	20	20	20	20	20
SERVIDOR NEXTCLOUD	CRITICO	20	20	20	25	20	21
DISOS DUROS COPIAS DE SEGURIDAD EQUPOS DE COMPUTO	CRITICO	20	20	20	25	20	21
EQUIPO DE COMPUTO ESTADISTICA	IMPORTANTE	20	20	20	20	9	18

Nota. Tomado del documento “Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Activos Críticos (21-25)

El proceso de Gerencia de la Información cuenta con dos activos críticos esenciales para garantizar el funcionamiento eficiente y continuo en la atención al paciente. Estos activos son:

Sistema de Información Dinámica Gerencial (Valoración: 25): Este sistema desempeña un papel clave en la gestión y análisis de datos estratégicos, proporcionando información fundamental para la toma de decisiones en el ámbito hospitalario.

Discos Duros para Copias de Seguridad (Equipos de Cómputo) (Valoración: 21): Almacenan respaldos esenciales de los datos operativos y clínicos, asegurando la disponibilidad y recuperación de información en caso de fallos en los sistemas principales.

Ambos activos son fundamentales para mantener la integridad, la continuidad operativa y la calidad del servicio a los pacientes.

Activos Importantes (16-20).

El proceso de Gerencia de la Información también incluye varios activos relevantes que contribuyen significativamente a la operación y seguridad del sistema hospitalario. Estos activos son:

Sistema de Información Compuconta (Valoración: 20): Herramienta clave para la gestión contable y financiera.

Firewall de Nueva Generación (Valoración: 20): Protege la red de amenazas externas, asegurando la integridad y confidencialidad de los datos.

Servidor Nextcloud (Valoración: 20): Garantiza la gestión y almacenamiento de información en la nube, facilitando la colaboración y el acceso remoto.

Servidor Compuconta (Valoración: 19): Infraestructura crítica para la operatividad del sistema contable.

Dispositivo Intermedio de Red (Switch Core) (Valoración: 19): Actúa como un nodo central en la red, facilitando la comunicación entre los diferentes sistemas y dispositivos.

Motor SQL Compuconta (Valoración: 18): Base de datos estructurada para la administración eficiente de la información contable.

Correo Electrónico Estadística (Valoración: 18): Canal esencial para la comunicación interna y externa en el área estadística.

Equipo de Cómputo Estadística (Valoración: 18): Herramientas indispensables para la recolección, análisis y presentación de datos.

Análisis de Amenazas. El objetivo principal es establecer un diagnóstico claro sobre la seguridad de los activos, determinar los niveles de riesgo inicial y residual, y proponer medidas correctivas o preventivas para garantizar la continuidad operativa, la integridad, y la disponibilidad de la información.

Los activos de información incluyen sistemas de software, hardware, servicios y datos críticos para la organización. Para cada activo, se han identificado amenazas potenciales (como destrucción, fugas o manipulación de información), vulnerabilidades existentes (como falta de copias de respaldo o procedimientos inadecuados), y los controles aplicados para mitigar estos riesgos. Además, se calcula el nivel de riesgo neto y residual, y se proponen recomendaciones prácticas para fortalecer la gestión de la seguridad de la información.

Activos con Mayor Riesgo (Críticos)

Estos activos son esenciales para el Hospital y presentan una valoración inicial alta debido a la criticidad de las amenazas y vulnerabilidades.

Sistema de Información Dinámica Gerencial

Riesgo Inicial: 75

Amenaza: Destrucción de información.

Vulnerabilidad: Copias de seguridad inexistentes o incompletas.

Control Actual: Copias de seguridad históricas transferidas por el proveedor, almacenadas en una máquina virtual.

ISO 27001 Aplicado: A12.3.1 (Respaldo de la información).

Riesgo Residual: 38

Recomendaciones:

Realizar pruebas periódicas de las copias de respaldo.

Implementar políticas de conservación y redundancia de los respaldos.

Automatizar la transferencia de respaldos a ubicaciones seguras.

Servidor Compuconta

Riesgo Inicial: 75

Amenaza: Avería de origen físico o lógico.

Vulnerabilidad: Ausencia de servidor de respaldo y mantenimiento insuficiente.

Control Actual: Mantenimiento preventivo anual.

ISO 27001 Aplicado: A11.2.4 (Mantenimiento de equipos).

Riesgo Residual: 38

Recomendaciones:

Establecer redundancia mediante un servidor espejo.

Incrementar la frecuencia del mantenimiento preventivo.

Implementar un sistema de monitoreo proactivo del estado del hardware.

Dispositivo Intermedio de Red (Switch Core)

Riesgo Inicial: 75

Amenaza: Avería de origen físico o lógico.

Vulnerabilidad:

Ausencia de copias de respaldo de la configuración.

Mantenimiento insuficiente.

Control Actual: Ninguno.

Riesgo Residual: 75

Recomendaciones:

Crear copias de seguridad periódicas de la configuración.

Implementar un plan de mantenimiento preventivo.

Adquirir un dispositivo de respaldo para garantizar la continuidad operativa.

Activos con Riesgo Moderado

Estos activos presentan riesgos iniciales moderados que han sido parcialmente mitigados por controles específicos.

Discos Duros Copias de Seguridad (Equipos de Cómputo)

Riesgo Inicial: 30

Amenaza: Pérdida de equipos.

Vulnerabilidad:

Almacenamiento sin protección.

Supervisión insuficiente del personal externo.

Control Actual: Bitácora de ingreso y salida de personal externo.

ISO 27001 Aplicado: A11.2.5 (Retiro de activos).

Riesgo Residual: 15

Recomendaciones:

Implementar medidas de seguridad física, como candados y cajas fuertes para equipos críticos.

Establecer vigilancia 24/7 en los centros de datos.

Sistema de Información Compuconta

Riesgo Inicial: 60

Amenaza: Fugas de información.

Vulnerabilidad:

Sesiones abiertas al abandonar el puesto de trabajo.

Asignación incorrecta de derechos de acceso.

Control Actual:

Procedimientos de asignación de derechos de acceso.

ISO 27001 Aplicado: A9.2.1 (Registro de usuarios).

Riesgo Residual: 30

Recomendaciones:

Configurar políticas de cierre automático de sesiones inactivas.

Sensibilizar al personal sobre la importancia de proteger sus sesiones.

Auditar regularmente los derechos de acceso asignados.

Activos con Riesgo Bajo

Estos activos tienen un impacto limitado, pero requieren controles básicos para mantener la continuidad y disponibilidad.

Motor SQL Compuconta

Riesgo Inicial: 30

Amenaza: Manipulación de los registros de actividad.

Vulnerabilidad:

Uso indebido de privilegios de acceso.

Falta de procedimientos adecuados de contratación.

Control Actual: Ninguno.

Riesgo Residual: 30

Recomendaciones:

Implementar registro y auditorías de accesos.

Establecer controles de acceso basados en roles.

Mejorar los procesos de contratación y capacitación en seguridad.

Correo Electrónico Estadística

Riesgo Inicial: 30

Amenaza: Suplantación de identidad del usuario.

Vulnerabilidad: Ausencia de políticas sobre el uso del correo electrónico.

Control Actual: Ninguno.

Riesgo Residual: 30

Recomendaciones:

Implementar políticas claras sobre el uso del correo electrónico.

Usar autenticación multifactor para todas las cuentas.

Revisar anexo 2 – Matriz de análisis de riesgos

Plan de Tratamiento. El plan de tratamiento aborda las amenazas y vulnerabilidades de los activos mediante medidas alineadas con los controles de la norma ISO 27001:2013. Estas acciones incluyen controles técnicos, físicos y organizativos que garantizan la protección de datos, el control de accesos, los respaldos, la seguridad física y la continuidad del negocio. El enfoque estructurado asegura la prevención, detección y respuesta a incidentes, priorizando la mitigación de riesgos y el cumplimiento de requisitos legales, contractuales y operativos.

Tratamiento de Riesgos. El plan utiliza cuatro estrategias principales para tratar los riesgos:

Mitigar: Es la estrategia más utilizada, reflejando el enfoque en reducir los impactos mediante controles técnicos y operativos.

Aceptar: Se indica como opción para ciertos activos cuando los riesgos son considerados manejables con las medidas existentes.

Eliminar: No se contempla en este caso, ya que los activos son esenciales para las operaciones.

Transferir: Tampoco se menciona, aunque podría aplicarse

Controles de la Norma ISO 27001 Aplicados.

Se identifican controles clave de la norma ISO 27001:2013 en varias categorías dominantes:

Para el activo Dinámica Gerencial, se identifica el siguiente plan de tratamiento:

Tabla de análisis de riesgos basada en la norma ISO 27001:2013, aplicada al Sistema de Información Dinámica Gerencial.

Figura 7

Análisis de riesgos basada en la norma ISO 27001:2013, aplicada al Sistema de Información Dinámica Gerencial

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DE RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal	Obligación	Requerimiento	Analisis de	
						Indique el control a aplicar a partir de la norma ISO 27001:2013												
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					Exclusión
1	SISTEMA DE INFORMACION DINAMICA GERENCIAL	25	SOFTWARE	[A18] Destrucción de información	I				X	DOMINIO_A12	OBJETIVO_A12_3	A12.3.1 Respaldo de la información -- Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Moniteo al cumpliento de transferencia de copias de seguridad por parte del proveedor Validacion y pruebas de las copias de seguridad enviadas por el proveedor.	X	X	X	X	

Nota. Tomado del documento “Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A12: Operación de la Seguridad

Control: *A12.3.1 Respaldo de la información.*

Aplicación: En activos de software y bases de datos críticos, se especifican respaldos regulares y validaciones.

Fortalezas: Monitoreo del cumplimiento de las copias y validaciones por parte de terceros.

Para el activo sistema de información Compuconta, se identifica el siguiente plan de tratamiento:

Figura 8

Análisis de riesgos basada en la norma ISO 27001:2013, aplicada al Sistema de Información Compuconta

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal	Obligación	Requerimiento	Análisis de	Exclusión
										Indique el control a aplicar a partir de la norma ISO 27001:2013								
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					
2	SISTEMA DE INFORMACION COMPUCONTA	20	SOFTWARE	[E19] Fugas de información	I				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Elaboracion de matriz de roles y perfiles de sistema informacion y monitoreo constante			X	X	

Nota. Tomado del documento "Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A9: Control de Acceso

Control: *A9.2.3 Gestión de derechos de acceso privilegiado.*

Aplicación: Diseño de matrices de roles y perfiles, y monitoreo constante de accesos privilegiados.

Fortalezas: Propuesta clara para limitar privilegios.

Figura 9

Análisis de Riesgos Basada en la Norma ISO 27001:2013, Aplicada al Motor SQL Compuconta

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal	Obligación	Requerimiento	Análisis de	Exclusión
										Indique el control a aplicar a partir de la norma ISO 27001:2013								
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					
3	MOTOR SQL COMPUCONTA	20	DATOS	[A3] Manipulación de los registros de actividad (log)	I				X	DOMINIO_A12	OBJETIVO_A12_4	A12.4.2 Protección de la información de registro --Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Realizar copias de seguridad de logs del sistema Elaboracion de matriz de roles y pefiles			X	X	

Nota. Tomado del documento "Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A12: Seguridad en las Operaciones

Control: A12.4.2 Protección de la información de registro.

Aplicación:

Realizar copias de seguridad de los registros (logs) del sistema.

Elaborar una matriz de roles y perfiles para restringir el acceso no autorizado.

Fortalezas:

Implementación de copias de seguridad que garantizan la disponibilidad de los registros ante fallos.

Delimitación clara de roles y permisos, reduciendo el riesgo de accesos no autorizados.

Oportunidades de Mejora:

Automatizar el proceso de respaldo de los logs para evitar errores humanos.

Utilizar herramientas de monitoreo en tiempo real que detecten alteraciones en los registros.

Figura 10

Análisis de Riesgos Basada en la Norma ISO 27001:2013, Aplicada al Correo Electrónico Estadística

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal	Obligación	Requerimiento	Analisis de	Exclusión
						Indique el control a aplicar a partir de la norma ISO 27001:2013												
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					
4	CORREO ELECTRONICO ESTADISTICA	10	SERVICIOS	[A5] Suplantación de la identidad del usuario	I				X	DOMINIO_A9	OBJETIVO_A9_3	A9.3.1 Uso de información de autenticación secreta --Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Elaboracion y socilaizacion de politica de control de acceso y uso adecuado de autenticacion secreta		X	X	X	

Nota. Tomado del documento “Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A9: Control de Acceso

Control: A9.3.1 Uso de información de autenticación secreta.

Aplicación:

Elaboración y socialización de una política de control de acceso.

Uso adecuado de mecanismos de autenticación secreta para proteger la identidad del usuario.

Fortalezas:

Desarrollo de políticas claras y estandarizadas para el manejo de información de autenticación.

Promoción de buenas prácticas entre los usuarios para reforzar la seguridad.

Oportunidades de Mejora:

Implementar autenticación multifactor (MFA) para mayor seguridad.

Incorporar monitoreo continuo para detectar intentos de suplantación de identidad en tiempo real.

Figura 11

Análisis de Riesgos Basada en la Norma ISO 27001:2013, Aplicada al Servidor Compuconta

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal	Obligación	Requerimiento	Analisis de	Exclusión
						Indique el control a aplicar a partir de la norma ISO 27001:2013												
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					
5	SERVIDOR COMPUCONTA	20	HARDWARE	[I5] Avería de origen físico o lógico	I				X	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información -- Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Elaboracion de un plan de respaldo de dispositivos Monitoreo al cronograma de mantenimientos preventivos de dispositivos		X	X	X	

Nota. Tomado del documento “Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A17: Aspectos de Seguridad de Continuidad

Control: *A17.2.1 Disponibilidad de instalaciones de procesamiento de información.*

Aplicación: Creación de planes de respaldo y monitoreo de cronogramas de mantenimiento.

Fortalezas: Priorización de dispositivos críticos como servidores y hardware de red.

Oportunidades de Mejora: Implementar redundancia activa y monitoreo proactivo en tiempo real.

Figura 12

Análisis de Riesgos Basada en la Norma ISO 27001:2013, Aplicada al Dispositivo Intermedio de Red

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal	Obligación	Requerimiento	Analisis de	Exclusión
						Indique el control a aplicar a partir de la norma ISO 27001:2013												
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					
6	DISPOSITIVO INTERMEDIO DE RED (SWITCH CORE)	19	HARDWARE	[I5] Avería de origen físico o lógico	I				X	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información -- Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Elaboracion de un plan de respaldo de dispositivos Monitoreo al cronograma de mantenimientos preventivos de dispositivos		X	X	X	

Nota. Tomado del documento “Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A17: Aspectos de Seguridad de Continuidad

Control:

A17.2.1 - Disponibilidad de instalaciones de procesamiento de información.

Este control garantiza que las instalaciones de procesamiento sean confiables y puedan soportar las operaciones críticas.

Aplicación:

Elaboración de un plan de respaldo de dispositivos.

Monitoreo del cronograma de mantenimientos preventivos de los dispositivos.

Fortalezas:

Priorización de la disponibilidad de dispositivos críticos, como dispositivos intermedios de red (switches/core).

Implementación de planes de mantenimiento que garantizan la operación continua de los equipos.

Oportunidades de Mejora:

Implementar redundancia activa para asegurar la continuidad del servicio incluso en caso de fallos.

Establecer monitoreo proactivo en tiempo real para identificar problemas antes de que afecten las operaciones.

Figura 13

Análisis de Riesgos Basada en la Norma ISO 27001:2013, Aplicada al Firewall de Nueva Generación

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal	Obligación	Requerimiento	Analisis de	Exclusión
						Indique el control a aplicar a partir de la norma ISO 27001:2013												
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					
7	FIREWALL DE NUEVA GENERACION	20	HARDWARE	[E23] Errores de mantenimiento / actualización de equipos (hardware)	I				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Elaborar cronograma de mantenimiento logico de dispsitivo Elaborar procedimiento de copias de configiracion de dispositivo Contar con equipo de respaldo		X	X	X	

Nota. Tomado del documento “Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A11: Seguridad Física y Ambiental

Control: A11.2.4 Mantenimiento de los equipos.

Este control asegura que los equipos sean mantenidos adecuadamente para garantizar su disponibilidad e integridad de manera continua.

Aplicación:

Elaboración de cronogramas de mantenimiento lógico para el firewall de nueva generación.

Definición de procedimientos para realizar copias de seguridad de la configuración del dispositivo.

Disposición de equipos de respaldo para garantizar la continuidad de las operaciones en caso de fallos.

Fortalezas:

Creación de planes específicos de mantenimiento que previenen fallas en equipos críticos.

Respaldo de configuraciones que permiten una rápida recuperación ante fallos o cambios inesperados.

