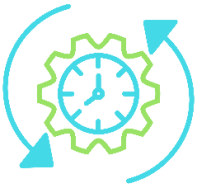
PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EJES TEMÁTICOS DE LA ACREDITACIÓN

TRANSFORMACIÓN CULTURAL PERMANENTE 	***MEJORAMIENTO CONTINUO*** 	***GESTIÓN CLÍNICA EXCELENTE Y SEGURA*** 
ATENCIÓN CENTRADA EN EL USUARIO 	***GESTIÓN DEL RIESGO*** 	***RESPONSABILIDAD SOCIAL*** 
HUMANIZACIÓN DE LA ATENCIÓN EN SALUD 	***GESTIÓN DE LA TECNOLOGIA*** 	

SANTIAGO DE CALI, ENERO 2026

CONTENIDO

1. POLÍTICA INSTITUCIONAL

La Gerencia del Hospital Departamental Mario Correa Rengifo Ese, está comprometida con la preservación de la confidencialidad, disponibilidad e integridad de la información de la institución y con el apoyo de la Unidad Funcional de Sistemas de Información, supervisara la protección de los bienes de la información contra uso, modificación, acceso o destrucción no autorizada

El comité de seguridad de la información definirá la estrategia para la implementación y administración el SGSI dentro del Hospital Departamental Mario Correa Rengifo ESE, definirá acuerdos de confidencialidad en la contratación interna (colaboradores) y externa (servicios), delegará roles y responsabilidades a sus colaboradores frente a la seguridad de la información.

El comité de seguridad de la información desarrollara mecanismos que permitan la adecuada identificación y clasificación de los activos de la información conociendo su propietario, ubicación y criticidad dentro de la institución, para gestionar su adecuada protección.

1.1. DECLARATORIA DE LA POLÍTICA GENERAL DEL MANEJO DE LA INFORMACIÓN

Aprobada mediante resolución interna número 487 de octubre 10 de 2022, declara que: La información interna y externa manejada en el Hospital Departamental Mario Correa Rengifo ESE, es identificada de acuerdo con las necesidades de los diferentes procesos, siendo tratada con el debido control y seguimiento, garantizando que al interior de la institución fluya de manera oportuna, segura, accesible y confidencial, constituyéndose en un instrumento válido para la toma de decisiones gerenciales.

ALCANCE

La política debe ser cumplida por los miembros de la institución: funcionarios, Contratistas, Proveedores, clientes y/o visitantes, que utilicen información generada a través de un aplicativo, transmitida por redes, en medio magnético o medio impreso

ACUERDO DE CONFIDENCIALIDAD

Las partes se obligan mutuamente a guardar la confidencialidad y reserva de los secretos que conozcan con motivo de las conversaciones precontractuales y las

subsiguientes que llevaron a la celebración de este contrato y a no divulgar, ceder, prestar, revelar, vender, usar, disertar, publicar o autorizar revelar a persona alguna ninguna información confidencial ni información alguna de propiedad de la otra parte, bajo ninguna modalidad, incluyendo la información que a partir de la fecha reciban. Devolver toda la información suministrada por la otra parte tan pronto como termine la labor encomendada o en el momento en que sea solicitada. Mantener en estricta reserva toda información que en razón de este contrato reciba de manera directa o indirecta, en forma verbal, escrita, gráfica, en medio magnético o bajo cualquier otra forma o modalidad, tomando todas las medidas necesarias para que la información no llegue por ningún motivo a manos de terceros bajo ninguna circunstancia y utilizarla únicamente para adelantar las tareas que se deriven directamente del cumplimiento del presente contrato.

1.2. POLÍTICA GOBIERNO DIGITAL

Aprobada mediante resolución interna número 488 de octubre 10 de 2022 establece en el Hospital: Gobierno digital contribuye a la transformación del Digital del Sector público, el cual implica un cambio en los procesos, la cultura y uso de la tecnología, tiene como finalidad en la ESE Facilitar el acceso a la información y ejecución de los trámites y procedimientos administrativos por medios electrónicos, creando las condiciones de confianza en el uso de los mismos, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, cumpliendo con los atributos de seguridad jurídica propios de la comunicación electrónica, la política de gobierno digital

La Política de Gobierno Digital se integrará a la cultura organizacional del Hospital a través de un plan de implementación dirigido por la alta dirección, en el cual se deleguen responsabilidades en toda la Institución, de tal forma que todos los servidores públicos y contratistas, Faciliten el acceso a la información y ejecución de los trámites y procedimientos administrativos por medios electrónicos y garanticen la seguridad transparencia y preservación de la información de la institución

La Gerencia del Hospital Departamental Mario Correa Rengifo Ese, está comprometida con la promoción, uso y aprovechamiento de las tecnologías de información y comunicaciones generando entorno digital de confianza, que permita el Hospital Departamental Mario Correa Rengifo Ese, transformarse en una empresa del sector salud, competitiva, proactiva e innovadora en la prestación de los servicios integrales de Salud a los ciudadanos.

Que tiene como objetivo “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”.

2. OBJETIVO

Implementar el SGSI Sistema de gestión de Seguridad de la Información en Hospital Departamental Mario Correa Rengifo ESE, para lograr la preservación de la confidencialidad, disponibilidad e integridad de la información, estableciendo un esquema de seguridad bajo la gestión del riesgo.

OBJETIVOS ESPECÍFICOS

- Actualizar los activos de información de la entidad y evaluar su criticidad en relación de integridad, confidencialidad y disponibilidad de la información en el 2026.
- Identificar y gestionar en el 2026 los riesgos de activos de información en los procesos del Hospital, que puedan afectar la integridad, confidencialidad y disponibilidad de la información.
- Atender de manera adecuada con el oficial de seguridad del Hospital los incidentes de seguridad de la información que afecte la integridad, confidencialidad y disponibilidad de esta durante el año.
- Cumplir la normatividad legal vigente de transparencia y derecho de acceso a la información pública nacional, la estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - Min TIC, la norma ISO 27001:2013, la Ley estatutaria de protección de datos personales (Ley 1581 de 2012) y sus decretos reglamentarios y las normas que las modifiquen, adicionen o sustituyan.
- Realizar campaña de cultura en seguridad y privacidad de la información en el año 2026, socialización de la política de seguridad y acuerdo de confidencialidad para los funcionarios, contratistas, terceros, aprendices, practicantes y proveedores.
- Ejecutar el mapa de ruta en el periodo indicado con el acompañamiento de la alta gerencia y la asignación de recursos para la implementación y mitigación de riesgos de seguridad de la información en la ESE.