Oportunidades de Mejora:

Implementar redundancia activa en los sistemas de firewall para mejorar la disponibilidad.

Adoptar monitoreo proactivo en tiempo real para identificar y mitigar errores antes de que afecten el rendimiento del hardware.

Figura 14

Análisis de Riesgos Basada en la Norma ISO 27001:2013, Aplicada al Servidor Nextcloud

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal				
						Indique el control a aplicar a partir de la norma ISO 27001:2013												
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control		Obligación	Requerimient	Analisis de	Exclusión
####	SERVIDOR NEXTCLOUD	21	SOFTWARE	(IS) Avería de origen físico o lógico	I				X	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información -- Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Elaboracion de un plan de respaldo de dispositivos Monitoreo al cronograma de mantenimientos preventivos de dispositivos		X	X	X	

Nota. Tomado del documento “Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A17: Aspectos de Seguridad Relacionados con las Operaciones

Control: A17.2.1 Disponibilidad de instalaciones de procesamiento de la información.

Aplicación:

Implementación de un plan de respaldo de dispositivos.

Monitorización del cronograma de mantenimientos preventivos de dispositivos.

Fortalezas:

Garantiza la disponibilidad de los sistemas mediante redundancia.

Refuerza los requisitos de continuidad operativa.

Oportunidades de Mejora:

Automatización de la monitorización de dispositivos para evitar fallos no detectados.

Inclusión de pruebas regulares de recuperación para validar la efectividad de los planes de respaldo.

Figura 15

Análisis de Riesgos Basada en la Norma ISO 27001:2013, Aplicada los Discos Duros

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento o Legal				
						Indique el control a aplicar a partir de la norma ISO 27001:2013												
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control		Obligación	Requerimient	Análisis de	Exclusión
####	DISOS DUROS COPIAS DE SEGURIDAD EQUIPOS DE COMPUTO	21	HARDWARE	[E25] Pérdida de equipos	I				X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.2 Controles de acceso físicos -- Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Instalacion de camara de videovigilancia Instalalacion de dispositivo de control de acceso Inventario y bitacora de dispositivos de almacenamiento		X	X	X	

Nota. Tomado del documento "Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A11: Seguridad Física y Ambiental

Control: A11.1.2 Controles de acceso físicos.

Aplicación:

Instalación de cámaras de videovigilancia para monitorear áreas seguras.

Implementación de dispositivos de control de acceso, como lectores biométricos o tarjetas de proximidad.

Elaboración y mantenimiento de bitácoras e inventarios actualizados para dispositivos de almacenamiento.

Fortalezas:

Proporciona una prevención efectiva contra la pérdida de activos físicos.

Refuerza la seguridad del acceso a áreas críticas mediante mecanismos específicos.

Oportunidades de Mejora:

Complementar el control con sistemas de seguimiento avanzados, como tecnología RFID, para monitorear dispositivos críticos en tiempo real.

Implementar auditorías regulares para verificar el cumplimiento de los controles.

Figura 16

Aspectos de Seguridad Relacionados con las Operaciones

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal				
						Indique el control a aplicar a partir de la norma ISO 27001:2013												
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control		Obligación	Requerimient	Analisis de	Exclusión
####	EQUIPO DE COMPUTO ESTADISTICA	18	HARDWARE	[IS] Avería de origen físico o lógico	I				X	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información -- Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Elaboracion de un plan de respaldo de dispositivos Monitoreo al cronograma de mantenimientos preventivos de dispositivos		X	X	X	
No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Plan de Tratamiento								Requerimiento Legal				
						Indique el control a aplicar a partir de la norma ISO 27001:2013												
						Trans	Acep	Elimi	Mitig	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control		Obligación	Requerimient	Analisis de	Exclusión
####	EQUIPO DE COMPUTO ESTADISTICA	18	HARDWARE	[IS] Avería de origen físico o lógico	I				X	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información -- Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Elaboracion de un plan de respaldo de dispositivos Monitoreo al cronograma de mantenimientos preventivos de dispositivos		X	X	X	

Nota. Tomado del documento "Matriz de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013", Universidad Nacional Abierta y a Distancia – UNAD, 2022.

Dominio A17: Aspectos de Seguridad Relacionados con las Operaciones

Control: A17.2.1 Disponibilidad de instalaciones de procesamiento de información.

Aplicación:

Elaboración de un plan de respaldo de dispositivos para garantizar la continuidad operativa.

Monitorización y cumplimiento del cronograma de mantenimientos preventivos de los dispositivos.

Fortalezas:

Reduce la probabilidad de interrupciones debido a fallos físicos o lógicos.

Asegura la disponibilidad de los sistemas mediante estrategias de redundancia.

Oportunidades de Mejora:

Incluir pruebas regulares de recuperación para validar la efectividad de los

respaldos.

Implementar sistemas automatizados para detectar fallos tempranamente y programar mantenimientos de manera proactiva.

Política Seguridad de la Información

El Hospital San Rafael debe implementar una política de seguridad de la información con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de la información que maneja. Esta política permitirá proteger los datos sensibles de pacientes, colaboradores y otras partes interesadas frente a riesgos como accesos no autorizados, pérdida de información, fraudes y amenazas cibernéticas. Además, garantizará el cumplimiento de normativas legales y regulatorias aplicables, fomentando una cultura de seguridad en toda la organización.

Se propone implementar la siguiente política de seguridad de la información:

La Dirección General del Hospital San Rafael de Pasto, comprometido con sus usuarios, la familia, la comunidad, proveedores, clientes y de más partes interesadas, establece la necesidad de implementar un Sistema de Gestión de Seguridad de la Información encaminado a proteger los activos de la información a través de la generación de Políticas específicas, procedimientos, lineamientos, apoyo en la implementación de herramientas tecnológicas de prevención y forjar una cultura de concientización de seguridad de la información en todos los colaboradores del Hospital todo esto con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, garantizando la continuidad del negocio y minimizar el impacto causado por los riesgos identificados, logrando así mantener la confianza y responder frente a las necesidades de sus diferentes grupos de interés.

Todo esto en concordancia con la misión y visión del Hospital, la normatividad vigente, los principios de la función administrativa y comprometidos con la Mejora

continua a través de la medición de la efectividad de los controles del Sistema de Gestión de Seguridad de la Información.

La Dirección General, aprueba la política general y políticas específicas de seguridad de la información que se generen y ofrecer respaldo tanto económico y administrativo para llevar a cabo todo el proceso de implementación y continuidad de un Sistema de Gestión de Seguridad de la Información.

La política se debe aplicar por parte de todos los colaboradores, usuarios, clientes, proveedores y demás partes interesadas, los cuales deben comprometerse con el cumplimiento total de esta política y las específicas que se generen en torno a la seguridad de la información.

Gestor de gerencia de la información. Es el responsable de velar por la implementación, el cumplimiento y seguimiento de la política de seguridad de la información

La política general y las especificas serán revisadas y actualizadas una vez al año, en los casos en que se vea necesario se ajustarán antes de su revisión.

Se socializará la política por los medios de comunicación con los que cuenta el Hospital entorno a la Seguridad de la información y Ciberseguridad será sancionada de acuerdo con el nivel de incumplimiento.

Objetivos de la Política de Seguridad

Implementar un Sistema de Gestión de Seguridad de la Información, que permita proteger los activos de la información.

Generar políticas específicas, procedimientos, lineamientos queapoyen la implementación de herramientas tecnológicas de prevención

Propender por una cultura de concientización de seguridad de la información en todos los niveles del Hospital, a fin de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información.

Asegurar la continuidad del negocio y minimizar el impacto causado por los riesgos identificados, logrando así mantener la confianza y responder frente a las necesidades de sus diferentes grupos de interés.

Cumplir con la normatividad vigente, el direccionamiento estratégico y la mejora continua, a través de la medición de la efectividad de los controles del Sistema de Gestión de Seguridad de la Información.

Se contempla políticas de seguridad especificas que complementen la seguridad de la información, estas son:

Politicas Especificas

Política 1: Control de Acceso

Propósito. Establecer los requisitos para el control adecuado de accesos a los Servicios deTecnologías de la Información y la infraestructura de HSRP.

Definiciones de la Política. Administración de Usuarios

a) Todos los colaboradores deben tener asignado solo una cuentade usuario (salvo excepciones que son justificadas por la Gerencia respectiva), la cual es de uso personal para

el desarrollo de las funciones de su cargo. Estas deberán ser nombradas y no genéricas.

b) Los usuarios sólo deben tener permisos de accesos a aquellos recursos,sistemas, aplicativos, servicios e información que estén debidamenteautorizados, sin acceder por la misma vía a otros recursos.

c) Todas las plataformas y sistemas en donde se procese y/o conserve información sensible deben tener implementado un sistema automático de control de acceso. En caso de que no pueda implementarse un sistemaautomático, el encargado del Área de Tecnologías de la Información debe informar al Administrador de Red y/o Encargado del área de Tecnologías de la Información.

d) El Área de Talento Humano debe enviar al Encargado del área de Tecnologíasde la Información, un Memorándum o correo electrónico, donde solicita la aprobación para la creación de la cuenta de usuario para el nuevo colaboradorque ha ingresado a la institución. En el caso de la creación de un usuario paraun tercero (Auditores Externos, etc.), serán autorizados por la Gerencia General y se enviará la solicitud correspondiente a través de memorándum ocorreo electrónico al Administrador de Red o encargado del área de Tecnologías de la Información.

e) La solicitud de creación de usuario debe indicar los siguientes datos: Nombre completo, area, cargo y perfil.

f) El Área de Tecnologías de la Información evaluará la solicitud de creación de la nueva cuenta de usuario; en caso de que no encuentre ninguna observaciónremitirá por correo electrónico la solicitud aprobada al encargado del área deTecnologías de la Información para la creación de la nueva cuenta de usuarioy asignación de perfiles; en caso encuentre alguna observación devolverá la solicitud al Área de Talento Humano o a la Gerencia correspondiente, informando los motivos de la observación para ser levantadas.

g) El Área de Tecnologías de la Información, debe efectuar el análisis correspondiente y proceder a la creación de la cuenta de usuario y a la asignación de los perfiles solicitados para el acceso a los recursos informáticos. En caso de hallar un requerimiento de perfil con característicasno definidas, el área de Infraestructura solicitará la evaluación y opinión del Encargado del Área de Tecnologías de la Información.

h) El nuevo usuario deberá suscribir un documento en el cual declare haber leídoy comprendido los alcances de las políticas de seguridad, así como su completa sujeción al cumplimiento de estas.

i) Cada colaborador debe tener una única cuenta de usuario personal e intransferible para el uso de los servicios informáticos e ingreso a los sistemas de Información, siendo el único responsable de su correcto uso. Estas deberán ser nombradas y no genéricas.

j) Las cuentas de usuario especiales se utilizan para la ejecución de los servicios de los servidores de aplicaciones o para el uso de software interno, los cuales deben ser aprobadas por el Encargado del Área de Tecnologías de la Información.

k) Se crearán cuentas de Superusuario que contaran con todos los privilegios y no se usaran para fines operativos, teniendo en cuenta lo siguiente:

- Su acceso es solamente para actividades críticas realizadas por el Áreade Infraestructura, previa autorización del Encargado del Área de Tecnología de la Información.

l) Toda cuenta de usuario que no haya accedido al sistema por más de treinta 30 días calendarios continuos debe bloquearse.

m) Las cuentas que no hayan sido utilizadas en los últimos noventa días deben ser eliminadas o inhabilitadas dependiendo del caso.

n) Está prohibido intentar ingresar a los servicios de cómputo y comunicacionescon la cuenta de otro personal o de otras personas (naturales, jurídicas, consultores, contratistas, temporales, terceras partes u otros).

o) El Área de Talento Humano debe hacer firmar a todos los colaboradores un compromiso de responsabilidad y confidencialidad del uso de su cuenta de usuario, de la respectiva contraseña asignada y de la información de los sistemas informáticos a los que accede.

Administración de Privilegios

a) Los responsables de solicitar la modificación de los perfiles de los usuarios son el Área de Talento Humano, el jefe de Área o Departamento, o el Gerente de Línea; quien deberá solicitar mediante correo electrónico al Área de Tecnología de Información la modificación de los perfiles de los usuariosque están a su cargo.

b) El Área de Talento Humano es responsable de efectuar un control mensual de las modificaciones de puestos de trabajo, notificar al Encargado del áreade Tecnologías de la Información para que efectúen los Controles periódicosde los usuarios y privilegios en el sistema.

c) El área de Tecnologías de la Información debe realizar un control mensual de los usuarios inactivos y proceder a notificar al respectivo jefe de Área o Departamento para que efectúe las acciones correspondientes.

d) Acceso a los recursos debe concederse en función de cada grupo (perfiles de cargo) y no en función de cada usuario.

e) La baja de una cuenta de usuario se realiza cuando un colaborador renunciao concluye su vinculación laboral con la institución.

f) El Área de Talento Humano envía al Área de Tecnología de la Información un

memorándum o correo electrónico (e-mail) solicitando la baja de la cuenta de usuario del colaborador que renuncia o concluye su vinculación laboral con la institución. En el caso de un usuario tercero autorizado, la Gerencia respectiva deberáinformar al término de sus actividades dentro de la Orden Hospitalaria de San Juan de Dios. Complementar con reporte mensual de ceses.

g) El Área de Talento Humano envía al Área de Tecnología de la Información notificara antes del retiro de un personal para sondear y asegurar la data del colaborador.

h) El área de Tecnología de la Información procede a deshabilitar la cuenta de usuario en el AD del dominio y a mover la cuenta a la Unidad organizativa de Retirados.

i) De acuerdo con las recomendaciones efectuadas por Auditoría Interna, Encargado de Tecnologías de la Información y/o Gerencia se pueden redefinir los accesos del personal en base a un memorándum emitido por Gerencia.

Gestión de Contraseñas

a) Cada personal debe tener asociada una contraseña que cumplacon las características de contraseñas seguras.

b) No está permitido que las demás personas (naturales, jurídicas, consultores, contratistas, temporales, terceras partes u otros) utilicen contraseñas asignadas al personal de la institución.

c) El HSRP mantendrá definido para todos sus sistemas de información un esquema de construcción de contraseñas fuertes que debe ser cumplida por todo el personal del HSRP (funcionarios, servidores, locadores de servicios y otros).

d) Las contraseñas deberán permanecer enmascaradas en todos los medios tecnológicos en los cuales son digitadas.

e) Es responsabilidad directa del personal del HSRP y demás personas (naturales,

jurídicas, consultores, contratistas, temporales o terceras partesu otros) el velar por la confidencialidad y buen uso de su contraseña.

f) Crear siempre un usuario para la gestión diaria y otro para la gestión de actividades críticas, en este último se deberá utilizar un control de contraseña para el acceso.

g) La contraseña de Superusuario debe cambiarse en coordinación con el Encargado de Tecnología de la Información, en los siguientes casos:

a. Al menos cada 6 meses.

b. Cada vez que se retire alguien que conoce la contraseña anterior.

c. Siempre que se sospeche una situación de inseguridad

h) No se deben almacenar contraseñas en formato legible en archivos tipo “batch”, scripts de logon automáticos, macros de software, teclas de funciónde terminales, computadores sin control de acceso, archivos de texto o en sitios donde personas no autorizadas puedan descubrirlos y utilizarlos.