3. ALCANCE

La implementación del SGSI Sistema de Gestión de Seguridad de la Información será en todos los procesos del Hospital Departamental Mario Correa Rengifo ESE y donde exista recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de

información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos, tiene como finalidad resguardar la información almacenada en los componentes informáticos de la institución y aplica específicamente a los datos sensibles y de riesgo, a los datos personales relacionados con la atención y los usuarios que utilizan los servicios del hospital.

4. NORMATIVA

Ley 44 de 1993 "por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor).

Ley 527 de 1999 "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".

Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

Decisión Andina 351 de 2015 "Régimen común sobre derecho de autor y derechos conexos".

CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.

Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL año 2018.

Norma Técnica Colombiana ISO27001:2013 tecnologías de la información, Técnicas de seguridad, sistemas de gestión de la seguridad de la información, requisitos.

Norma Técnica Colombiana ISO27002:2013 tecnologías de la información, técnicas de seguridad, código de practica para controles de seguridad de la información.

Norma Técnica Colombiana ISO27035:2013 tecnologías de la información, Gestión de Incidentes de Seguridad de la Información**.**

Norma Técnica Colombiana ISO31000:2013. ISO31010:2013

5. DEFINICIONES

TERMINO	DEFINICIÓN
Confidencialidad	Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
AoAs	Áreas de análisis que son la infraestructura, las aplicaciones, operaciones, y la gente.
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.
Estándar	Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001
Gestión del riesgo	Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
Incidente de seguridad de la información	Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.
Información	Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla
Integridad	Propiedad de exactitud y completitud.
Aplicaciones	Software informático que proporciona funcionalidad al usuario final. Requiere la existencia de un sistema operativo en el que ejecutarse. Algunos ejemplos son los procesadores de texto, las hojas de cálculo o los programas de gestión de bases de datos.
Inventario de activos	Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos

TERMINO	DEFINICIÓN
Política de seguridad de información	Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información
Antivirus (AV)	Software o tecnología de hardware que protege al entorno informático frente a cualquier software peligroso.
Perfil de riesgos para la empresa (BRP)	Medida del riesgo al que está expuesto una empresa, según el entorno empresarial y el sector en que compite.
Riesgo	Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales Se expresa en términos de probabilidad y consecuencias.
Riesgo de seguridad y privacidad	Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias
Índice de defensa en profundidad (DiDI)	Medida de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en una empresa.
Zona desmilitarizada (DMZ)	Parte de la red separada de la red interna mediante un cortafuego y conectada a Internet a través de otro cortafuego.
Servidor de seguridad (cortafuegos)	Dispositivo de hardware o software que ofrece protección a los equipos frente al acceso no autorizado a través de la red.
Infraestructura	Funcionalidad de red, así como su administración y mantenimiento para ofrecer compatibilidad con la defensa de red, respuesta frente a incidentes, disponibilidad de red y análisis de errores. Incluye compatibilidad con los procesos empresariales internos y externos, y acerca de cómo se crean e implementan los hosts.
Autenticación multifactor	Autenticación que requiere una combinación de al menos dos de los siguientes elementos: algo que se sabe; algo que se tiene; o algo propio del usuario. Por ejemplo, la tarjeta de débito de su banco es una autenticación de dos factores: requiere algo que tiene (la tarjeta) y algo que sabe (el número PIN). Solicitar a alguien que teclee múltiples contraseñas para la autenticación, supone una autenticación de un solo factor al tratarse únicamente de algo que sabe el usuario. Por lo general, cuantos más factores, más segura es la autenticación. Así, un sistema que requiera una tarjeta identificativa (algo que posee), un PIN (algo que sabe) y una huella

TERMINO	DEFINICIÓN
	dactilar escaneada (algo propio) es más seguro que cualquier otro que únicamente solicite el nombre de usuario/contraseña (factor único) o una tarjeta de identidad y el PIN.
Operaciones	Los miembros de una empresa, así como las directivas, los procesos, los procedimientos y las prácticas que se relacionan con su protección y la de la empresa.
Personal	Los miembros de una empresa, así como las directivas, los procesos, los procedimientos y las prácticas que se relacionan con su protección y la de la empresa.
Infraestructura de clave pública (PKI)	Conjunto integrado de tecnologías necesario para proporcionar un cifrado por clave pública y firmas digitales. Utiliza una combinación de cifrado por clave pública y privada que ofrece gestión de claves e integridad y confidencialidad de los datos.
Proceso	Serie documentada de tareas secuenciales que se utiliza para realizar una función del negocio.

6. RIESGOS

Los riesgos identificados están consolidades en la matriz de riesgos o mapa de calor con base en el levantamiento de los activos de información siguiendo los lineamientos de la guía para la administración del riesgo y diseño de controles en entidades públicas, (riesgos de gestión, Corrupción y seguridad Digital) de la Función Pública, Dirección de gestión y desempeño Institucional, de los riesgos identificados en la aplicación del Mapa de Calor en el inventario de activos de Información se reflejaron un 30% extremos y Altos a los cuales se implementaran Objetivos de control para minimizar su impacto si se logran materializar.

RIESGOS	ACCIONES
Perdida de Confidencialidad, disponibilidad e integridad de la Información	1. Socialización de la política de gobierno digital. 2. Implementar el acuerdo de confidencialidad para los funcionarios, contratistas, terceros, aprendices, practicantes y proveedores.

	3. Ejecutar el mapa de ruta en el periodo indicado con el acompañamiento de la gerencia. 4. Asignación de recursos para la implementación y mitigación de riesgos de seguridad de la información. 5. Actualización de los activos de la información. 6. Plan de Implementación. 7. Realización comité de seguridad de la información. 8. Asignación de roles y responsabilidades a sus colaboradores frente a la seguridad de la información.
Posibilidad de asignación de usuarios en el sistema de información sin tener en cuenta el rol o perfil del cargo para su acceso.	1. Formato creación, retiro, modificación, inactivación de usuarios. 2. Procedimiento de registro y cancelación de usuarios 3. Tener fuentes de respaldo de la información del sistema de información
Divulgar información confidencial y reservada a terceros a cambio de un beneficio	1. Implementar el acuerdo de confidencialidad para los funcionarios, contratistas, terceros, aprendices, practicantes y proveedores. 2. Asignación de roles y responsabilidades a sus colaboradores frente a la seguridad de la información.