Controles de acceso a la red

a) Todo personal externo (clientes, proveedores, visitas, etc.), que requiera conectar un equipo de trabajo a la red de la institución, deberá pasar por un control y análisis previo del personal de Soporte Técnico, con el fin de detectary eliminar posibles infecciones que representen un riesgo de seguridad.

b) Ninguna persona que labore en el Área de Tecnología de la Información tendrá acceso a los datos en producción, en modalidad diferente a la de consulta, a excepción del Encargado de la Base de Datos o cuando se realice por expresa solicitud y autorización del responsable del Área de Tecnología de la Información.

c) El Área de Tecnología de la Información garantizará a la entidad que el personal

del HSRP y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) reportadas como ausentes por motivo devacaciones, incapacidades, licencias, término del servicio, etc., no podrá tener acceso a la red interna de la institución, salvo que se justifique y se realicepor expresa solicitud y autorización del responsable del Área de Tecnología de la Información.

d) Restringir la cuenta de usuario a una sola sesión de trabajo, siempre y cuando se dispongan de las herramientas automáticas para realizarlo. Las excepciones deberán ser aprobadas por el Comité de Sistemas.

e) Para los usuarios genéricos, especiales, mayor riesgo, en caso de que lo soliciten los Jefes de Área o Gerencias, se deberá limitar las conexiones sólo a las estaciones de trabajo autorizadas y adicionalmente se debe implementar en el sistema de control de acceso el registro de los eventos relacionados con la seguridad.

f) El acceso a Internet es principalmente para fines laborales. Un poco de navegación personal limitada se permite si al hacerlo no hay consumo perceptible de los recursos de los sistemas de Tecnologías de la Información y la productividad del trabajo no se ve afectada. La navegación personal no es recomendada durante lashoras de trabajo.

g) El acceso a sitios pornográficos, sitios de hacking, y otros sitios de riesgo está estrictamente prohibido.

h) El tráfico entrante y saliente es regulado, utilizando servidores de seguridad.

i) Los usuarios, al acceder a Internet deben comportarse de una manera compatible con el prestigio y valores de la Organización. Los ataques como la denegación de servicio, el spam, la pesca (fishing), el fraude, la piratería, la distribución de material cuestionable, infracción de derechos de autor y otros están estrictamenteprohibidos.

j) Para acceder a los recursos internos desde ubicaciones remotas, los usuarios

deben tener la autorización necesaria del Administrador de la Seguridad de la Información.

k) Sólo los canales seguros con autenticación entre el servidor y cliente deben estar disponibles para el acceso remoto. Tanto el servidor y los clientes deben recibir certificados de confianza mutua.

l) El acceso remoto a la información confidencial no se debe permitir. La excepción a esta regla sólo podrá autorizarse en los casos estrictamente necesarios.

m) Las aplicaciones incluirán un adecuado control de acceso basado en el análisis de las funciones que la aplicación tiene desarrolladas y las autorizaciones por gruposde usuarios, roles y perfiles.

n) El personal del HSRP y demás personas no tendrán acceso de escritura a los datos de producción por fuera de los sistemas de información, a excepción del Encargado de la Administración de Base de Datos.

Controles de acceso a las aplicaciones

a) Todo usuario que haya intentado el acceso al sistema en forma fallida registrando erróneamente su contraseña de forma consecutiva hasta cinco (5) veces, su cuenta de usuario será bloqueado automáticamente, para desbloquear su cuenta de forma inmediata deberá informar del hecho a su Jefe inmediato superior; quien deberá enviar un correo electrónico al Área deTecnología de la Información solicitando el desbloqueo de la cuenta, siendo esteprocedimiento no aplicable para los super usuarios.

b) Para todas las cuentas especiales, el desbloqueo debe ser documentado y comunicado al Encargado del Área de Tecnología de la Información.

c) Se debe bloquear toda sesión activa cuando la estación de trabajo no seencuentre en uso durante 15 minutos. Asimismo, se debe utilizar las facilidadesde protector de pantalla con contraseña para las estaciones de trabajo, con activación automática a los 15

minutos de inactividad en el sistema.

d) Cualquier sistema que maneja información valiosa y / o confidencial de la organización debe estar protegida con un sistema de control de acceso basadoen contraseñas.

e) Las aplicaciones incluirán un adecuado control de acceso basado en el análisis de las funciones que la aplicación tiene desarrolladas y las autorizaciones por grupos de usuarios, roles y perfiles.

f) Se debe implementar de manera automática en el sistema un mensaje almomento que el usuario ingresa a los sistemas. El mensaje debe manifestar queel sistema sólo puede ser utilizado para los propósitos autorizados para sus tareas y que el usuario tiene el compromiso de responsabilidad y confidencialidad de su cuenta de usuario asignada y de la información a la que accede.

Política 2: Gestión de los Activos

Propósito. La Política de los activos de Tecnologías de la Información, define los requisitos para elmanejo adecuado y seguro de todos los Activos de Tecnologías de la Información, así como determinar el responsable de realizar la actividad.

Definiciones de la Política. Todos los Activos de Tecnología de la Información, deben ser registrados, clasificados, afectados o asignados para su uso aceptable en las actividades del proceso inmerso.

a) Cada activo de información propiedad del Hospital San Rafael de Pasto, debe estar asignado a un personal de la entidad quien se responsabilizará por el mismo.

b) Cada usuario es responsable de la conservación y utilización de los Activos de Tecnología de la Información que le han sido asignados.

c) En el caso se brinde un activo a un tercero, el jefe del área que recibe el servicio asume la responsabilidad del activo.

d) Todos los Activos de Tecnología de la Información deben mantenerse en lugares apropiados, con restricciones de acceso, condiciones ambientales y el diseño de acuerdo con la clasificación de seguridad y las especificaciones técnicas de los citados activos.

e) Toda adquisición de cualquier naturaleza que haga la entidad en materia de hardware, software, servicios en temas informáticos e información debe tener uncontrol a través del Área de Tecnología de la Información.

f) Se debe realizar un control de todo hardware y software que sea recibido, en cuanto a su ubicación y protección, desde que se adquieren o arriendan, hasta suretiro de uso.

g) El acceso a los Activos de Tecnologías de la Información está prohibido para personas no autorizadas. Los préstamos y movilizaciones de un activo, debe hacerse a través de la gestión de solicitudes de servicio y procesos de gestión de accesos. Los espacios en donde se ubican los Activos de Tecnologías de la Información deben estar ordenados, limpios y libre de objetos que atente contra su funcionamiento. Los colaboradores deben apoyar a la cultura de buen uso y cuidado de los activos.

h) El Equipo de Soporte de Tecnologías de la Información es el único responsable demantener y actualizar las configuraciones. Ningún otro usuario está autorizado a cambiar o actualizar la configuración de los Activos de TIC. Eso incluye la modificación de hardware o software de instalación. Las configuraciones de red, dispositivos móviles, dispositivos de almacenamiento móviles, tarjetas dememoria, memoria flash, chips, entre otras deben ser registradas y autorizadas por el área de Tecnologías de la Información.

i) Los dispositivos de almacenamiento móviles (pendrive) se usan en forma

restringida y temporalmente, deben ser declarados a través de documento, indicando el plazo y las razones de uso.

j) Está terminantemente prohibido la extracción de un Activo de Tecnologías de la Información de las instalaciones que no esté clasificado como un activo portable por el usuario. Es necesario, acreditar el registro de salida y retorno.

k) Todos los Activos de Tecnologías de la Información que sean transportados al exterior de las instalaciones, deben permanecer en posesión del colaborador, evitando su exposición al público.

l) Las pérdidas, robos, daños, manipulación u otro incidente relacionado con los Activos de Tecnologías de la Información que compromete la seguridad, deben ser reportados a la brevedad posible al área de Tecnologías de la Información.

m) En caso de pérdida o robo, se deberá realizar los siguientes pasos:

n) Deberá informar al área de Tecnologías de la Información.

o) Realizar la denuncia policial, la cual deberá ser presentada a la persona encargada del área de Tecnología de la Información; la misma que podrá serverificada, de encontrar alguna observación en dicha denuncia, esta podrá ser considerará como falta grave, debiendo cumplirse la devolución del valordel equipo.

p) Si la pérdida se suscite dentro de un ambiente de la institución, durante el ejercicio de sus funciones, el caso será evaluado por la Alta Gerencia.

q) La reposición del equipo será asumida por el colaborador al 100%, el equipo repuesto deberá ser el mismo modelo (cumpliendo las mismas características señaladas en el acta de entrega), en caso el modelo del equipo quede descontinuado, deberá entregar un modelo cercano al equipoperdido o robado (contando con las mismas características iniciales que se entregaron) en un plazo no mayor a 10 días calendarios, caso contrario se

hará el descuento por planilla de acuerdo al precio actual del mercado.

r) Todos los Activos de Tecnologías de la Información deben pasar por el respectivo mantenimiento acorde a la programación anual de mantenimientos preventivos provista en el plan anual.

Disposición o Reutilización de Equipos de Cómputo y Medios Removibles

a) Cuando sea necesario disponer de algún equipo o medio removible ya sea por daño o por obsolescencia de hardware, se debe realizar una disposición de medios.

b) Identificar si es posible o acceder a la información contenida en el dispositivo de almacenamiento.

c) Si no es posible acceder a la información, se procede a la destrucción del medio de almacenamiento por daño físico irreparable: sacar el disco duro desarmarlo y dañar el disco con un martillo donde se almacena la información y se relaciona en el formato de disposición de medios.

d) Si es posible acceder a la información se debe:

Respaldar mediante copia.

Identificar la valoración del activo según las dimensiones de seguridad de la información (Confidencialidad, integridad, disponibilidad).

Aplicar procedimiento de borrado seguro del medio por medio de blanqueamiento de los sectores

Decidir si se reutiliza o se debe destruir

e) Si la información es clasificada en nivel alto de integridad se debe sacar una imagen del mismo o de sus archivos y calcularse el hash de los mismos utilizando el algoritmo seguro disponible.

f) Si es información catalogada como Altamente confidencial el propietario de esta información deberá Respaldar la información existente en este, cifrarla con contraseña, definir un serial al archivo y la clave de cifrado deberá ser almacenada en un sitio separado y seguro para evitar su perdida en el tiempo, esto podría ser incluso en un correo electrónico, lo importante es que no esté ni lógica ni físicamente en el mismo espacio. El tiempo de caducidad será definido por el propietario del activo.

g) Entendiéndose como información altamente confidencial aquella que se considere como secreto empresarial que es cualquier información no divulgada que una persona natural o jurídica legítimamente posea, que pueda usarse en alguna actividad productiva, industrial o comercial, y que sea susceptible de transmitirse a un tercero, en la medida que dicha información cumpla las siguientes condiciones:

Secreta (La información de un secreto empresarial podrá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o, a los medios o formas de distribución o comercialización de productos o prestación de servicios).

Tenga un valor comercial por ser secreta

Haya sido objeto de medidas razonables tomadas por su legítimo poseedor para mantenerla secreta.

Esta información será clasificada así por Gerencia General

a) Es necesario mantener un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de la infraestructura tecnológica de procesamiento de información, con el fin de identificar y controlar el consumo de recursos y prever su crecimiento de forma planificada.

Periódicamente, se realizarán mediciones de las variables críticas de operación de la

infraestructura tecnológica con el objetivo de verificar el estado y uso de los recursos.

De esta forma, es posible definir proyecciones de crecimiento que aseguren la integridad de procesamiento y disponibilidad de la infraestructura.

Los resultados de dichas mediciones serán analizados y en caso de ser necesario la adquisición de nuevos recursos o elementos para soportar la demanda, se proceda a planificar la consecución de dichos elementos.

Política 3: Seguridad Sobre el Talento Humano

Propósito. Definir claramente las condiciones contractuales y de seguridad, incluyendo los acuerdos de confidencialidad, entregar la debida identificación para el ingreso a los sistemas de información y revocar éstos cuando ya no se usen o la persona esté por fuera de la empresa. Tener un proceso de control disciplinario y/o administrativo dondese evalúen las faltas y den sanciones. Registrar el compromiso de aceptación de uso deequipamiento y normas de seguridad de información de usuarios finales, mediante la firma de documentos de aceptación.

Definiciones de la Política. Todo personal nuevo del HSRP, que hayan aprobado los procesos de selección,deberá conocer, entender, aceptar y asumir sus responsabilidades con respecto ala seguridad de la información, según el rol a desempeñar. Igualmente es responsabilidad de todo personal vinculado a la entidad con anterioridad a la elaboración de este documento, conocer, entender, aceptar y asumir sus responsabilidades con respecto a la seguridad de la información, según el rol a desempeñar.

a) El incumplimiento de esta Política de Seguridad de la Información, así como las normas, procedimientos y formatos que regulan el SGSI que conlleve a un incidente de seguridad, implicará un proceso disciplinario y/o las acciones legalescorrespondientes,

dentro del marco legal vigente, por parte de la entidad para establecer la responsabilidad del usuario involucrado.

b) El término del contrato de trabajo con el HSRP implica el cumplimiento de los procesos de entrega de activos de información y remoción de privilegios sobre la plataforma tecnológica de la entidad.

c) Todos los usuarios deben conocer y dar cumplimiento al manual de uso de la tecnología (uso del correo, uso de las impresoras, navegación en Internet, etc.) establecido por el Área de Tecnología de la Información del HSRP.

Política 4: Capacitación y Entrenamiento

Propósito. Contar con personal de Tecnologías de la Información altamente capacitado y actualizado en la constante modernización de las tecnologías y telecomunicaciones, asícomo también concientizar y sensibilizar a los coladores sobre la seguridad y protección de datos.

Alcance. Aplica al personal de Tecnologías de la Información y los colaboradores del HSRP

Definiciones de la Política. Todo el personal del HSRP será entrenado en los temas de seguridad necesarios para asegurar que se cumpla el esquema de seguridad, evitando su incumplimiento debido a falta de capacitación o desconocimiento del SGSI.

a) Capacitar de manera constante (mínimo una vez al año) al personal encargado de: Seguridad de la Información, Administrador de Redes e Infraestructura, Administradores de Base de Datos, sobre las mejoras de seguridad, nuevas brechas de seguridad, actualizaciones en los programas desarrollados, etc.

Política 5: Seguridad Física y Ambiental

Propósito. Resguardar los centros de datos y las redes, teniendo un control del acceso físico a las instalaciones, protegiéndolo contra amenazas internas y externas.

Definiciones de la Política. Todo el personal del HSRP deberá portar constantemente y en un lado visible su fotocheck que lo identifica como personal de la entidad.

a) Todas las demás personas que hagan su ingreso a las instalaciones de la entidad deberán estar adecuadamente identificadas y anunciar su llegada a través del personal de vigilancia de las instalaciones. Cualquier elemento que entre o salga de las diferentes unidades debe ser anunciado al personal de vigilancia para que este proceda a hacer el registro correspondiente.

b) Las puertas de acceso a las áreas de manipulación o administración de información confidencial o privada deberán permanecer cerradas en todo momento.

c) El HSRP proporcionará el ambiente adecuado para la conservación de medios magnéticos y equipos (extintores, aire acondicionado, ups, etc.).

d) El HSRP mantendrá en condiciones óptimas de limpieza, seguridad, mantenimiento y funcionalidad de cada uno de los elementos que forman parte del centro de cómputo y para el resguardo de los backups de la información, de acuerdo con las recomendaciones que sobre cada uno provea el fabricante.

e) El Área de Tecnología de la Información debe establecer los mecanismos de seguridad necesarios para la correcta protección del Centro de Datos (o centro decómputo), de manera que se mantenga la confidencialidad y seguridad de la información que se procesa, así como la integridad de los equipos.

f) El HSRP mantendrá las condiciones físicas y ambientales óptimas recomendadas

para centros de cómputo, así como controles automáticos para incendio y temperatura (humedad, monitoreo por el CCTV, etc.).

g) El HSRP dispondrá de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

h) El HSRP contara con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del HSRP.

i) El HSRP habilitará un correcto cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

Utilizar piso ducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.

Proteger el cableado de red contra intercepción no autorizada o daño.

Evitar las interferencias entre los cables de energía de los cables decomunicaciones.

Proteger el tendido del cableado troncal (backbone).

Para los sistemas sensibles y críticos se instalará conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.

j) Para los sistemas sensibles y críticos se utilizará rutas o medios de transmisión alternativos.

k) Es responsabilidad del Área de Tecnología de la Información realizar el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor. El responsable de

TI mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

Establecer que sólo el personal de TI autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

Registrar el retiro de equipamiento del área para su mantenimiento.

Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

Política 6: Gestión de las Redes y los Sistemas Informáticos

Propósito. Gestionar todos los accesos a las redes, atacando los primeros frentes como son:alcance del internet, antivirus y acceso remoto.

Definiciones de la Política. El tráfico de Internet se debe supervisar en los cortafuegos. Cualquier ataque o abuso debe ser reportado inmediatamente al responsable de Seguridad de la Información.

a) Los servidores, estaciones de trabajo y equipos deben contener mecanismos para la detección y prevención de ataques y abusos. Estos incluyen firewalls, detecciónde intrusos y otros.

b) Todos los equipos y dispositivos con acceso a la red de la organización deben tener instalado un cliente antivirus con protección en tiempo real.

c) Todos los servidores y estaciones de trabajo de propiedad de la Organización o permanentemente en uso en las instalaciones de la Organización deben tener un antivirus gestionado de forma centralizada. Eso también incluye dispositivos de viaje que se conecta regularmente a la red de la organización, o que se pueden gestionar a través de canales

seguros de Internet.

d) Computadoras de la Organización que trabajan permanentemente en la red de otra organización pueden quedar exentos de la regla anterior si así lo requiere la política de seguridad de la otra organización, siempre y cuando dichos equipos estén protegidos.

e) Todos los antivirus deben actualizar de forma automáticamente su definición de virus. Ello debe ser supervisado para asegurar que se la actualización se llevó a cabo con éxito.

f) Ordenadores visitantes y todos los equipos que se conectan a la red de la Organización están obligados a mantenerse "sanos", es decir, con un antivirus instalado y actualizado. Estos equipos deberán pasar por una revisión previa por parte del personal de Soporte Técnico.