7. CONTENIDO

7.1. INTRODUCCIÓN

El Hospital desde el año 2021 inicio su proceso de implementación gradual de los componentes de seguridad de la información y largo de estos años se fortaleció gradualmente con elementos físicos de seguridad informática de TI, que deben acompañar la política de seguridad de la información, e iniciando un proceso de transformación cultural al interior de la organización reconociendo la información como un producto valioso de la las organización, se inició nombrando el Ciso, u oficial de seguridad, socializando la política e involucrando a la alta gerencia, la implementación del modelo de privacidad y seguridad de la información en el Hospital Departamental Mario Correa Rengifo se establece con conjunto de actividades basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) para crear condiciones de uso confiable en el entorno

digital y físico de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información las metodologías utilizadas para valorar la madurez de la seguridad en el Hospital son basado en la Norma Técnica Colombiana ISO27001:2013 y la autoevaluación MSAT de Microsoft.

La madurez de la seguridad incluye los controles (tanto físicos como técnicos), la Competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. La madurez de la seguridad se puede medir únicamente a través de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas. Debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir las áreas en las que centrar los programas de seguridad de la empresa. No todas las empresas deben esforzarse por alcanzar el nivel óptimo, pero todas deben evaluar en qué punto se encuentran y determinar el lugar que deberían ocupar en vista de los riesgos comerciales a los que se enfrentan. Por ejemplo, puede que una empresa con un entorno de bajo riesgo no necesite nunca subir encima del límite superior del nivel básico o el límite inferior del nivel estándar. Las empresas con un entorno de alto riesgo probablemente entren de lleno en el nivel optimizado. Los resultados del perfil de riesgos para la empresa le permiten hacer un balance de los riesgos.

Este documento contiene objetivos, generalidades, contexto, alcance, contexto normativo, definiciones, metodología de implementación y mapa de ruta con las actividades a ejecutar con sus correspondientes fechas y responsables.

Se define para el 2026, siguiendo los lineamientos de MINTIC quien adopta la norma ISO27000 y ISO 31000 para gestión de riesgos como framewords de gestión de seguridad de la información para implementar en las organizaciones del estado, con base en estos lineamientos se aprueba en enero del 2022 el plan de tratamiento a riesgos de seguridad de la información donde se definen 4 fases y 7 etapas para ejecutar para la implementación de las buenas prácticas de seguridad de la información, 7 etapas (1. SGSI como un proyecto transversal a la organización, 2.- inventario de activos, 3.- levantamiento e identificación de riesgos, 4.-implementacion de controles y requisitos de la ISO 27002, 5.- pruebas de la seguridad de la información, 6.- capacitacion y socialización. 7 mantenimientos y actualizaciones, por ser una norma ISO con una puesta en marcha largo plazo se define una metodología para gestionar el indicador que evalué la implementación y se realiza de acuerdo a madurez de controles de CMM que referir a: Capability Maturity Model), quien define una metodología evaluar el modelo basados en la madurez con las siguientes variables, Inexistente, Inicial / Ad-hoc,Reproducible, pero intuitivo, Proceso definido, Gestionado y medible y Optimizado, la evaluación se realiza sobre los 114 controles del sistema de gestiona de seguridad de la información y se evalúan los procesos definidos, donde los

procesos definidos evidencian proceso de adherencia al uso de las buenas prácticas de gestiona de la seguridad de la información en la ESE

En el año 2023 se logró avanzar en la implementación de las etapas (1. SGSI como un proyecto transversal a la organización, 2.- inventario de activos, 3.- levantamiento e identificación de riesgos, 2024 Y 2025 se entra a la etapa más compleja que está relacionada 4.-implementacion de controles y requisitos de la ISO27002, seguimiento trimestral al comportamiento de la matriz de riesgos e implementación del procedimientos para gestionar objetivos de control a los riesgos extremos y altos identificados en el mapa de calor y reporte a planeación de los riesgos materializados e intervenidos en cada trimestre, de acuerdo con el mapa de ruta en el 2026, se continuara con el afianzamiento y seguimiento de la implementación de los objetivos de control con base en el procedimiento y la matriz aprobada para reportar y analizar incidentes de seguridad de la información **ETAPA 6.- CAPACITACION Y SENSIBILIZACION** Elaborar, aprobar y socializar Plan de sensibilización y capacitación en Seguridad y Privacidad de la información, implementar Plan de sensibilización y capacitación del Sistema de Gestión de Seguridad de la información, Análisis de resultados del Plan de sensibilización y capacitación del Sistema de Gestión de Seguridad de la información
ETAPA 7.- MANTENIMIENTO Y ACTUALIZACION, Elaborar, aprobar y socializar programa para la evaluación y seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información, Evaluar Acciones Correctivas y Acciones de Mejora del Sistema de Gestión de Seguridad de la Información, Revisar y gestionar e intervenir resultados de las Auditorías al Sistema de Gestión de Seguridad de la Información ,Revisar, gestionar e intervenir los reportes de Incidentes de Seguridad de la Información, Evaluar los resultados y tendencias de los indicadores trazadores del Sistema de Gestión de Seguridad de la Información

7.2. RESEÑA HISTORICA

El Hospital es una institución de Nivel II de complejidad, de carácter público Departamental, creado desde 1.972 para atender a la población de escasos recursos económicos del Municipio de Cali - Colombia, ubicado en el barrio Mario Correa de la Comuna 18. Inicialmente funciona como un centro de atención para la tuberculosis y con el correr del tiempo, el Hospital sufrió muchos cambios a su interior, con la apertura progresiva de nuevos servicios asistenciales, fortaleciendo su recurso humano y tecnológico, para satisfacer la demanda creciente, especialmente en servicios como urgencias, cirugía y hospitalización. En los años 80 el hospital genera una expansión de sus servicios asistenciales y se construyen nuevas áreas administrativas y para la atención de pacientes en Urgencias, Pediatría y Pensionados. El hospital entonces se constituye en pieza clave y protagónica de la red de prestadores de servicios de salud de Cali y el Valle del Cauca. Adecuándose

a la Ley de Seguridad Social en Salud, las directivas de la entidad tomaron la decisión de reorganizar y modernizar cada uno de los servicios asistenciales y de apoyo administrativo, con el fin de convertir la entidad, en una Institución Prestadora de Servicios (IPS) fundamentado en los principios de calidad y eficiencia. En el año de 1995 se convierte en Empresa Social del Estado descentralizada (Decreto 1808 del 7 de noviembre de 1995), con autonomía administrativa y patrimonio propio.