Política 7: Sistemas de Respaldo y Recuperación.

Propósito. Tener sistemas de respaldo y procedimientos de recuperación, protección de medios de almacenamiento y control de acceso

Definiciones de la Política. Toda la información del HSRP debe ser respaldada por medio de copias de seguridad siguiendo el procedimiento adecuado según el componente. Esto incluye la información de las estaciones de trabajo que cada responsable de área considere necesario, previa coordinación con el responsable del Área de Tecnología de la Información para incluirlos en el procedimiento de backup.

a) Es responsabilidad de cada personal del HSRP ubicar en una unidad de red la información referida únicamente a El HSRP que requiera ser respaldada por el Área de Tecnología de la Información.

b) Dentro del personal del Área de Tecnología de la Información debe existir un responsable de la seguridad de los backups.

c) Ningún tipo de información referida a El HSRP puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo. Para estos casos, es responsabilidad de cada usuario replicar la información en los directorios públicosque residen en los servidores y/o repositorios en la nube.

d) Deben existir al menos dos copias de la información, una de las cuales deberá permanecer fuera de las instalaciones de la entidad, con excepción de aquellos archivos que provienen de entidades externas, o que, debido a cambios en la tecnología, no puedan ser duplicados.

e) Es responsabilidad del Área de Tecnología de la Información, definir los periodos de retención y la frecuencia de los Backups que garanticen la continuidadde las operaciones y la consulta histórica de su información.

f) Es responsabilidad del Área de Tecnología de la Información el mantenimiento adecuado de las versiones de las aplicaciones en el medio de almacenamiento utilizado en su momento que le permita atender requerimientos legales o internos.

g) Toda restauración de datos en producción debe ser autorizada por el Área de Tecnología de la Información.

h) Es responsabilidad del Área de Tecnología de la Información garantizar a la entidadque se están recogiendo en forma adecuada los backups de información que garanticen la continuidad de los servicios de la plataforma tecnológica.

i) Es responsabilidad de cada unidad orgánica y del personal mantener depurada la información de sus archivos públicos, como mejor práctica para la optimización del uso de los recursos que entrega la entidad a su personal.

Política 8: Transacciones Electrónicas de Alcance Externo

Propósito. Monitorear la seguridad perimetral del HSRP, asegurando los accesos a losservidores y a la red de la organización.

Definiciones de la Política. Es responsabilidad del Área de Tecnología de la Información contar conlos mecanismos que permitan definir los atributos de acceso definidos por elusuario dueño de los datos.

a) Es responsabilidad del Área de Tecnología de la Información mantener un constante monitoreo sobre la red interna, implementando las herramientas que le permitan detectar, prevenir y recuperarse del código malicioso encontrado en su plataforma tecnológica.

b) Es responsabilidad del Área de Tecnología de la Información mantener un esquema de pruebas de vulnerabilidad a los componentes de la red dependiendodel análisis de riesgos.

c) En los medios y transmisiones electrónicas que El HSRP determine, se deberán mantener esquemas de cifrado que cumplan los requerimientos específicos establecidos para tal fin. Para esto creará una política específica que regule el usode dicho esquema.

d) El HSRP realizará un monitoreo permanente de la red a través de los diferentes logs establecidos y configurados a conveniencia de la entidad. Estos logs serán revisados y analizados de acuerdo con las tareas programadas dentro del Área deTecnología de la Información.

e) Todo el personal del HSRP tiene prohibido instalar o utilizar software o productos sin licencias autorizadas por la entidad. Se exceptúan de esta política los productos de software con licencia de libre utilización o que sean soportados con certificado de propiedad de licencia de terceros. En todo caso, cualquier instalación

de software debe ser solicitada y obtenida a través del Área de Tecnología de la Información.

f) El Área de Tecnologías de la Información mantendrá una lista de las categorías deacceso no permitido para la navegación en Internet. En todas las ocasioneslos intereses, el buen nombre y la seguridad de la Orden deben ser protegidospor todo el personal del HSRP y demás personas que presentan sus servicios.

g) Todas las conexiones de personas terceras a la red interna del HSRP debenser autorizadas, revisadas y monitoreadas por el Área de Tecnología de la Información, según sus requerimientos.

Política 9: Servicio de Correo Electrónico

Propósito. Establecer los requisitos para el uso adecuado de correo electrónico en El HSRP.

Definiciones de la Política

a) Los servicios de correo electrónico serán administrados por el Área de TI.

b) Para la comunicación oficial del HSRP debe utilizarse la cuenta de correo institucional.

c) El acceso a los servicios de correo electrónico estará disponible para todos los usuarios del HSRP, si las condiciones de infraestructura tecnológica y administrativa lo permiten.

d) El correo electrónico institucional es una herramienta de comunicación e intercambio oficial de información y no una herramienta de difusión indiscriminada de información.

e) El uso del servicio de correo electrónico deberá ser exclusivamente para apoyar y mejorar la calidad de las funciones administrativas y técnicas.

f) El Área de TI asignará las cuentas de correo de acuerdo con las licencias disponibles.

g) Está prohibido facilitar u ofrecer las cuentas de correo a terceras personas.

h) El servidor principal de correo electrónico debe mantener actualizada la herramienta de detección de virus para los correos entrantes y salientes.

i) Se prohíbe a los empleados formar parte de cadenas de mensajes o SPAM, ya que esto contribuye a la saturación de las redes de telecomunicación y facilita la divulgación de su cuenta de correo y la proliferación de virus en la red.

j) Se prohíbe a los funcionarios que tengan acceso al servicio de correo electrónico abrir mensajes de procedencia desconocida.

k) Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.

l) Los usuarios deben realizar revisiones periódicas de los mensajes almacenados con el fin de no mantener información innecesaria.

m) El Área de Talento Humano deberá notificar al Área de TI cuando se deba crear,cerrar o inhabilitar una cuenta de correo electrónico.

n) Está prohibida la utilización abusiva del correo electrónico y de las listas de distribución incluyendo la realización de prácticas tales como:

Actividades comerciales privadas.

Propagación de cartas encadenadas o participación en esquemaspiramidales o actividades similares.

El insulto, la amenaza o la difamación a cualquier persona.

Suscribirse a periódicos, revistas, semanarios, buscadores de parejas,chats; ni a ningún otro tipo de actividades o boletines electrónicos que no sea el

estrictamente relacionado con el área profesional de trabajo del funcionario.

Descargar archivos de música, programas, videos, pornografía y cualquier otro tipo de información que no guarde estricta relación con el área profesional del colaborador. El Área de TI procurará tomar las previsionesdel caso para que se bloquee por medio de software especializado, el acceso no autorizado a los servicios antes mencionados.

Política 10: Instalación de Software

Propósito. Prevenir y combatir el uso ilegal de programas de cómputo, con el fin de cumplircon las disposiciones sobre derechos de autor que establece la Ley.

Proteger la información mediante directrices que contribuirán de manera determinante a aumentar la eficiencia en el trabajo y garantizar la continuidad de las operaciones de la empresa.

Definiciones de la Política

Licenciamiento de Software

a) La Oficina de TI, es la única área autorizada para llevar a cabo la administración del software de los equipos del HSRP.

b) La Oficina de TI deberá Mantener bajo custodia las licencias de uso de software

c) La Oficina de TI, llevará un control exacto de las licencias en operación vigentes y el equipo en el cual se encuentra en uso para informar a Gerencia.

d) La Oficina de TI, organizará la inspección de los equipos de cómputo en intervalos regulares.

e) La Oficina de TI, difundirá a los colaboradores las Políticas de Uso de Software.

f) La Oficina de TI, realizará un análisis de necesidades y requerimientos de software, con la finalidad de adquisición.

g) El Área de TI dará la asesoría necesaria a los Usuarios del HSRP en el tema de licencias. Los usuarios deben asegurarse de que disponen de las licencias adecuadas al uso que hagan del respectivo software, ya sea mediante licencias adquiridas de forma centralizada por el HSRP (para software de uso común), porla adquisición individual de las correspondientes licencias, o bien por el uso de software libre. De no ser así, la responsabilidad recaerá totalmente sobre el usuario.

h) El Área Administrativa y Financiera gestionará mediante los presupuestos ordinarios y extraordinarios, la compra de licencias de "software" con la finalidadde que siempre el HSRP se mantenga al día con el uso de licencias.

i) El Área de TI removerá cualquier programa de las máquinas cuando no exista licencia, sin responsabilidad para ésta de los problemas que ocasione directa o indirectamente. Llevará un registro de los programas instalados ilegalmente, paraque, ante la reincidencia de mantener programas instalados en forma ilegal, se proceda a reportar el asunto al Área de Talento Humano o ante las autoridades superiores, para aplicar la sanción que corresponda por desobediencia, lo cual debe tipificarse como falta grave. Para ello, el Área de TI cuidará de no violentar el derecho a la privacidad de las personas, solicitando previamente la autorizaciónal usuario para proceder con la remoción del programa ilegal.

Instalación y Soporte

a) El proceso de Tic es la única área autorizada, así como responsable de realizar la instalación del software y proporcionar soporte del mismo en todos los computadores de la empresa.

b) Si alguna área desea la instalación de un software específico debe notificarlo al área de Tic y solicitar la autorización correspondiente.

c) Los medios de instalación originales o acceso a los portales de descarga serán custodiados por el Área de TI.

d) Software que no puede ser instalado:

Copias ilegales de cualquier programa.

Software descargado de Internet.

Software que no se haya identificado como del HSRP.

Instalaciones no autorizadas o que no hayan sido solicitadas a Tic

Software adquirido para uso personal del usuario (sin fines institucionales)

Software de esparcimiento

e) El uso de cualquier software sin licencia es ilegal y puede exponer a la empresa a sanciones por lo que no se permitirá la utilización de software sin licencia o no autorizado por ningún colaborador. Asimismo, todo colaborador que sea descubierto copiando software de manera ilegal o que copie software para entregarlo a un tercero se le iniciará un proceso disciplinario.

f) Se prohíbe la instalación de software de propiedad del HSRP en equipos que no pertenezcan a la institución. En los casos de convenios de cooperación debe existiruna cláusula que así lo permita.

Política 11: Desarrollo de Software y Soluciones

Propósito. Mitigar los riesgos en la implementación de nuevas soluciones.

Definiciones de la Política

a) Las nuevas aplicaciones que se pongan en operación deben cumplir los requerimientos de seguridad mínimos establecidos para asegurar confidencialidad, integridad y disponibilidad en la información que manejan.

b) El Área de Tecnología de la Información es responsable de mantener a

disposición la infraestructura tecnológica más conveniente de acuerdo con sus requerimientos y lo que ofrece el mercado.

Política 12: Gestión de incidentes de seguridad.

Propósito. Contar con un proceso para la atención, detección, control, tratamiento y respuestade incidentes de seguridad

Definiciones de la Política

a) Todo el personal debe reportar cualquier incidente de seguridad quedetecte, al Encargado de Seguridad de la Información lo antes posible de la formaestablecida en el procedimiento de Gestión de Incidentes.

b) El alcance fundamental es que cualquier personal de TI pueda identificar, clasificar y reportar de manera sencilla los incidentes de seguridad, manteniendo abierta la posibilidad de reportar los incidentes en forma oportuna,de tal forma que siempre haya habilitado por lo menos un mecanismo de reporte.

c) Todos estos incidentes y eventos de seguridad serán monitoreados y cuantificados a través del Sistema de Gestión de la Seguridad de la Información (SGSI), el cual alser un sistema cíclico recibe información de los incidentes y eventos sucedidos, ayudando a identificar cuáles son los que más se repiten o de gran impacto para la entidad; logrando que el sistema mejore constantemente, implementando controles más avanzados o adicionales, y así limitar la frecuencia, daño y costos de ocurrencias futuras.

d) El Encargado de Seguridad de la Información debe realizar el debido estudio y seguimiento de todos los incidentes de seguridad, valiéndose de la asistencia de todos los usuarios involucrados cuando éste lo requiera.

e) Es responsabilidad del Encargado del área de Tecnologías de la Información

mantener actualizadas las estadísticas de mantenimiento de emergencia, clasificadas en técnicas y de usuario, siendo éstas reportadas mensualmente al Gerente del centro.

f) Es responsabilidad del Área de Tecnología de la Información divulgar las estadísticas de mantenimientos de emergencia, clasificados en técnicas y de usuario a las instancias que determine la entidad.

Política 13: Planes de Contingencia

Propósito. Contar con planes para la recuperación ante incidentes que eviten el normal desempeño operativo de los sistemas de cada centro

Definiciones de la Política

a) El HSRP diseñará y mantendrá vigente un Plan de Continuidad de Operaciones que atienda los requerimientos de Seguridad de la Información en laentidad según el análisis de riesgos determinado para tal fin, el cual deberáestar catalogado por niveles (1,2,3) de acuerdo con el grado de contingencia que se deba atender, por ejemplo: Grado 1, contingencias menores que se atienden con el personal dentro de las instalaciones. Grado 2, que no se permita el ingresoal edificio, grado 3, por desastre.

b) La entidad realizará pruebas periódicas y mantenimiento al Plan de Continuidad de Operaciones por lo menos UNA vez en el año.

c) La entidad contará con un contrato de custodia externa de la información, como parte del plan de continuidad de operaciones.

Política 14: Sobre la Documentación

Propósito. Contar con toda la documentación y registros en general del HSRP.

Definiciones de la Política

a) Todos los procedimientos operativos del HSRP estarán adecuadamente

documentados, mantenidos y a disposición de los usuarios a quienes compete.

b) Es responsabilidad del Área de Tecnología de la Información, mantener debidamente actualizada toda la documentación referente a laplataforma tecnológica de la entidad.

Política 15. Escritorio Limpio Pantalla Limpia

Propósito. Prevenir la perdida, daño o robo de la información que se encuentre disponible en las estaciones de trabajo y equipos de cómputo.

Definiciones de la Política

a) Todo usuario al terminar su labor cotidiana debe cerrar su sesión y apagar su equipo o PC antes de retirarse; asimismo, cuando deba ausentarse por comisión de servicio, vacaciones, licencias u otro motivo. salvo en casos en que tenga asignada una cuenta de acceso remoto y/o sistemas en nube para trabajo a distancia.

b) Conservar sobre el escritorio únicamente las cosas que necesita para ejercer su trabajo.

c) Archivar carpetas, documentos o medios extraíbles que no se necesiten en el momento y con mayor razón si son activos de la información críticos, guardarlos en un archivador y bajo llave.

d) Si debe ausentarse de su puesto de trabajo por cierto lapso de tiempo asegúrese de no dejar información sensible sobre su escritorio.

e) Al finalizar su jornada laboral no deje documentos sobre él, a fin de conservar la seguridad de la información, es fundamental que archive debidamente los documentos.

f) Cuando se imprima información clasificada o sensible, se debe retirar inmediatamente de la impresora.

g) No utilizar como papel de reciclaje hojas impresas con información sensible.

h) Cuando se reciba soporte técnico remoto se debe cerrar archivos y salir de programas que no se relacionen con el soporte a recibir.

i) Cuando se reciba soporte técnico, se debe hacer con la supervisión del usuario a cargo del equipo de cómputo.

Política 16: Relación con los Proveedores

Propósito. Proteger los activos de la información de uso indebido de la información por parte de los proveedores.

Definiciones de la Política

a) Todos los proveedores con los que la empresa tiene contratos y que tengan acceso a información de la empresa, deberán acogerse a los siguientes lineamientos:

b) Todo proveedor y sus colaboradores deberán cumplir con las Políticas y lineamientos de seguridad de la información establecidos por la empresa.

c) Todo proveedor deberá firmar un contrato donde se estipule además de las cláusulas normales de la prestación de los servicios, las cláusulas de confidencialidad y no divulgación y los términos durante y después de finalizado el contrato con respecto a la seguridad de la información y el proveedor a su vez deberá extender esta confidencialidad a los colaboradores que participen del objeto contractual.

d) Los proveedores deberán hacer reporte de las debilidades de seguridad que puedan encontrar durante la ejecución del contrato.

e) Todo proveedor adquiere el compromiso de reportar los impactos de los cambios aplicados en producción a los procesos y subprocesos de la empresa, desde la realización de las pruebas hasta la salida a producción del requerimiento y/o servicio.

f) Los Supervisores de contratos con proveedores, deben administrar los cambios en el suministro de servicios por parte de los mismos, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

g) Todos los proveedores deberán en caso de un evento de seguridad de la información hacer el reporte conforme al procedimiento de reporte de incidentes establecido como proceso interno de la empresa.

h) Se deberá realizar transferencia de conocimiento y/o acompañamiento a los funcionarios responsables del proceso en la empresa.

i) Los proveedores tienen el compromiso de aportar y realizar sugerencias para el mejoramiento de los procesos y óptimo aprovechamiento del servicio que se está prestando.

j) Se deberá por parte del proveedor entregar reporte de actividades realizadas el cual debe estar soportado por las evidencias del servicio prestado ya se actas, fotos, manuales, videos, formatos de recepción del servicio por el usuario de la empresa que lo recibió.

k) El Supervisor de los contratos evaluará periódicamente el cumplimiento del objeto del contrato y de las normas de seguridad de la empresa.

Documentación para SGSI

El Sistema de Gestión de Seguridad de la Información (SGSI) del Hospital San Rafael tiene como objetivo proteger la confidencialidad, integridad y disponibilidad de la información crítica La seguridad de la información es esencial para garantizar la privacidad de los pacientes, el cumplimiento normativo y la eficiencia operativa del hospital.

La documentación de este SGSI está dirigida al proceso de Gerencia de la Información, estableciendo directrices claras para la gestión de la seguridad de los datos del proceso. Incluye un procedimiento formalizado para la implementación y mejora continua de medidas de seguridad, junto con formatos específicos para asegurar su cumplimiento.

El SGSI se basa en el principio de mejora continua y el cumplimiento de normas internacionales como ISO/IEC 27001, buscando adaptarse a nuevos riesgos y necesidades del entorno. Esta documentación es esencial para los responsables de la Gerencia de la Información y todo el personal involucrado en la gestión de la seguridad de la información, promoviendo una cultura organizacional comprometida con la protección de los datos y el cumplimiento de normativas.

Se propone un procedimiento para el SGSI, junto con los formatos necesarios para su implementación y seguimiento.

Procedimiento de SGSI para el Hospital San Rafael

Objetivo

Establecer los lineamientos y actividades necesarios para implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) del Hospital San Rafael de Pasto, asegurando la confidencialidad, integridad y disponibilidad de la información.

Alcance

El presente procedimiento aplica desde la definición del alcance del SGSI hasta su certificación, abarcando las actividades de análisis de riesgos, implementación de controles, monitoreo, revisión y mejora continua, cubriendo todos los procesos y activos de información críticos del hospital.

Definiciones

SGSI: Sistema de Gestión de Seguridad de la Información basado en ISO 27001:2022.

Activo de Información: Cualquier recurso que tiene valor para la organización y requiere protección.

Riesgo: Probabilidad de que ocurra un evento que impacte la seguridad de la información.

Control de Seguridad: Medida implementada para mitigar riesgos a la información.

Condiciones Generales

Todo colaborador debe conocer las políticas de seguridad de la información y cumplir con ellas.

Las actividades deben realizarse según los principios de mejora continua establecidos en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar).

Los incidentes deben reportarse a la mesa de ayuda para su gestión oportuna.

Tabla 3

Descripcion del Proceso

No	Actividad	Responsable	Descripcion	Documento
1	Definición del alcance del SGSI	Gestor TIC, Dirección	Identificar procesos y activos de información relevantes. Documentar el alcance del SGSI incluyendo áreas, recursos y partes interesadas.	Informe de Alcance
2	Análisis de riesgos	Gestor TIC, Analista de Riesgos	Aplicar la metodología MAGERIT para identificar activos, amenazas y vulnerabilidades. Evaluar riesgos y definir el nivel de aceptación de los mismos.	Matriz de Riesgos
3	Plan de tratamiento de riesgos	Gestor TIC, Dirección	Diseñar estrategias para mitigar, transferir, aceptar o eliminar riesgos. Establecer controles alineados con el Anexo A de ISO 27001.	Plan de Tratamiento
4	Implementación de controles	Gestor TIC, Equipo TIC	Desarrollar e implementar controles técnicos, organizativos y físicos como: autenticación multifactor, respaldos, segregación de funciones y capacitaciones.	Manuales y Registros
5	Desarrollo de documentación del SGSI	Gestor TIC, Documentación	Elaborar políticas, procedimientos, instructivos y formatos necesarios para garantizar la operatividad del SGSI.	Procedimientos Documentados
6	Monitoreo y medición	Gestor TIC	Elaborar políticas, procedimientos, instructivos y formatos necesarios para garantizar la operatividad del SGSI.	Informes de Auditoría
7	Revisión y mejora continua	Dirección, Gestor TIC	Revisar periódicamente el desempeño del SGSI y tomar acciones correctivas y preventivas basadas en los resultados.	Informe de Revisión
8	Certificación del SGSI	Dirección, Gestor TIC	Contratar una entidad certificadora que valide el cumplimiento con ISO 27001:2022 y mantener la certificación mediante auditorías externas.	Certificado de Cumplimiento

Nota. Elaboración propia que describe las etapas del proceso de implementación de un SGSI conforme a la norma ISO/IEC 27001:2022, incluyendo desde la definición del alcance hasta la certificación.

Documentos de Referencia

- Norma ISO 27001:2022: Requisitos para sistemas de gestión de la seguridad de la información.
- Manual de Seguridad del Hospital: Políticas y lineamientos internos.
- Plan de Tratamiento de Riesgos: Estrategias y controles establecidos para la mitigación de riesgos.

Tabla 4

Control de Cambios

Revision	*Fecha*	*Modificado Por*	*Descripcion*
1	17/12/2024	Sandra Jimena Burbano	Creación inicial del procedimiento para implementar el SGSI basado en ISO 27001:2022.

Nota. Elaboración propia que describe el control de cambios del procedimiento de un SGSI conforme a la norma ISO/IEC 27001:2022.

Formatos para el SGSI

Formato 1: Informe de Alcance del SGSI

Nombre del Documento: Informe de Alcance del SGSI

Código: GI-SGSI-01

Contenido

- Fecha:

- Preparado por:
- Revisado por:
- Aprobado por:
- Descripción del Alcance:
  - Áreas Incluidas:
  - Activos Gestionados:
  - Límites del SGSI:
  - Exclusiones:
- Observaciones:

Formato 2: Matriz de Riesgos

Nombre del Documento: Matriz de Riesgos del SGSI

Código: -SGSI-02

Tabla 5

Formato de Matriz de Riesgo

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Control Aplicado	Estado
Servidor X	Ataque DDoS	Falta de mitigación	Alto	Medio	Alto	Firewall Avanzado	Implementado

Nota. Elaboración propia que describe el formato de Matriz de Riesgo, conforme a la norma ISO/IEC 27001:2022.

Formato 3: Plan de Tratamiento de Riesgos

Nombre del Documento: Plan de Tratamiento de Riesgos

Código: GI-SGSI-03

Tabla 6

Plan de Tratamiento de Riesgos

Riesgo Identificado	Estrategia	Control Propuesto	Responsable	Fecha de Implementación	Estado
Pérdida de datos	Mitigar	Respaldos automáticos	Gestor TIC	DD/MM/AAAA	En Proceso

Nota. Elaboración propia que describe el plan de tratamiento de Riesgo, conforme a la norma ISO/IEC 27001:2022.

Formato 4: Registro de Incidentes de Seguridad

Nombre del Documento: Registro de Incidentes

Código: GI-SGSI-04

Contenido

Fecha del Incidente:

Tipo de Incidente:

Descripción:

Activo Afectado:

Impacto:

Acción Tomada:

Estatus del Incidente:

Comentarios:

Formato 5: Lista de Control de Activos de Información

Nombre del Documento: Lista de Activos de Información

Código: GI-SGSI-05

Tabla 7

Lista de Control de Activos de Información

Activo	Tipo	Ubicación	Propietario	Valoración de Seguridad
Servidor Principal	Hardawre	Data Center	Gestor Tics	Alto

Nota. Elaboración propia que describe la lista de control de activos de la informacion, conforme a la norma ISO/IEC 27001:2022.

Formato 6: Informe de Auditoría Interna

Nombre del Documento: Informe de Auditoría Interna

Código: GI-SGSI-06

Contenido

Fecha de Auditoría:

Auditor:

Aspectos Evaluados:

Hallazgos:

Conformidades:

No Conformidades:

Acciones Correctivas Propuestas:

Observaciones Generales:

Formato 7: Informe de Revisión por la Dirección

Nombre del Documento: Informe de Revisión

Código: GI-SGSI-07

Contenido

Fecha de Reunión:

Participantes:

Aspectos Revisados:

Desempeño del SGSI

Indicadores Clave

Cambios en el Contexto

Decisiones Tomadas:

Acciones Pendientes:

Recomendaciones

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo requiere no solo el cumplimiento de normas y procedimientos técnicos, sino también el compromiso y la participación de todos los miembros de la organización. En este contexto, las recomendaciones presentadas a continuación buscan fortalecer las prácticas de seguridad de la información a través de enfoques estratégicos y operativos que aseguren una protección integral de los datos. Estas recomendaciones están orientadas a mejorar la capacitación, sensibilización y la cultura organizacional en cuanto a la seguridad de la información, garantizando que todos los colaboradores comprendan y asuman su responsabilidad en la gestión y protección de los datos. Implementar estas acciones permitirá a la organización mitigar riesgos, cumplir con los estándares internacionales y crear un entorno más seguro y resiliente.

Realizar una auditoría inicial estructurada para evaluar el cumplimiento del proceso de Gerencia de la Información con la norma NTC-ISO-IEC 27001:2022. Esto incluye la revisión documental, entrevistas con el equipo involucrado y la observación de actividades operativas. Es clave usar herramientas de evaluación, como el instrumento de análisis de requisitos y el del anexo A, empleando la escala de madurez para identificar el estado de los controles desde "Desconocido" hasta "Optimizado". El informe final debe detallar el nivel de cumplimiento, identificar brechas, y ofrecer recomendaciones específicas para mejorar el SGSI, estableciendo una base sólida para futuras acciones.

Implementar de manera prioritaria el Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2022. Este proyecto es fundamental para proteger la confidencialidad, integridad y disponibilidad de la información crítica del hospital. Los principales beneficios de implementar este SGSI serían:

Mitigar los riesgos de seguridad identificados, especialmente en los activos considerados como críticos, como el Sistema de Información Dinámica Gerencial y los discos duros con copias de seguridad. Esto garantizaría la continuidad operativa y la calidad de los servicios médicos.

Fortalecer el cumplimiento de normativas internacionales y buenas prácticas en seguridad de la información, lo que reforzaría la confianza de pacientes, colaboradores y terceros en los procesos del hospital.

Promover una cultura organizacional orientada a la ciberseguridad mediante la implementación de controles técnicos, físicos y administrativos alineados con la norma ISO 27001.

Mejorar la resiliencia del hospital frente a incidentes de seguridad, al contar con procesos definidos para la prevención, detección y respuesta oportuna.

Posicionar al Hospital San Rafael como un referente en seguridad de la información en el sector salud, lo que le otorgaría ventajas competitivas y de prestigio.

Implementar un programa integral para fomentar una cultura de seguridad de la información en toda la organización. Este programa debe incluir actividades de sensibilización y capacitación dirigidas a todos los colaboradores, destacando su responsabilidad en el cumplimiento de las políticas y procedimientos establecidos.

Las capacitaciones deben ser periódicas, interactivas y adaptadas a los diferentes roles dentro de la organización, abordando temas clave como la protección de datos, identificación de riesgos y mejores prácticas para prevenir incidentes de seguridad. Adicionalmente, se sugiere realizar campañas de concienciación mediante boletines, carteles informativos y correos electrónicos para reforzar los mensajes clave de seguridad.

Conclusiones

A continuación, se presentan las conclusiones derivadas del proceso de análisis y evaluación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Hospital San Rafael de Pasto. Estas conclusiones resumen los aspectos clave identificados a lo largo del proyecto, destacando la importancia de implementar un SGSI conforme a la norma ISO 27001:2022 y los beneficios que este sistema traerá tanto para la protección de la información como para el fortalecimiento de la organización. Además, se resalta la metodología adoptada para llevar a cabo este proceso, que combina diversas herramientas y enfoques para garantizar una implementación efectiva y adaptada a las necesidades específicas del hospital.

Hospital San Rafael de Pasto ha identificado de manera clara la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los lineamientos de la norma ISO 27001:2022, con el objetivo primordial de garantizar la protección de la información confidencial de los pacientes. Este sistema es esencial para asegurar el cumplimiento de las regulaciones y normativas específicas del sector salud, que requieren elevados estándares de protección de datos.

El propósito de la implementación del SGSI es reforzar la seguridad de la información, minimizando los riesgos de filtración o pérdida de datos, y al mismo tiempo, fomentar una cultura organizacional sólida de seguridad informática, en la que cada colaborador se sienta responsable de proteger la información manejada en el hospital.

El éxito de este proyecto no solo representará un avance significativo en la protección de la información, sino que también será una inversión estratégica para el hospital. Mejorará la continuidad de los servicios médicos, fortalecerá la confianza de los

pacientes y contribuirá al posicionamiento positivo de la institución, resguardando su reputación ante posibles incidentes de seguridad.

El análisis de contexto es un paso crucial para comprender las necesidades y particularidades del hospital, lo que permitirá desarrollar un SGSI robusto y adaptado a su entorno específico. Además, se implementará una metodología rigurosa que combina técnicas cuantitativas y cualitativas, utilizando herramientas como el análisis documental, entrevistas, talleres colaborativos y revisiones bibliográficas, con el fin de asegurar que el SGSI se construya sobre una base sólida, enfocada en la mejora continua y en la protección efectiva de la información.

Referencias Bibliografícas

AGESIC. (2012). Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC), Guía Metodológica Implantación de un SGSI. Uruguay.

Aliaga, L. (2013). Diseño de un sistema de gestión de seguridad de información para un instituto educativo. Tesis de especialización Lima, Perú: Pontifica Universidad Católica del Perú. Facultad de Ciencias e Ingeniería.

Alvarado, C. (sf). Sistema de gestión de seguridad de la información: qué es y sus etapas. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

Alvares, J. (2016). Diseño de un sistema de gestión de seguridad de la información - SGSI basado en la norma ISO27001 para el colegio pro-colombiano de la ciudad de Bogotá, que incluye: asesoría, planeación. Tesis de especialización Bogotá, Colombia: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería.

Chardon, A y González, J. (2002). Indicadores para la Gestión de Riesgos. Universidad Nacional de Colombia – Sede Manizales. Colombia.

Chiavenato, I. (2006). Introducción a la Teoría General de la Administración, Séptima Edición, McGraw-Hill Interamericana.

Colombia.com. (2023, September 15). ¿Qué está pasando con Sanitas? La EPS confirma que fueron hackeados. Esto es lo que se sabe. Colombia.com. https://www.colombia.com/actualidad/nacionales/que-esta-pasando-con-sanitas-la-eps-confirma-que-fueron-hackeados-esto-es-lo-que-se-sabe-378917

Coral, J. (2016). Diseño de un sistema de gestión de seguridad para la red de datos bajo la

norma ISO27001:2013 en el centro de estudios EMSSANAR CETEM de la ciudad de Pasto. Tesis de especialización Pasto, Colombia. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería.

Córdova, C., Morales, G., y Samamé, J. (2015). Desarrollo de un SGSI para los Colegios Profesionales en la Región Lambayeque. Caso de estudio: Colegio de Ingenieros. Chiclayo, Perú: Revista de la Universidad Católica Santo Toribio de Mogrovejo.

Diaz, A., Collazos, G., Ortiz, L. Herazo, G.. (2013). Implementación de un sistema de gestión de seguridad de la información (sgsi) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma ISO 27001, 2011

Fiorito, F. (2006). La simulación como una herramienta para el manejo de la incertidumbre. Buenos Aires, Argentina. Universidad del CEMA.

Fiorito, F. (2006). La Simulación como una herramienta para el manejo de la incertidumbre. Universidad del CEMA, Master en finanzas. 2006

Fundación Carlos Slim. (2015). Vulnerabilidades Informáticas. Técnico en seguridad informática.

García, M. (1998). Francisco Javier. El concepto de información: Una aproximación trandisciplinar. Universidad de Zaragoza. España.

Hurtado, M. (2012). MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. En Gestión de riesgo: Metodologías OCTAVE y MAGERIT (Universidad Piloto de Colombia).

Hyperconectado. (2023). Despliegan estrategia de estafa digital con información médica de pacientes de EPS Sura. https://muchohacker.lol/2023/02/despliegan-estrategia-de-estafa-digital-con-informacion-medica-personal-de-pacientes-de-eps-sura/

IBM. (2024). IBM Security X-Force Threat Intelligence Index 2024. IBM. https://www.ibm.com/reports/threat-intelligence

ICONTEC, Instituto Colombiano de Normas Técnicas y Certificación. Norma técnica NTC-ISO/IEC Colombiana 27001. Sistema de Gestión de la Seguridad de la Información.