7.3. UBICACIÓN

La ESE Hospital Mario Correa Rengifo, está ubicado en la comuna 18 de la ciudad Santiago de Cali, más específicamente en la carrera 78 Oeste No. 2ª -00, teniendo como área de influencia las comunas 1, 3, 9, 17, 18,19, 20 y corregimientos aledaños como la Buitrera y Pance y demás que colindan con el occidente de Cali.

7.4. MISIÓN

Somos una institución prestadora de servicios de salud de mediana complejidad, que brinda una atención oportuna, humanizada, segura e incluyente, para nuestros usuarios y clientes, con talento humano calificado y comprometido con el mejoramiento continuo.

7.5. VISIÓN

Para el año 2026 seremos una institución acreditada, reconocida por la prestación de servicios de salud con énfasis quirúrgico, apoyada con una adecuada tecnología y una cultura organizacional humanizada, sostenible y amigable con el medio ambiente.

7.6. CONTEXTO ESTRATÉGICO

El presente plan está alineado y contribuye al logro de la misión, visión y mega y demás elementos del direccionamiento estratégico del Hospital, los cuales se estipulan en el Plan de desarrollo – vigente (2024-2027).

7.6.1. ARTICULACIÓN CON MIPG

Gestión y Desempeño Institucional - MIPG	• Política Gobierno Digital • Política de Seguridad Digital

	• Política de Gestión Documental • Política de Transparencia, acceso a la información pública, lucha contra la corrupción y las comunicaciones. • Gestión del conocimiento y la innovación • Política de Gestión Documental • Política Gestión de la información estadística

7.7. DESARROLLO DEL PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

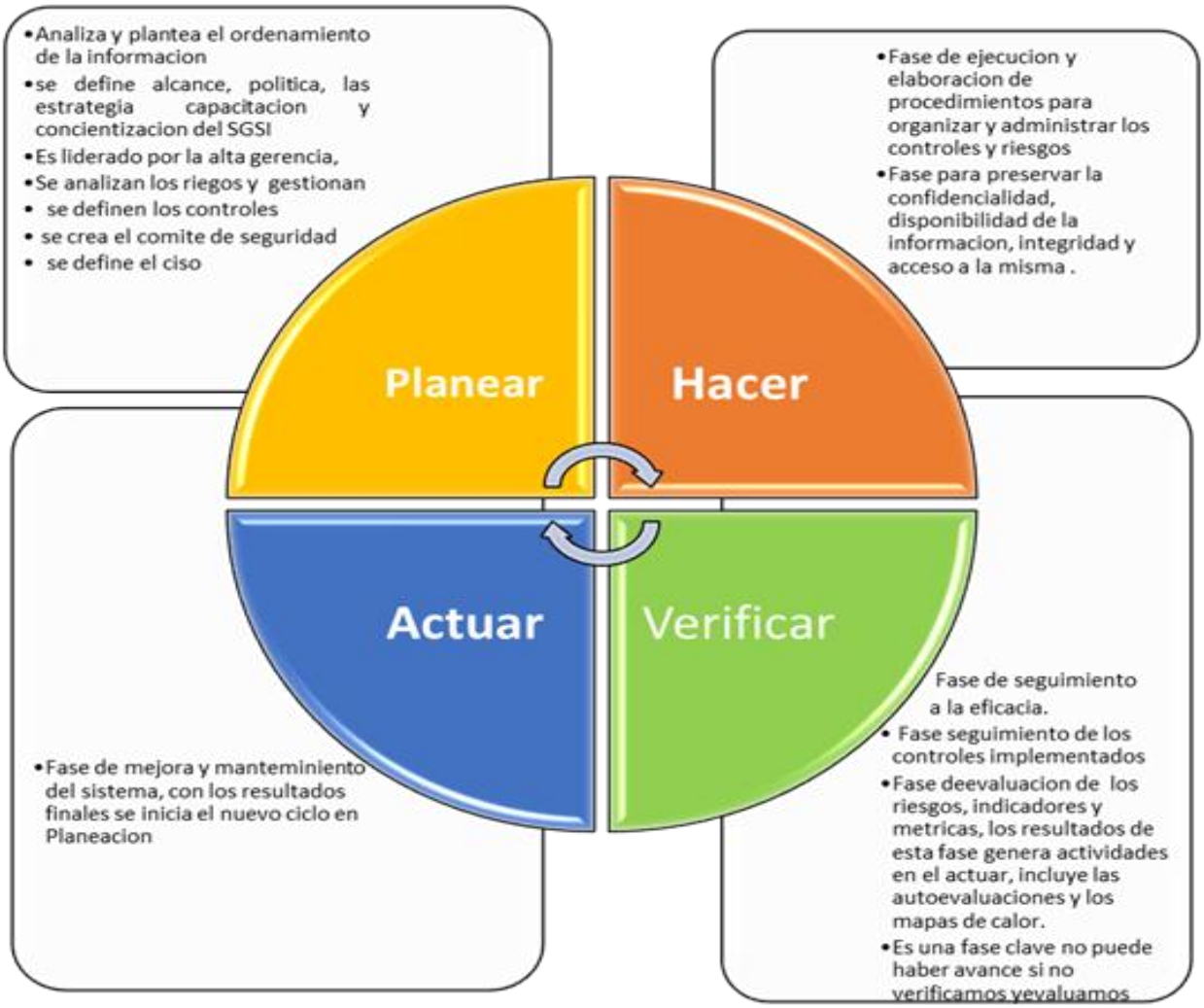
7.7.1. METODOLOGÍA DE IMPLEMENTACIÓN

La metodología de implementación del Plan de Seguridad y Privacidad para el Hospital Departamental Mario Correa Rengifo ESE, está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC:

7.7.2. CICLO DEL SGSI SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El sistema de gestión de la seguridad de la información tiene un enfoque sistémico, se administra bajo el enfoque PHVA planear, hacer, verificar y actuar.