Icontec. (2006). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos (Apartado 14237). Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

INCIBE. (2016, diciembre 29). Inventario de activos y gestión de la seguridad en SCI. Recuperado de https://www.incibe-cert.es

Infobae. (2022, December 21). Ciberataque a EPS Sanitas: Se habrían filtrado datos personales de pacientes y empresas. Infobae. https://www.infobae.com/america/colombia/2022/12/21/ciberataque-a-eps-sanitas-se-habrian-filtrado-datos-personales-de-pacientes-y-empresas/

Infobae. (2023, September 15). Gobierno hizo balance del grave ciberataque que afecta las instituciones en Colombia: Fueron afectados 55 millones de datos del Ministerio de Salud. Infobae. https://www.infobae.com/colombia/2023/09/15/gobierno-hizo-balance-del-grave-ciberataque-que-afecta-las-instituciones-en-colombia-fueron-afectados-55-millones-de-datos-del-ministerio-de-salud/

Ingenio Learnig. (2022). SGSI: ¿Qué es un sistema de gestión de seguridad de la información? https://ingenio.edu.pe/blog/sgsi-que-es-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Ingenio. (2022, June 14). SGSI: ¿Qué es un sistema de gestión de seguridad de la información? Ingenio. https://ingenio.edu.pe/blog/sgsi-que-es-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Instituto colombiano de normas técnicas y certificación. Tecnología de la información. Técnicas de seguridad. Sistemas, gestión de la seguridad de la información (sgsi). Requisitos. Bogotá, Icontec, 2013. p. 2 (ntc-iso/iec 27001)

Instituto Nacional de Salud (INS). (2023). Ministerio de Salud emitió circular tras ciberataque, estas son las medidas del plan de contingencia. https://www.semana.com/salud/articulo/ministerio-de-salud-emitio-circular-tras-ciberataque-estas-son-las-medidas-del-plan-de-contingencia/202342/

Intobae. (2023). Ciberataque a EPS Sanitas: se habrían filtrado datos personales de pacientes y empresas. https://www.infobae.com/america/colombia/2022/12/21/ciberataque-a-eps-sanitas-se-habrian-filtrado-datos-personales-de-pacientes-y-empresas/

Jiménez, M. M. (2022, septiembre 14). Riesgos informáticos más comunes a los que se exponen las empresas

Mañas, J. A. (2006). MAGERIT – Versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Administraciones Públicas

Paulus, N. (2004). el concepto de Riesgo: Conceptualización del Riesgo en Luhmann y Beck. Colombia. Universidad de Chile. Departamento de Antropología.

Pinzón, S. (2022). Ataque cibernético a Sanitas, Colsanitas y Medisanitas: ¿Está en riego la información de los usuarios?https://www.colombia.com/actualidad/nacionales/que-esta-pasando-con-sanitas-la-eps-confirma-que-fueron-hackeados-esto-es-lo-que-se-sabe-378917

Protecdata. (n.d.). Estafa digital con información médica personal de pacientes de EPS Sura. Protecdata. https://protecdatalatam.com/noticias/estafa-digital-con-informacion-medica-personal-de-pacientes-de-eps-sura/

Pulido, C. (2015). Diseño de un sistema de gestión de seguridad e la información para las áreas administrativa y académica de la institución System Plus Pasto LTDA, basado en el estándar internacional ISO/IEC 27001:2013. Tesis de especialización Pasto, Colombia: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería.

Quodem. (2024). ISO 27001 en el sector salud: 10 razones para contar con un partner acreditado. https://quodem.com/blog/iso-27001-en-el-sector-salud-10-razones-para-contar-con-un-partner-acreditado/

Quodem. (n.d.). ISO 27001 en el sector salud: 10 razones para contar con un partner acreditado. Quodem. https://quodem.com/blog/iso-27001-en-el-sector-salud-10-razones-para-contar-con-un-partner-acreditado/

Revista Semana. (2023). Ministerio de Salud y Superintendencia de Salud también fueron blanco del ataque cibernético; evalúan si hay secuestro de información. https://www.semana.com/nacion/articulo/ministro-de-salud-confirma-que-fueron-34-instituciones-publicas-atacadas-ciberneticamente-tecnicos-evaluan-si-se-presento-secuestro-de-informacion/202343/

RIOS, J. (2013). El concepto de información: dimensiones bibliotecológica, sociológica y cognoscitiva. Instituto de Investigaciones Bibliotecológicas y de la Información de la UNAM. México.

Ruiz, J. (2005). De la construcción social del riesgo a la manifestación del desastre: Reflexiones en torno al imperio de la vulnerabilidad. Desacatos, (19):99–110

Ruiz, N. (2011). La definición y medición de la vulnerabilidad social. Un enfoque normativo. Departamento de Geografía Social, Instituto de Geografía, Universidad Nacional Autónoma de México, Circuito de la Investigación Científica, 04510, Coyoacán, México.

Sáenz, H. (2025). Gobierno hizo balance del grave ciberataque que tiene en problemas a varias entidades: fueron afectados 55 millones de datos del Ministerio de Salud. https://www.infobae.com/colombia/2023/09/15/gobierno-hizo-balance-del-grave-ciberataque-que-afecta-las-instituciones-en-colombia-fueron-afectados-55-millones-de-datos-del-ministerio-de-salud/

Salgueiro, A. (2001). Indicadores de Gestión y Cuadro de Mando. Editorial Díaz de Santos. Madrid España,

Semana. (2023, April 2). Ministerio de Salud emitió circular tras ciberataque: Estas son las medidas del plan de contingencia. Semana. https://www.semana.com/salud/articulo/ministerio-de-salud-emitio-circular-tras-ciberataque-estas-son-las-medidas-del-plan-de-contingencia/202342/

Semana. (2023, September 15). Ministro de Salud confirma que fueron 34 instituciones públicas atacadas cibernéticamente: Técnicos evalúan si se presentó secuestro de información. Semana. https://www.semana.com/nacion/articulo/ministro-de-salud-confirma-que-fueron-34-instituciones-publicas-atacadas-ciberneticamente-tecnicos-evaluan-si-se-presento-secuestro-de-informacion/202343/

Solarte, J., Rosero, J., & Benavides, A. (año). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001

Tarazona, C. (2014). Amenazas Informáticas y de Seguridad de la Información. 2014

UNESCO. 2011). Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), Manual De Gestión De Riesgos De Desastre Para Comunicadores Sociales, Perú.

UNIR. (2021, junio 16). Qué es la seguridad informática y cuáles son sus tipos. Wikipedia. Última consulta: 28 de septiembre de 2015, de https://es.wikipedia.org/wiki/Riesgo_(inform%C3%A1tica)

Apéndice

Apéndice A

Estado de implementation norma ISO 27001

Estado de Implementación ISO 27001

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios
4	**Contexto de la organización**				
4,1	**Comprensión de la organización y de su contexto**				
4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inicial			
4,2	**Comprensión de las necesidades y expectativas de las partes interesadas**				
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Definido			
4.2 (b)	Determinar los requerimientos y oblicaciones relevantes de seguridad de la información	Inexistente			
4,3	**Determinación del alcance del SGSI**				
4,3	Determinar y documentar el alcande del SGSI	Inexistente		Documentación obligatoria ¿Existe el documento?	
4,4	**SGSI**				
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estandar	Inexistente			El proces se esta iniciando
5	**Liderazgo**				
5,1	**Liderazgo y compromiso**				
5,1	La administración debe demostrart liderazgo y compromiso por el SGSI	Inicial			El proces se esta iniciando
5,2	**Política**				
5,2	Documentar la Política de Seguridad de la Informacion	Inexistente		Documentación obligatoria ¿Existe el documento?	
5,3	**Roles, responsabilidades y autoridades en la organización**				
5,3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Inexistente			
6	**Planificación**				
6,1	**Acciones para tratar los riesgos y oportunidades**				
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportinidades	Inexistente			No se cuenta
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Inexistente		Documentación obligatoria ¿Existe el documento?	No se cuenta
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Inexistente		Documentación obligatoria - Controles Anexo A ¿Existe el documento?	No se cuenta
6,2	**Objetivos de seguridad de la información y planificación para su consecución**				
6,2	Establecer y documentar los planes y objetivos de la seguridad de la información	Inexistente		Documentación obligatoria ¿Existe el documento?	
7	**Soporte**				
7,1	**Recursos**				
7,1	Determinar y asignar los recursos necesaraios para el SGSI	Inexistente			
7,2	**Competencia**				
7,2	Determinar, documentar hacer disponibles las competencias necesarias	Inexistente		Documentación obligatoria ¿Existe el documento?	
7,3	**Concienciación**				
7,3	Implementar un programa de concianciación de seguridad	Inexistente			
7,4	**Comunicación**				
7,4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Inexistente			
7,5	**Información documentada**				
7.5.1	Proveer documentacion requerida por el estandar más la requerida por la organización	Inexistente			
7.5.2	Proveer un titulo, autor, formato consistente, revisión y aprobacion a los documentos	Inexistente			
7.5.3	Mantener un control adecuado de la documentación	Inexistente			
8	**Operación**				
8,1	**Planificación y control operacional**				
8,1	Planificar, implementar, controlar y documentar el proceso de gestion de riesgos del SGSI (Tratamiento de riesgos)	Inexistente		Documentación obligatoria ¿Existe el documento?	
8,2	**Apreciación de los riesgos de seguridad de la información**				
8,2	Evaluar y documentar los riesgos de seguridad regularment y cuando hay cambios	Inexistente		Documentación obligatoria ¿Existe el documento?	
8,3	**Tratamiento de los riesgos de seguridad de la información**				
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Inexistente		Documentación obligatoria ¿Existe el documento?	
9	**Evaluación del desempeño**				
9,1	**Seguimiento, medición, análisis y evaluación**				
9,1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Inexistente		Documentación obligatoria ¿Existe el documento?	
9,2	**Auditoría interna**				
9,2	Planificar y realizar una auditoria interna del SGSI	Inexistente		Documentación obligatoria ¿Existe el documento?	
9,3	**Revisión por la dirección**				
9,3	La administración realiza una revision periodica del SGSI	Inexistente		Documentación obligatoria ¿Existe el documento?	
10	**Mejora**				
10,1	**No conformidad y acciones correctivas**				
10,1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Inexistente		Documentación obligatoria ¿Existe el documento?	
10,2	**Mejora continua**				
10,2	Mejora continua del SGSI	Inexistente			

Apéndice B

Estado y aplicabilidad de controles de Seguridad de la Informacion

Estado y Aplicabilidad de controles de Seguridad de la Información					
Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas	Comentarios
A5	**Políticas de seguridad de la información**				
A5.1	**Directrices de gestión de la seguridad de la información**				
A5.1.1	Políticas para la seguridad de la información	Inexistente		¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada? ¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes? ¿Cómo se autorizan, comunican, comprenden y aceptan las políticas? ¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores? ¿Hay acuerdos adecuados de cumplimiento y refuerzo? ¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)? ¿Están las políticas bien escritas, legible, razonable y viable? ¿Incorporan controles adecuados y suficientes? ¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.? ¿Cuán madura es la organización en esta área?	
A5.1.2	Revisión de las políticas para la seguridad de la información	Inexistente		¿Todas las políticas tienen un formato y estilo consistentes? ¿Están todos al día, habiendo completado todas las revisiones debidas? ¿Se han vuelto a autorizar y se han distribuido?	
A6	**Organización de la seguridad de la información**				
A6.1	**Organización interna**				
A6.1.1	Roles y responsabilidades en seguridad de la información	Inexistente		¿Se le da suficiente énfasis a la seguridad y al riesgo de la información? ¿Hay apoyo de la administración? ¿Existe un foro de alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad? ¿Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas? ¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información? ¿Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información? ¿Hay coordinación dentro de la organización entre las unidades de negocio? ¿funciona efectivamente en la práctica? ¿Existe una conciencia y un apoyo adecuados para la estructura de riesgo y seguridad de la información?	
A6.1.2	Segregación de tareas	Inicial		¿Son los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas? ¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea? Responsable | Accountable | Consulted | Informed ¿Existe una política que cubra la segregación de deberes? ¿Cómo llegan las decisiones con respecto a tal segregación? ¿Quién tiene la autoridad para tomar tales decisiones? ¿Se realiza un seguimiento regular de las actividades y los registros de auditoría?	
A6.1.3	Contacto con las autoridades	? Desconocido		¿Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias? ¿Quién es el responsable de contactar a las autoridades y en qué punto de un incidente / evento se realiza este contacto y cómo? ¿La lista es actual y correcta? ¿Hay un proceso de mantenimiento?	
A6.1.4	Contacto con grupos de interés especial	Administrado		¿Hay un contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad, tales como los capítulos locales de ISACA, ISC 2, ISSA, ISO27k? ¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches?	
A6.1.5	Seguridad de la información en la gestión de proyectos	Inexistente		¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes? ¿La etapa del proyecto incluye actividades apropiadas?	
A6.2	**Los dispositivos móviles y el teletrabajo**				
A6.2.1	Política de dispositivos móviles	Inexistente		¿Existen política y controles seguridad relacionados con los usuarios móviles? ¿Se distinguen los dispositivos personales de los empresariales? ¿Cómo se mantienen y controlan los sistemas portátiles para garantizar que estén actualizados sobre las definiciones de antivirus y los parches de seguridad? ¿Se emplean soluciones de MDM y soluciones MAM para controlar las aplicaciones, el acceso y el cifrado completo de disco?	
A6.2.2	Teletrabajo	Inexistente		¿Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina? ¿Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (Always-on-VPN), antivirus, copias de seguridad, parches, registro de seguridad y monitoreo, encriptación y continuidad del negocio?	

A7	Seguridad relativa a los recursos humanos				
A7.1	**Antes del empleo**				
A7.1.1	Investigación de antecedentes	Definido		¿El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo? ¿Se hace en la empresa o se subcontrata a un tercero? Si se subcontrata a un tercero, ¿Se han revisado sus procesos y se han considerado aceptables? ¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección? ¿Existen procesos de selección mejorados para los trabajadores en roles críticos? ¿Cómo se logra todo esto? ¿Hay un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH?	
A7.1.2	Términos y condiciones del empleo	? Desconocido		¿Están claramente definidos los términos y condiciones de empleo? ¿Se hace distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general? ¿Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles? ¿Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información?	
A7.2	**Durante el empleo**				
A7.2.1	Responsabilidades de gestión	Inexistente		¿Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia? ¿Se hace de forma regular y está a día? ¿El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados? ¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad? ¿Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización?	
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inexistente		¿Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente? ¿Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores? ¿Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos? ¿Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos? ¿Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas? ¿Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento? ¿Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas?	
A7.2.3	Proceso disciplinario	Inicial		¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores? ¿Cómo se informa a los trabajadores sobre el proceso, incluidas las expectativas de la organización y sus derechos? ¿Está esto cubierto por contratos y acuerdos, capacitación inicial y conocimiento continuo? ¿Se actualiza el proceso de forma regular?	
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**				
A7.3.1	Responsabilidades ante la finalización o cambio	Inicial		¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización? ¿Se tienen en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos? ¿Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso?	