CICLO DEL SGSI



7.7.3. ACTIVIDADES REALIZADAS

Etapas previas a la implementación:

- Estado inicial de la entidad se identificó frente a la norma iso el estado actual Identificar el nivel de madurez se inició con un nivel de madurez del 18% en al cerrar el 2021 de los 114 controles de seguridad un 39% eran reproducibles pero instructivos, no se había logrado identificar una metodología adecuada que permitiera avanza en la implementación de la normas de seguridad de la información mediante un ciclo PHVA, en el 2022, se estructuraron la 7 etapas siguiendo los lineamientos de las guías MINTIC, logrando de esta manera reorientar el proceso de implementación evidenciando avances notorios como el levantamiento de activos de información por procesos con análisis de criticidad y el levantamiento del mapa de calor de acuerdo a las guías Mintic y se logró avanzar de la 1 a la 4 en el 2024 se identificaron los objetivos de control y se implementaron mediante un procedimiento aprobado para guardar y preservar la seguridad de la información siguiendo los lineamientos del ciclo PHVA de implementación de la seguridad de la información en la ESE, en el 2024 se cerró con una madurez del 58,77%. Y en el 2025 e logro cerrar con una madurez del 76.65% logrando un avance en procesos definidos y procesos gestionados y medibles

- A nivel se seguridad informática se alineo la identificación de debilidades y se cerraron las brechas relacionadas con el requerimiento de necesidades de TI relacionadas con infraestructura de seguridad firewall físico, licenciamiento antivirus, política de seguridad, comité de seguridad y mapa de riesgos y procedimiento administración usuarios y perfiles.

Planificación:

- Contexto de la entidad.
- Liderazgo para implementar seguridad desde TI hacia las buenas prácticas Planeación se conforma comité de seguridad de la información y se nombra siso Soporte se adopta iso27001 como estándar a seguir e implementar Inventario de activos 1era fase físicos y lógicos

Implementación:

- Control y planeación operacional

- Evaluación de riesgos de Seguridad y Privacidad de la Información
- Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Evaluación de Desempeño:
- Monitoreo, medición, análisis y evaluación.
- Mejora continua:
- Acciones correctivas y no conformidades

En las etapas 6 y 7 del ciclo PHVA:

- Evaluación de Desempeño:
- Revisión por la dirección
- Mejora continua:
- Auditoría interna
- Actualización del Inventario de Activos fase 2025, juntamente con la implementación del FUID formato único de inventario de gestión Documental

7.7.4. CUMPLIMIENTO DE LA IMPLEMENTACIÓN

En la elaboración del plan de tratamiento de seguridad de la información integramos tres (3) framewors para su consolidación, msat, isaca y iso27001, msat nos permitió realizar una autoevaluación de detallada de cada categoría y subcategoría de los componentes de seguridad de la información, isaca nos permitió evaluar los riesgos materializados para lograr su intervención, en el 2025 se realizaron 4 mediciones y se reportaron al proceso líder de riesgos de la ESE y iso27001 valorar el avance y madurez de la implementación y de controles y requisitos de seguridad de la información

al finalizar el periodo 2025 Se gestiono el indicador de acuerdo a madurez de controles de CMM que referir a: Capability Maturity Model), quien define una metodología evaluar el modelo basados en la madurez con las siguientes variables, Inexistente, Inicial / Ad-hoc,Reproducible, pero intuitivo, Proceso definido, Gestionado y medible y Optimizado, la evaluación se realiza sobre los 114 controles del sistema de gestión de seguridad de la información y se evalúan los procesos definidos, en el cuarto se llegó a la meta de controles definidos y con madurez 67 controles que representan un 58,77% de los controles a implementar, y 11 controles gestionados y medibles que representan el 10%, la implementación se realiza de acuerdo a las guías mintic definidas para la implementación del sistema de gestión de la seguridad que adopta is027000 con framewoks , se logró un avance en el levantamiento del inventario de activos de información y el análisis de la criticidad de la misma con 89 activos de información de 4 procesos , para lo cual se entregaron

y socializo un instructivo e instrumento para el diligenciamiento, ningún proceso reporto avances, se realiza las solicitudes para el último trimestre con la entradas y salidas de las caracterizaciones de los procesos , pendiente de levantar proceso algunos procesos administrativos y el total de los asistenciales para continuar en el 2026 con la implementación de controles de la norma is027002

7.8. INVENTARIO ACTIVOS DE INFORMACION 2024

Tipología del Inventario de Activos

NOMBRE DEL ACTIVO	CANTIDAD
INSTRUCTIVO PARA GENERAL COPIA RESPALDO EQUIPOS CLIENTE	1
PLAN ESTRATEGICO DE TECNOLOGIA DE INFORMACIÓN 2023 (PETI)	1
12 SINF-P-011-02 Plan de contingencia informática	1
24.-SINF-P-011-04 Procedimiento para restauración de la copia de seguridad del sistema de información V3	1
Acces Pont Total 10 AP	1
Actas y autorizaciones	1
BASE DE DATOS NOMINA 1992 A 2002	1
BASES DE DATOS NOMINA 1992 - 2001 pensionados	1
BASES DE DATOS NOMINA 1992 - 2001 planta	1
CARACTERIZACION PROCESO DE TI	1
Centro de Computo	1
Consola de Antivirus con 325 licencias	1
CONTRATO EMCALI CONTRATO DE PRESTACION DE SERVICIOS Y/O SOLUCIONES DE COMUNICACIONES	1
Contratos y actas de soporte y seguimiento proveedores TI	1
CTO 018-2021 ZYNKO	1
DATAISS	1
Descripción de módulos de Panacea	1
DIAGRAMA DE LA RED	1
ESTRUCTURA ORGANIZACIONAL	1
Firewall - UTM	1
FUID FORMATO UNICO DE INVENTARIO	1