A8	Gestión de activos				
A8.1	**Responsabilidad sobre los activos**				
A8.1.1	Inventario de activos	Inexistente		¿Hay un inventario de activos de la información? ¿Contiene la siguiente información? • Datos digitales • Información impresa • Software • Infraestructura • Servicios de información y proveedores de servicios • Seguridad física • Relaciones comerciales • Las personas ¿A quién pertenece el inventario? ¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI? ¿Es suficientemente detallado y está estructurado adecuadamente?	
A8.1.2	Propiedad de los activos	Inexistente		¿Los activos tienen propietario de riesgo? ¿Los activos tienen responsable técnico? ¿Cómo se asigna la propiedad poco después de crear o adquirir los activos críticos? ¿Cómo se etiquetan los activos? ¿Cómo se informa ante incidentes de seguridad de la información que los afectan?	
A8.1.3	Uso aceptable de los activos	Inexistente		¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.? ¿Cubre el comportamiento del usuario en Internet y en las redes sociales? ¿Se permite el uso personal de los activos de la empresa? En caso afirmativo, ¿En qué medida y cómo se controla / asegura esto? ¿Se describe de forma explícita lo qué constituye un uso inapropiado? ¿Se distribuye esta información a toda la empresa? ¿El uso de la criptografía cumple con todas las leyes, acuerdos / contratos y normativas relevantes?	
A8.1.4	Devolución de activos	Inexistente		¿Existe un procedimiento para recuperar los activos tras una baja o despido? ¿Es un procedimiento automatizado o manual? Si es manual, ¿Cómo se garantiza que no haya desvíos? ¿Cómo se abordan los casos en los que los activos no han sido devueltos?	
A8.2	**Clasificación de la información**				
A8.2.1	Clasificación de la información	Inexistente		¿Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información? ¿La clasificación es impulsada por obligaciones legales o contractuales? ¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad? ¿Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen? ¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados?	
A8.2.2	Etiquetado de la información	Inexistente		¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica? ¿Está sincronizado con la política de clasificación de la información? ¿Cómo se garantiza el correcto etiquetado? ¿Cómo se garantiza que solo aquellos con permisos de acceso aprobados accedan a la información de la clasificación relevante? ¿Cómo se garantiza que no haya acceso no autorizado? ¿Se revisan los niveles de clasificación en intervalos predefinidos?	
A8.2.3	Manipulado de la información	Inexistente		Más allá de A.8.2.1 ¿Están los niveles de clasificación adecuadamente asignados a los activos? ¿Se considera los gimiente? Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios electrónicos y físicos, divulgación, intercambio, intercambio con terceros, etc.	
A8.3	**Manipulación de los soportes**				
A8.3.1	Gestión de soportes extraíbles	Inicial		¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles? ¿Los medios extraíbles están debidamente etiquetados y clasificados? ¿Los medios se mantienen y almacenan de forma adecuada? ¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?	
A8.3.2	Eliminación de soportes	Inexistente		Más allá de A.8.3.1 ¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios? ¿Se documenta la aprobación en cada etapa para la eliminación de los medios? ¿Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación? ¿Se tiene en cuenta los periodos de retención? ¿Los datos particularmente confidenciales se eliminan de forma segura (borrado criptográfico, desmagnetización o destrucción física)?	
A8.3.3	Soportes físicos en tránsito	Inexistente		¿Se utiliza un transporte o servicio de mensajería confiable? ¿Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia? ¿Se verifica la recepción por el destino?	

A9	Control de acceso				
A9.1	**Requisitos de negocio para el control de acceso**				
A9.1.1	Política de control de acceso	Inexistente		¿Existe una política de control de acceso? ¿Es consistente con la política de clasificación? ¿Hay una segregación de deberes apropiada? ¿Existe un proceso documentado de aprobación de acceso? ¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?	No se cuenta con una política de control de acceso solo existe un control de acceso al ingreso a la entidad El acceso a servidores y dispositivos de red administrables se encuentran controlados con contraseñas
A9.1.2	Acceso a las redes y a los servicios de red	Inexistente		¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado? ¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados? ¿Cómo monitoriza la red para detectar acceso no autorizado? ¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)? ¿La organización mide la identificación y los tiempos de respuesta ante incidentes?	El acceso VPN es autorizado, controlado y autorizado el inalambrico solo se autoriza para el acceso solo se utiliza ingreso contraseña Se cuenta con firewall de nueva generación borde y críticos. No se ha contratado el servicio de pentesting No se ha reportado incidentes
A9.2	**Gestión de acceso de usuario**				
A9.2.1	Registro y baja de usuario	Inicial		¿Se utiliza un ID de usuario únicos para cada usuario? ¿Se genera en función a una solicitud con aprobaciones y registros apropiados? ¿Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido? ¿Existen una comunicación eficiente ente la Administración de Seguridad y Recursos Humanos? ¿Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes? ¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios? ¿Qué impide que los ID de usuario sean reasignados a otros usuarios?	En el caso de redes y servidores como administración Se utiliza un id para cada usuario en el caso de redes no se genera solicitud para aprobaciones y registros aprobados Si se deshabilita No se cuenta con auditoria periodica En redes se elimina el ID Evitar un posible acceso no autorizado
A9.2.2	Provisión de acceso de usuario	Inexistente		¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio? ¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones? ¿Existe un registro documental de la solicitud y aprobación de acceso?	En redes si se hace con base a las necesidades del negocio No hay políticas de control de acceso No hay documentación
A9.2.3	Gestión de privilegios de acceso	Inicial		Más allá de A.9.2.2 ¿Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios? ¿Se genera un ID de usuario separado para otorgar privilegios elevados? ¿Se ha establecido una caducidad para los ID de usuario con privilegios? ¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?	No hay un proceso de revisiones Si se genera un ID de usuario separado No se ha establecido caducidad Si se controlan las actividades de los usuarios
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inexistente	? Desconocido	¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.? ¿Se verifica rutinariamente si hay contraseñas débiles? ¿Se requiere confirmar la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas? ¿Se transmite dicha información por medios seguros? ¿Se generan contraseñas temporales suficientemente fuertes? ¿Se cambian las contraseñas por defecto de los fabricantes? ¿Se recomienda a los usuarios usar el software adecuado de protección de contraseñas? ¿Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?	en redes algunos dispositivos exigen calidad de contraseñas no se verifica si hay contraseñas debiles la asignación se hace de manera presencial Las contraseñas de los fabricantes si se cambia No es una opción recomendable
A9.2.5	Revisión de los derechos de acceso de usuario	Inexistente		¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones? ¿Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios? ¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente?	No se ha establecido un procedimiento de revisión periódica de los dispositivos de red.
A9.2.6	Retirada o reasignación de los derechos de acceso	Inicial		¿Existe un proceso de ajuste de derechos de acceso? ¿Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo? ¿Incluye el acceso físico a las instalaciones y el acceso lógico a la red? En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan?	En redes existe un proceso no documentado de retiro o ajuste de derechos de acceso se retiran los accesos cuando el personal se retira de la entidad

A9.3	**Responsabilidades del usuario**				
A9.3.1	Uso de la información secreta de autenticación	Inexistente		¿Cómo se asegura la confidencialidad de las credenciales de autenticación? ¿Existe un proceso de cambio de contraseñas en caso de ser comprometida? ¿Existen controles de seguridad relativas a las cuentas compartidas?	No se cuenta con la gestión de contaseñas
A9.4	**Control de acceso a sistemas y aplicaciones**				
A9.4.1	Restricción del acceso a la información	Inicial		Más allá de A.9.2.2 ¿Existen controles de acceso adecuados? ¿Se identifican los usuarios de forma individual individuales? ¿Cómo se definen, autorizan, asignan, revisan, gestionan y retiran los derechos de acceso, los permisos y las reglas asociadas?	Los controles de acceso no se gestionan de manera adecuada los usuarios si se identifican de manera individual La asignación se hace mediante procesos no formalizados
A9.4.2	Procedimientos seguros de inicio de sesión	Definido		¿Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado? ¿Cómo se autentican las identidades de usuario durante el proceso de inicio de sesión? ¿Se utiliza autenticación multifactor para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.? ¿La información de inicio de sesión solo se valida una vez imputadas las credenciales? ¿Las contraseñas no válidas desencadenan demoras o bloqueos, entradas de registro y alertas / alarmas? ¿Se registran los inicios de sesión exitosos? ¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?	En redes si
A9.4.3	Sistema de gestión de contraseñas	Repetible		¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos? ¿Las reglas tienen en cuenta lo siguiente? • Longitud mínima de la contraseña • Evitan la reutilización de un número específico de contraseñas • Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.) • Requiere el cambio forzado de contraseñas en el primer inicio de sesión • Esconde la contraseña durante la imputación ¿Se almacenan y transmiten de forma segura (cifrado)?	En redes si
A9.4.4	Uso de utilidades con privilegios del sistema	Inicial		¿Quién controla los servicios privilegiados? ¿Quién puede acceder a ellos, bajo qué condiciones y con qué fines? ¿Se verifica que estas personas necesidad comercial para otorgar el acceso según su roles y responsabilidades? ¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado? ¿Se tiene en cuenta la segregación de tareas?	Personal Tics , bajo las condiciones de autorización si se tiene en cuenta la segregación de tareas, no existe un proceso auditable de aprobación.
A9.4.5	Control de acceso al código fuente de los programas	? Desconocido		¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios? ¿El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.? ¿Cómo se modifica el código fuente? ¿Cómo se publica y se compila el código? ¿Se almacenan y revisan los registros de acceso y cambios?	

A10	**Criptografía**				
A10.1	**Controles criptográficos**				
A10.1.1	Política de uso de los controles criptográficos	Inexistente		¿Existe una política que cubra el uso de controles criptográficos? ¿Cubre lo siguiente? • Los casos en los que información debe ser protegida a través de la criptografía • Normas que deben aplicarse para la aplicación efectiva • Un proceso basado en el riesgo para determinar y especificar la protección requerida • Uso de cifrado para información almacenada o transferida • Los efectos de cifrado en la inspección de contenidos de software • Cumplimiento de las leyes y normativas aplicables ¿Se cumple con la política y requerimientos de cifrado?	No existe una política de controles criptográficos
A10.1.2	Gestión de claves	Inexistente		¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)? ¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas? ¿Se generan claves diferentes para sistemas y aplicaciones? ¿Se evitan claves débiles? ¿Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)? ¿Se hacen copias de respaldo de las claves? ¿Se registran las actividades clave de gestión? ¿Cómo se cumplen todos estos requisitos?	No existe una política de controles criptográficos
A11	**Seguridad física y del entorno**				
A11.1	**Áreas seguras**				
A11.1.1	Perímetro de seguridad física	? Desconocido		¿Las instalaciones se encuentran en una zona de riesgo? ¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)? ¿El techo exterior, las paredes y el suelo son de construcción sólida? ¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado? ¿Las puertas y ventanas son fuertes y con cerradura? ¿Se monitorea los puntos de acceso con cámaras? ¿Existe un sistema de detección de intrusos y se prueba periódicamente?	
A11.1.2	Controles físicos de entrada	? Desconocido		¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)? ¿Hay procedimientos que cubran las siguientes áreas? • Cambio regular código de acceso • Inspecciones de las guardias de seguridad • Visitantes siempre acompañados y registrados en el libro de visitantes • Registro de movimiento de material • Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas) ¿Se utiliza autenticación multi-factor de autenticación (ej. Biométrico más el código PIN)? ¿Se requiere para las áreas críticas? ¿Existe un registro de todas las entradas y salidas?	
A11.1.3	Seguridad de oficinas, despachos y recursos	? Desconocido		¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)? ¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos? ¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?	
A11.1.4	Protección contra las amenazas externas y ambientales	? Desconocido		¿Qué tipo de protecciones existen contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.? ¿Existe un procedimiento de recuperación de desastres? ¿Se contemplan sitios remotos?	
A11.1.5	El trabajo en áreas seguras	? Desconocido		¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo? ¿Se hace un análisis para evaluar que los controles adecuados están implementados? Controles de acceso físico Alarmas de intrusión Monitoreo de CCTV (verificar la retención y frecuencia de revisión) Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación Políticas, procedimientos y pautas ¿Cómo se asegura que la información de carácter sensible permanece confidencial a personal autorizado?	
A11.1.6	Áreas de carga y descarga	? Desconocido		¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado? ¿Se verifica que el material recibido coincide con un número de pedido autorizado? ¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?	

A11.2	Seguridad de los equipos				
A11.2.1	Emplazamiento y protección de equipos	? Desconocido		¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas? ¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada? ¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales? • Agua / inundación • Fuego y humo • Temperatura, humedad y suministro eléctrico • Polvo • Rayos, electricidad estática y seguridad del personal ¿Se prueban estos controles periódicamente y después de cambios importantes?	
A11.2.2	Instalaciones de suministro	? Desconocido		¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad? ¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente? ¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante? ¿Son probados con regularidad? ¿Hay una red de suministro eléctrico redundante? ¿Se realizan pruebas de cambio? ¿Se ven afectados los sistemas y servicios? ¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos? ¿Están ubicados apropiadamente? ¿Hay una capacidad adecuada de A / C para soportar la carga de calor? ¿Hay unidades redundantes, de repuesto o portátiles disponibles? ¿Hay detectores de temperatura con alarmas de temperatura?	
A11.2.3	Seguridad del cableado	? Desconocido		¿Hay protección física adecuada para cables externos, cajas de conexiones? ¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias? ¿Se controla el acceso a los paneles de conexión y las salas de cableado? ¿Existen procedimientos adecuados para todo ello?	
A11.2.4	Mantenimiento de los equipos	? Desconocido		¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)? ¿Hay programas de mantenimiento y registros / informes actualizados? ¿Se aseguran los equipos?	
A11.2.5	Retirada de materiales propiedad de la empresa	? Desconocido		¿Existen procedimiento relativos al traslado de activos de información? ¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados? ¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo? ¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?	
A11.2.6	Seguridad de los equipos fuera de las instalaciones	? Desconocido		¿Existe una "política de uso aceptable" que cubra los requisitos de seguridad y "obligaciones" con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas? ¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras? ¿Existen controles para asegura todo esto? ¿Cómo se les informa a los trabajadores sobre sus obligaciones? ¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?	
A11.2.7	Reutilización o eliminación segura de equipos	? Desconocido		¿Cómo evita la organización que se revele la información almacenada en equipos tras su reasignación o eliminación? ¿Se utiliza cifrado fuerte o borrado seguro? ¿Se mantienen registros adecuados de todos los medios que se eliminan? ¿La política y el proceso cubren todos los dispositivos y medios de TIC?	
A11.2.8	Equipo de usuario desatendido	? Desconocido		¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción? ¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado? ¿Se protegen los bloqueos de pantalla con contraseña? ¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC? ¿Cómo se verifica el cumplimiento?	
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	? Desconocido		¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas? ¿Funciona en la práctica? ¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos? ¿Se activa automáticamente tras de un tiempo inactivo definido? ¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?	

A12	Seguridad de las operaciones				
A12.1	**Procedimientos y responsabilidades operacionales**				
A12.1.1	Documentación de procedimientos operacionales	? Desconocido		¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.? ¿Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez? ¿Los procesos son razonablemente seguros y están bien controlados? ¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal? ¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)? ¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?	
A12.1.2	Gestión de cambios	? Desconocido		¿Existe una política de gestión de cambios? ¿Existen registros relacionados a la gestión de cambios? ¿Se planifican y gestionan los cambios? ¿Se evalúan los riesgos potenciales asociados con los cambios? ¿Los cambios están debidamente documentados, justificados y autorizados por la administración?	
A12.1.3	Gestión de capacidades	Repetible		¿Existe una política de gestión de capacidad? ¿Existen registros relacionados a la gestión de capacidad? ¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante? ¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?	No existe politica de gestión de capacidad no existen registros en aire acondicionado, si se gestiona, en capacidad técnica y almacenamiento en servidores si se gestiona a nivel de red esta no se puede potenciar. La prioridad se habasado en la disponibilidad de servicios críticos, servidores, red.
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	? Desconocido		¿Se segregan entornos de TIC de desarrollo, prueba y operacionales? ¿Cómo se logra la separación a un nivel de seguridad adecuado? ¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)? ¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos? ¿Cómo se promueve y se lanza el software? ¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección? ¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros? ¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?	Se identificaron usuarios con axeso multiple a Dev, pruebas y Prod
A12.2	**Protección contra el software malicioso (malware)**				
A12.2.1	Controles contra el código malicioso	? Desconocido		¿Existen políticas y procedimientos asociados a controles antimalware? ¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado? ¿Cómo se compila, gestiona y mantiene la lista y por quién? ¿Hay controles de antivirus de "escaneado en acceso" y "escaneo programático" en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT? ¿Se actualiza el software antivirus de forma automática? ¿Se general alertas accionables tras una detección? ¿Se toma acción de forma rápida y apropiada para minimizar sus efectos? ¿Cómo se gestionan las vulnerabilidades técnicas? ¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte? ¿Existe un mecanismo de escalación para incidentes graves?	Se maneja a criterio profesional
A12.3	**Copias de seguridad**				
A12.3.1	Copias de seguridad de la información	Definido		¿Existen políticas y procedimientos asociados a las copias de seguridad? ¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio? ¿Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.? ¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales? ¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido? ¿Se mantienen copias off-line para evitar una propagación de ransomware catastrófica? ¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar? ¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?	En redes se hace copia de los dispositivos Las copias de seguridad se hacen hacia otro servidor ubicado en el mismo lugar del servidor priincipal la copia de servidores se hace de la información de aplicaciones y de las configuraciones. No se hace restauracion de copias
A12.4	**Registros y supervisión**				
A12.4.1	Registro de eventos	Administrado		¿Existen políticas y procedimientos para el registro de eventos? ¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí? ¿Se registra lo siguiente? • cambios en los ID de usuario • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web ¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados? ¿Cuál es el periodo de retención de eventos? ¿Existe un proceso para revisar y responder adecuadamente a las alertas de seguridad?	se cuenta con Sislog, firewall de nueva generación y antivirus El personal Tics es el encargado de seguimiento El periodo de retención es trimestral No se cuenta con un proceso para revisar y responder adecuadamente a las alertas de seguridad
A12.4.2	Protección de la información del registro	Inexistente		¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable? ¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado? ¿Quién tiene o podría obtener acceso a leer / escribir / eliminar registros de eventos? ¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención? ¿Existen copias de seguridad de los registros?	No existe gestión de la información de registro
A12.4.3	Registros de administración y operación	Inicial		Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)? ¿Cómo se recogen, almacenan y aseguran, analizan los registros? ¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?	Los responsables de la información de registro es Tics se recogen en el sislog, antivirus y firewall de nueva generación y se alamacenan durante 3 meses, no se cuenta con historico
A12.4.4	Sincronización del reloj	Inexistente		¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión? ¿Hay un tiempo de referencia definido (ej. Reloj atómicos, GPS o NTP)? ¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales? ¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.? ¿Existe una configuración de respaldo para la referencia de tiempo?	No se cuenta con servidor de hora

A12.5	**Control del software en explotación**				
A12.5.1	Instalación del software en explotación	? Desconocido		¿Existe una política acerca de la instalación de software? ¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción? ¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)? ¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.? ¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados? ¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas? ¿Existe un control de cambio y aprobación adecuado para la aprobación de software?	
A12.6	**Gestión de la vulnerabilidad técnica**				
A12.6.1	Gestión de las vulnerabilidades técnicas	Inexistente		¿Existe una política la gestión de vulnerabilidades técnicas? ¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada? ¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes? ¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes? ¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC? ¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo? ¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución? ¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? ¿Los procesos para implementar parches urgentes son adecuados? ¿Se emplea una administración automatizada de parches? ¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?	No hay gestión de vulnerabilidades tecnicas
A12.6.2	Restricción en la instalación de software	? Desconocido		¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados? ¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos? ¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?	Si hay política pero se puede instalal Software de diferentes formas
A12.7	**Consideraciones sobre la auditoria de sistemas de información**				
A12.7.1	Controles de auditoría de sistemas de información	? Desconocido		¿Existe una política que requiera auditorias de seguridad de la información? ¿Existe un programa definido y procedimientos para auditoría? ¿Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales? ¿Se define el alcance de la auditoría en coordinación con la administración? ¿El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado?	