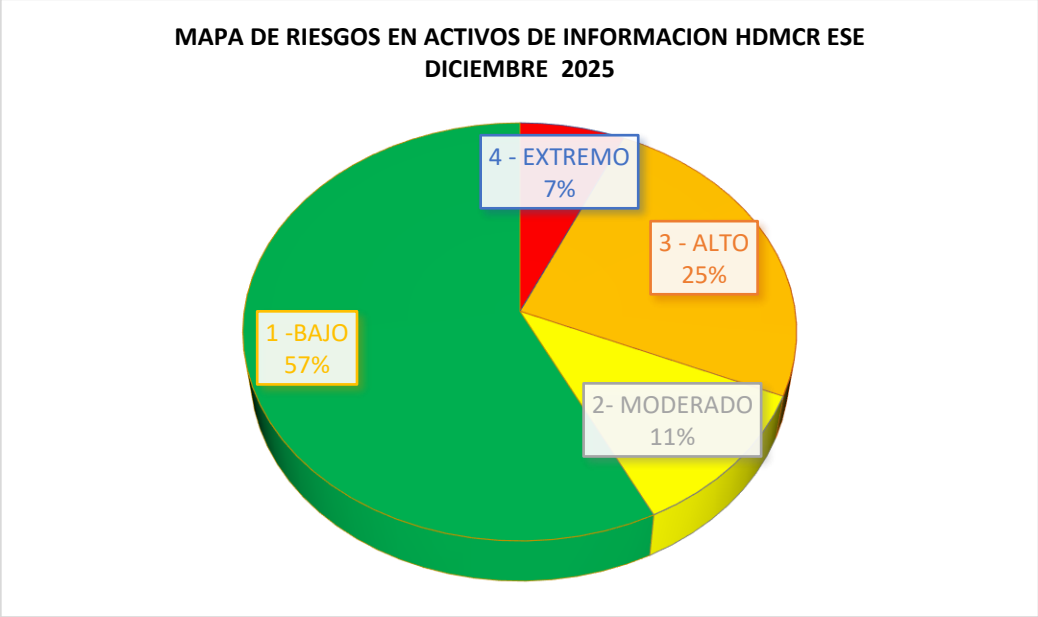
NOMBRE DEL ACTIVO	CANTIDAD
infraestructura tecnológica de tecnologías de información, red eléctrica regulada, no regulada, planta eléctrica y central eléctrica	1
INSTRUCTIVO PARA LEVANTAMIENTO DE ACTIVOS DE INFORMACION	1
LICENCIA HOSTING PAGINA WEB	1
LICENCIA PANACEA CNT SISTEMAS DE INFORMACION S. A	1
LICENCIA RFAST	1
LICENCIA WINDOWS SERVER	1
LICENCIAMIENTO MICROSOFT OFFICE TIGO UNE	1
LICENCIAMIENTO UTM	2
LICENCIAS F-SECURE LICENSE CERTIFICATE	1
MANUAL DE CLASIFICACION DOCUMENTAL	1
MANUAL DE GESTION DE LA INFORMACION	1
MANUAL DE USUARIO RFAST	1
MANUAL DE USUARIO SATHO Y SAS Y ACTIVOS FIJOS	1
MANUAL DE VALORACION DOCUMENTAL	1
MANUALES DE USUARIO PANACEA	1
MICROSOFT VOLUME LICENSING SERVICE CENTER	2
Nodos de Red lógica	1
OS 012-2021-MEGABUSINESS	1
OS 038-2021 CNT PANACEA	1
OS 039-2021 UNE TIGO	1
OS 047-2021-MES DE OCCIDENTE (ANTIVIRUS)	1
OS 067-2021-TECHNOLY WORLD GROUP	1
OS-023-2021 SERVIMANTENIMIENTO	1
Página Web Institucional	1
PLAN DE MANTENIMIENTO EQUIPOS DE COMPUTO PROPIOS	1
PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD DE LA INFORMACION	1
PLAN INSTITUCIONAL DE ARCHIVO PINAR	1
PMA	1
PROCEDIMIENTO DE MINERIA DE DATOS	1
PROCEDIMIENTO PARA LA GESTION DE NECESIDADES DE SISTEMAS DE INFORMACION	1
PROCEDIMIENTOS DE ADMINISTRACION Y CANCELACION DE USUARIOS	1
PROCESO DE GESTION DE SISTEMAS DE INFORMACION	1
PROGRAMA DE GESTION DOCUMENTAL PGD	1
REDES ELECTRICAS QUE SOPORTAN EL PROCESO DE TI DEL hospital	1
Rfast sistema de información cliente Servidor	1
Roter_Claro Roter_Movistar	1
Satho Sistema Administrador y liquidador de Nomina	1
Servidor de aplicaciones de Pruebas en Máquina virtual	1
Servidor de Aplicaciones Sistemas de información Panacea	1
Servidor de BD Asistencial y administrativa	1

NOMBRE DEL ACTIVO	CANTIDAD
Servidor HIS Panacea y Annar exámenes de laboratorio a Panacea	1
Servidor Máquina virtual panacea remoto por IP Publica	1
Servidor sistema de información RFAST sistema de información contable año 2001 a 2020	1
Servidor SRVAPP1 Controlador de Dominio o directorio activo	1
Servidor SRVAPP3 servidor de aplicaciones Sistema de información Panacea	1
SINF-P-011-10 Procedimientos de ventanilla única	1
SINF-P-011-11 Procedimiento de transferencia primaria	1
Sistema de información COSTOS	1
Sistema de información Panacea Web	1
Sistema de información SIAGHO	1
Sistemas de información administración datos biométrico	1
SOFTWARE DEPOSITOS JUDICIALES	1
SOFTWARE GEMA ACTIVOS FIJOS	1
SOFTWARE HELISA	1
SOFTWARE INDICADORES	1
SOFTWARE MODULO PROGRAMACION DE CIRUGIA	1
SOFTWARE RFAST4 Y CARTERA	1
SOFTWARE SARP	1
SOFTWARE SAS	1
SOFTWARE SATISFACCION	1
Software Ventanilla Única	1
SW_Core - Cantidad 1	1
Switches - Cantidad 8	1
Tabla de indicadores trazadores del proceso de TI	1
TABLAS DE RETENCION DOCUMENTAL APROBADAS	1
Videos guía Historia clínica Urgencias, medicamentos, ingreso de pacientes, ordenes quirúrgicas y ayudas diagnosticas	1
Total, general	**89**