A13	**Seguridad de las comunicaciones**				
A13.1	**Gestión de la seguridad de las redes**				
A13.1.1	Controles de red	Administrado		¿Existen políticas de redes físicas e inalámbricas? ¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red? ¿Existe un mecanismo de registro i monitorización de la red y los dispositivos que se conectan ella? ¿Hay un sistema de autenticación para todos los accesos a la red de la organización? ¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos? ¿Los usuarios se autentican adecuadamente al inicio de sesión? ¿Cómo se autentican los dispositivos de red? ¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.? ¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?	No existen politicas Si hay separación de la administración de las operaciones de los sistmas y de la infraestructura de red No existe sistema de autienticación no se limita el acceso a personas existe segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc. Se gestiona los puertos
A13.1.2	Seguridad de los servicios de red	Definido		¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada? ¿Existe un monitoreo de servicios de red? ¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)? ¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red? ¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?	si Se gestionan, clasifican y protegen los servicios de red de forma adecuada No existe un monitoreo de servicios de red el acceso a la red es con autenticación el cifrado es deacuerdo al sistema de información
A13.1.3	Segregación en redes	Administrado		¿Existe una política de segmentación de red? ¿Qué tipo de segmentación existe? ¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)? ¿Cómo se monitorea y controla la segregación? ¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados? ¿Hay controles adecuados entre ellos? ¿Cómo se controla la segmentación con proveedores y clientes? ¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?	No se cuenta con politica de segmentación de res La segmentación es pon Vlan esta basada en la clasificación de las funcciones se monitorea a travez del sislog, router firewall
A13.2	**Intercambio de información**				
A13.2.1	Políticas y procedimientos de intercambio de información	? Desconocido		¿Existen políticas y procedimientos relacionados con la transmisión segura de información? ¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.? ¿Está basado en la clasificación de la información? ¿Existen controles de acceso adecuados para esos mecanismos? ¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)? ¿Se sigue el principio de confidencialidad y privacidad? ¿Existen un programa de concientización, capacitación y cumplimiento?	
A13.2.2	Acuerdos de intercambio de información	? Desconocido		Más allá de A.13.2.1 ¿Qué tipos de comunicaciones se implementan las firmas digitales? ¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos? ¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas? ¿Cómo se mantiene una cadena de custodia para las transferencias de datos?	
A13.2.3	Mensajería electrónica	? Desconocido		¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.? ¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)? ¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?	
A13.2.4	Acuerdos de confidencialidad o no revelación	? Desconocido		¿Existen acuerdos de confidencialidad? ¿Han sido revisados y aprobados por el Departamento Legal? ¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)? ¿Han sido aprobados y firmados por las personas adecuadas? ¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?	

A14	Adquisición, desarrollo y mantenimiento de los sistemas de información				
A14.1	**Requisitos de seguridad en los sistemas de información**				
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	? Desconocido		¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software? ¿Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo? ¿Son estos procedimientos obligatorios para todos los nuevos desarrollos y cambios en los sistemas existentes (ej. Actualizaciones de sistema operativo / aplicaciones en las actualizaciones, cambios de criptografía, etc.) ¿Se aplican estos controles para sistemas / software comercial, incluidos los productos "a medida" o personalizados?	
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	? Desconocido		¿La organización usa o proporciona aplicaciones web de comercio electrónico? ¿Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio? ¿Contiene controles tales como validación de datos de entrada, validación de procesamiento, encriptación, autenticación de mensajes e irrenunciabilidad? ¿Se fuerza https? ¿Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)? ¿Se analizan y documentan las amenazas de forma rutinaria? ¿Existe una gestión de incidentes y cambios para tratarlos?	
A14.1.3	Protección de las transacciones de servicios de aplicaciones	? Desconocido		Más allá de A.14.1.2 ¿Las transacciones se realizan y almacenan en un entorno interno seguro o expuesto a internet? ¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.? ¿Cumplen con todos los requisitos legales, regulatorios y de cumplimiento?	
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**				
A14.2.1	Política de desarrollo seguro	? Desconocido		¿Existe una política de desarrollo seguro que abarque la arquitectura de seguridad? ¿Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios? ¿Los métodos de desarrollo incluyen pautas de programación segura? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?	
A14.2.2	Procedimiento de control de cambios en sistemas	? Desconocido		¿Existen políticas, procedimientos y registros relacionados de la gestión de cambios? ¿Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión? ¿Incluye un procedimiento para cambios de emergencia? ¿Se aplica los cambios significativos en equipos informáticos y de telecomunicaciones? ¿Los cambios en el sistema están debidamente documentados, justificados y autorizados por la administración?	
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	? Desconocido		¿Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado? ¿Hay registros de estas actividades?	
A14.2.4	Restricciones a los cambios en los paquetes de software	? Desconocido		¿Se hacen cambios a paquetes software adquiridos? ¿Se verifica que los controles originales no han sido comprometidos? ¿Se obtuvo el consentimiento y la participación del proveedor? ¿El proveedor continúa dando soporte tras los cambios? ¿Se exploró la posibilidad de obtener actualizaciones de programas estándar por parte de los proveedores? ¿Se hace una comprobación de compatibilidad con otro software en uso?	
A14.2.5	Principios de ingeniería de sistemas seguros	? Desconocido		¿Se siguen principios de SDLC que incluye controles de seguridad? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?	
A14.2.6	Entorno de desarrollo seguro	? Desconocido		¿Se aíslan los entornos de desarrollo? ¿Cómo se desarrolla, prueba y lanza el software? ¿Quién es responsable de garantizar que el software nuevo / modificado no interrumpa otras operaciones? ¿Se realizan comprobaciones de antecedentes de los desarrolladores? ¿Tienen que cumplir con un NDA? ¿Cuáles son los reglamentos y los requisitos de cumplimiento que afectan el desarrollo? ¿Cómo se protegen los datos de prueba de la divulgación y dónde están almacenados?	
A14.2.7	Externalización del desarrollo de software	? Desconocido		Más allá de A.14.2.6 ¿Se tienen en cuanta los siguientes aspectos cuando el desarrollo es lleva a cabo por un tercero? • Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual • Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba • Acceso al código fuente si el código ejecutable necesita ser modificado • Controles de prueba de seguridad de aplicaciones • Evaluación de vulnerabilidad y tratamiento	
A14.2.8	Pruebas funcionales de seguridad de sistemas	? Desconocido		Más allá de A.14.2.7 ¿Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados? ¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual?	
A14.2.9	Pruebas de aceptación de sistemas	? Desconocido		¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red? ¿Las pruebas replican situaciones y entornos operativos realistas? ¿Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado? ¿Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo? ¿Se actualizan los controles de resiliencia y recuperación tras incidentes para reflejar los sistemas nuevos, modificados y retirados?	
A14.3	**Datos de prueba**				
A14.3.1	Protección de los datos de prueba	? Desconocido		¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.? ¿Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas? ¿Existen registros de estas actividades?	Hay procedimiento que no se lleva a cabo

A15	Relación con proveedores				
A15.1	**Seguridad en las relaciones con proveedores**				
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	? Desconocido		¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI? ¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo? ¿Los contratos y acuerdos abordan lo siguiente? • Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada • Información / propiedad intelectual, y obligaciones / limitaciones derivadas • Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001 • Identificación de controles físicos y lógicos • Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio • Habilitación de seguridad de los empleados y concienciación • Derecho de auditoría de seguridad por parte de la organización ¿Existe una obligación contractual de cumplimento? ¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?	
A15.1.2	Requisitos de seguridad en contratos con terceros	? Desconocido		¿Los contratos o acuerdos formales con proveedores cubren lo siguiente? • Gestión de las relaciones, incluyendo riesgos • Cláusulas de confidencialidad vinculantes • Descripción de la información que se maneja y el método de acceder a dicha información • Estructura de la clasificación de la información a usar • La Inmediata notificación de incidentes de seguridad • Aspectos de continuidad del negocio • Subcontratación y restricciones en las relaciones con otros proveedores • Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, "robo de empleados", etc.)	
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	? Desconocido		Más allá de A.15.1.1 y A.15.1.2 ¿Cómo se validan los requisitos de seguridad de los productos o servicios adquiridos? ¿Cómo se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros? ¿Se puede rastrear el origen del producto o servicio?	
A15.2	**Gestión de la provisión de servicios del proveedor**				
A15.2.1	Control y revisión de la provisión de servicios del proveedor	? Desconocido		¿Existe una monitorización de servicios y quien responsable de esta actividad? ¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia? ¿Se generan informes y / o métricas relacionadas a las reuniones y las decisiones tomadas? ¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría? ¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?	
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	? Desconocido		¿Cómo se comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados? ¿Cómo se comunican cambios en las políticas y requerimientos legales de la organización? ¿Se actualizan los acuerdos relacionados con los cambios?	

A16	Gestión de incidentes de seguridad de la información				
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**				
A16.1.1	Responsabilidades y procedimientos	? Desconocido		¿Existen políticas, procedimientos e ITT´s para la gestión de incidentes? ¿Qué cubre? • I plan de respuesta a incidentes • Puntos de contacto para la notificación de incidentes, seguimiento y evaluación • Monitoreo, detección y reporte de eventos de seguridad • Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio • Método de recolección de evidencias y pruebas forenses digitales • Revisión post-evento de seguridad y procesos de aprendizaje / mejora ¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre?	
A16.1.2	Notificación de los eventos de seguridad de la información	? Desconocido		¿Cómo se informan los eventos de seguridad de la información? ¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen? ¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución. ¿Qué pasa con esos informes?	
A16.1.3	Notificación de puntos débiles de la seguridad	? Desconocido		Más allá de A.16.1.2 ¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual? ¿Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo?	
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	? Desconocido		¿Qué tipos de eventos se espera que informen los empleados? ¿A quién informan? ¿Cómo se evalúan estos eventos para decidir si califican como incidentes? ¿Hay una escala de clasificación? ¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes graves? ¿En qué se basa?	
A16.1.5	Respuesta a incidentes de seguridad de la información	? Desconocido		¿Cómo se recolecta, almacena y evalúa la evidencia? ¿Hay una matriz de escalación para usar según sea necesario? ¿Hay medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes? ¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?	
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	? Desconocido		¿Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes? ¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias? Además, ¿Se está utilizado para formación y concienciación? ¿La organización cuenta con un proceso de gestión de incidentes relativamente maduro? ¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?	
A16.1.7	Recopilación de evidencias	? Desconocido		¿La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área? ¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el rol? (cadena de evidencia rigurosamente mantenida, evidencia asegurada en almacenamiento, herramientas y técnicas) ¿Quién decide emprender un análisis forense, y en qué criterio se base? ¿Existen obligaciones relacionadas con la jurisdicción, las diferentes normas forenses y los requisitos legales asociados?	

A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**				
A17.1	**Continuidad de la seguridad de la información**				
A17.1.1	Planificación de la continuidad de la seguridad de la información	? Desconocido		¿Cómo se determinan los requisitos de continuidad del negocio? ¿Existe un plan de continuidad de negocio? ¿Existen un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos? ¿Se identifica el impacto potencial de los incidentes? ¿Se evalúan los planes de continuidad del negocio? ¿Se llevan a cabo ensayos de continuidad?	
A17.1.2	Implementar la continuidad de la seguridad de la información	? Desconocido		¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción? ¿Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares? ¿La planificación de la continuidad es consistente e identifica las prioridades de restauración? ¿Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades? ¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos?	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	? Desconocido		¿Existe un método de pruebas del plan de continuidad? ¿Con qué frecuencia se llevan a cabo dichas pruebas? ¿Hay evidencia de las pruebas reales y sus resultados? ¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios?	
A17.2	**Redundancias**				
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	? Desconocido		¿Cómo se identifican los requisitos de disponibilidad de servicios? ¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga? ¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí? ¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?	
A18	**Cumplimiento**				
A18.1	**Cumplimiento de los requisitos legales y contractuales**				
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	? Desconocido		¿Existe una política acerca del cumplimiento de requisitos legales? LOPD, GDPR, etc. ¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables? ¿Hay una persona encargada de mantener, usar y controlar el registro? ¿Cómo se logra y se garantiza el cumplimiento? ¿Existen controles adecuados para cumplir con los requisitos?	
A18.1.2	Derechos de Propiedad Intelectual (DPI)	? Desconocido		¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?	
A18.1.3	Protección de los registros de la organización	? Desconocido		¿Existe una política que contemple lo siguiente? Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos. ¿Se almacenan las firmas digitales de forma segura? ¿Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado? ¿Se verifica periódicamente la integridad de los registros? ¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo?	
A18.1.4	Protección y privacidad de la información de carácter personal	? Desconocido		¿Hay un mecanismo para instruir al personal en el manejo de información de carácter personal? ¿Hay un responsable de privacidad en la organización? ¿Es el responsable conocedor de la información de carácter personal que es recopilado, procesado y almacenados por la organización? ¿Cuáles son los controles de acceso a información de carácter personal? ¿Cuál es el nivel de acceso y roles (de personal) que tienen acceso a estos activos?	
A18.1.5	Regulación de los controles criptográficos	? Desconocido		¿Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico? ¿Estas actividades cumplen con los requisitos legales y reglamentarios?	
A18.2	**Revisiones de la seguridad de la información**				
A18.2.1	Revisión independiente de la seguridad de la información	? Desconocido		¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información? ¿Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos? ¿Están los objetivos y el alcance de auditoria autorizados por la gerencia? ¿Está adecuadamente controlado el acceso a las herramientas / software de auditoría del sistema de información? ¿Se documentan los hallazgos de auditoría y las actuaciones para solventarlos?	
A18.2.2	Cumplimiento de las políticas y normas de seguridad	? Desconocido		¿Cómo garantizar que todos los procedimientos de seguridad dentro de un área de responsabilidad se llevan a cabo correctamente? ¿Se hace una verificación periódica?	
A18.2.3	Comprobación del cumplimiento técnico	? Desconocido		¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares? ¿Las pruebas son realizadas por profesionales debidamente cualificados, competentes y confiables? ¿Cómo informa, analiza y utilizan los resultados de dichas pruebas? ¿La prioridad de tratamiento se basa en un análisis de riesgos? ¿Hay evidencias de medidas tomadas para abordar los problemas identificados?	Hay escaneo de vulnerabilidades por parte del area de seguridad pero no se llevan a cabo los planes de remediación

Apéndice C

Informe de Auditoría inicial

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad
? Desconocido	No ha sido verificado	0%	58%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	89%	25%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	7%	9%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	0%	2%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	4%	4%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	0%	4%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0%	0%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%	0%
	Total	100%	100%