De inventarió de activos el 43% de la información es publica, el 32% es reservada, la pública como manuales y guías se publicó en el portal del Estado Colombiano www.datos.gov.co

NIVEL DE CRITICIDAD DE LOS ACTIVOS DE INFORMACION

Tipo Riesgos	Cantidad	FR	FA
4 - EXTREMO	6	6,74%	7%
3 - ALTO	22	24,72%	31%
2- MODERADO	10	11,24%	43%
1 -BAJO	51	57,30%	100%
Total, general	**89**		



EL nivel de criticidad el 7% extremo, 7% Alto 11% moderado y 57% bajo del inventario

7.9. MAPA DE RIESGOS

De acuerdo con la guía para la administración del riesgo y diseño de controles en entidades públicas de la Función Pública se construyó el instrumento para la valoración del riesgo de los activos de información de la ESE, valorando la probabilidad y el impacto del activo, de la valoración de 86 activos de información el 21% se clasificaron de acuerdo con la tabla de medición en riesgo Extremo.

PROBABILIDAD DE IMPACTO						
Casi Seguro	5	51	52	53	54	55
Probable	4	41	42	43	44	45
Posible	3	31	32	33	34	35
Improbable	2	21	22	23	24	25
Rara Vez	1	11	12	13	14	15
		1	2	3	4	5
		Insignificante	menor	Moderado	Mayor	catastrófico

IMPACTO

Fuente Adaptado de Instituto de auditores internos COSO ERM 2017

Importante: Matriz de criticidad de 5x5 significa que para ubicar el nivel de riesgo se cuenta con 5 niveles en probabilidad y 5 niveles en impacto

Extremo			**15 - 25 - 34 - 35 - 44 - 45 - 53 - 54 - 55**
Alto			**14 - 24 - 33 - 42 - 43 - 51 - 52**
Moderado			**13 - 23 - 32 - 41**
Bajo			**11 - 12- 21- 22 - 31**

MATERIALIZACION DE LOS RIESGOS DE TI DICIEMBRE DE 2025

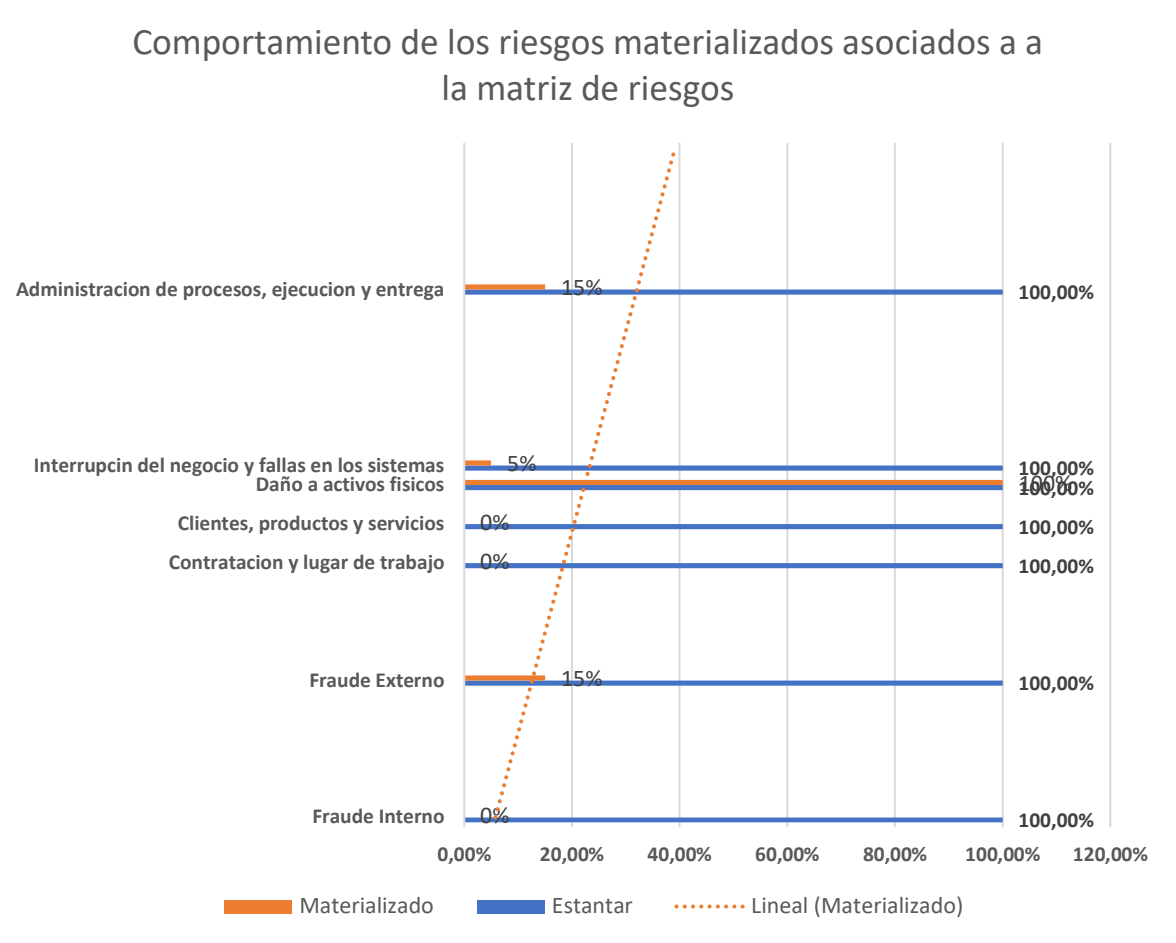
Tipos de evento de riesgo con los aspectos de tecnología relacionados			**Impacto**	**Se Materializo**	**Observación**	
Tipo de Evento	**Aspectos de TI**	**Estándar**				Materializado
Fraude Interno	Manipulación indebida de los programas	100,00%	10%	NO		0%
	Uso no autorizado de funciones para modificación de programas		20%	NO		
	manipulación deliberada de las instrucciones del sistema		10%	NO		
	Manipulación deliberada del Hardware		5%	NO		
	Cambios deliberados a los sistemas aplicaciones por medio de accesos internos no autorizados		20%	NO		
	Uso indebido de Software no autorizado o sin licencia		5%	NO		
	Evasión interna de los privilegios de acceso		30%	NO		
Fraude Externo	Cambios deliberados a los sistemas y aplicaciones mediante accesos externo no autorizados	100,00%	15%	NO		15%

Tipos de evento de riesgo con los aspectos de tecnología relacionados			Impacto	Se Materializo	Observación	
	Obtención de acceso por parte de intrusos hacia documentos físicos o electrónicos		15%	SI	Peridad de la información bases de datos de la operación de la empresa, por el uso inadecuado de los lineamientos para las copias de seguridad diaria y periódica a dispositivos seguros y confiables, el hospital por la debilidad presupuestal no tiene la capacidad de financiar una copia en la nube o externa y en el momento de un ataque que afecte toda la red interna puede afectar las copias de seguridad que se almacenan de manera interna **COPIAS DE SEGURIDAD EN LA NUBE**	
	Evasión externa de los privilegios de acceso		15%	NO		
	Intercepción de los canales de comunicación		10%	NO		
	Contraseñas comprometidas		15%	NO		
	Virus		30%	NO		
	Uso indebido de los recursos de tecnología de información	100,00%	20%	NO		0%

Tipos de evento de riesgo con los aspectos de tecnología relacionados			Impacto	Se Materializo	Observación	
Contratación y lugar de trabajo	Carecer de responsabilidad hacia la seguridad informática		80%	NO		
Clientes, productos y servicios	Divulgación de información sensitiva hacia terceros por parte de los empleados	100,00%	70%	NO		0%
	Administración de Proveedores		30%	NO		
Daño a activos físicos	Daños intensionales, accidentales, o riesgos posibles a la infraestructura física de tecnología de información	100,00%	100%	SI	El centro de cómputo del Hospital al ser evaluado frente a las buenas prácticas de TI no cumple en requisitos internos como son los puestos de trabajo, el acceso restringido, aire acondicionado húmedo y sin contingencia, detectores de humo, y lo más riesgoso la seguridad perimetral den centro de cómputo, puerta de acceso un madera, paredes en superboard, hacinamiento de puestos de trabajo y equipos, ausencia de área de taller, siendo el centro de concentración de los servidores de bases de datos, nodo principal de la red y servidores de aplicaciones,	100%

Tipos de evento de riesgo con los aspectos de tecnología relacionados			Impacto	Se Materializo	Observación	
					puede convertirse en objetivo de robo ò secuestro de servidores e información por la debilidades en la seguridad perimetral expuesta ***CENTRO DE COMPUTO***	
Interrupción del negocio y fallas en los sistemas	Mal funcionamiento de hardware o software	100,00%	5%	NO		5%
	Fallas en las comunicaciones		5%	SI	Se presenta un daño irreparable a la planta telefónica de vigencia 2004 en estado de obsolencia y sin repuestos en el mercado de proveedores **PLANTA TELEFONICA**	
	Sabotaje de los empleados		5%	NO		
	Perdida de personal clave de tecnología		5%	NO		
	Destrucción de archivos de datos o Software		18%	NO		
	Virus computacionales		15%	NO		
	Fallas en los respaldos de información		20%	NO		
	Ataques para negar el servicio		7%	NO		
	Errores en la configuración		5%	NO		
Administración de procesos,	Errores en la manipulación de datos electrónicos	100,00%	15%	NO		15%

Tipos de evento de riesgo con los aspectos de tecnología relacionados			Impacto	Se Materializo	Observación	
ejecución y entrega	Estaciones de trabajo sin atención		5%	SI	Falta de mantenimiento a las baterías de las upss que soportan los 5 nodos de red, desconexión de servicios de ti de los puntos conectados a los nodos, riesgo de incendio, inundación y daño de equipos, control de acceso débi**l UPS COBERTURA**	
	Errores al realizar cambios		10%	NO		
	Entradas de datos incompletas a las transacciones del sistema		20%	NO		
	Errores de entrada o salida de datos		20%	NO		
	Errores de programación o de pruebas		15%	NO		
	Errores de operación		10%	SI	Operación de ti no soportada por una fuente regular de energía que garantice la disponibilidad del fluido eléctrico constante para soportar la continuidad del negocio **CENTRAL DE TRASFERENCIA ELECTRICA Y PLANTA ELECTRICA**	
	errores de procesamiento manual		5%	NO		
Fuente ISACA, The IT Dimesion of basel II		**100,00%**				**19,29%**



En la gráfica de materialización de riesgos extremos según la matriz de riesgos 1.0 de la hoja 1 del archivo se puede observar un riesgo expuesto a materializarse relacionado con vulnerabilidades en el centro de cómputo relacionados con su seguridad fiscal perimetral, generado por la débil infraestructura física que presenta el centro de cómputo frente a los requisitos de buenas prácticas definidas, el hospital puede ser objeto de un secuestro de servidores y bases de datos almacenadas y también esta vulnerable a la interrupción de algún tipo de persona a las instalaciones, por no contar con un control de acceso seguro, puerta de acceso madera, oficina y centro de cómputo sin separación segura y divisiones en superboard, la débil cobertura de las UPS en el hospital que representan el 50% de la cobertura total expone el procesamiento de información en las estaciones de trabajo de los usuarios, de la misma manera la debilidad observada en la central de transferencia y planta eléctrica expone la operación u el funcionamiento de la red lógica y eléctrica que soporta el sistema de información del hospital, incluyendo la debilidad observada en el procedimiento de copias de seguridad de la información por no contar con un proveedor o servicio de copias externas o en la nube expedito, la razón y ausencia y debilidad de estos riesgos el débil presupuesto asignado en la vigencia 2025, y la débil relación con los proveedores de TI del hospital, la solución a todos estos riesgos en proceso de materialización está en la

asignación de los recursos presupuestales para fortalecer la relación con los proveedores y adquirir las deficiencias, en la evaluación de materialización o posible materialización representa en la matriz ISACA UN 19,29%

Al finalizar el 2025 y al analizar y clasificar los activos de información de tecnologías de información en el mapa de Riesgos siguiendo los lineamientos de los anexos técnicos de MINTIC y MIPG que adopta ISO27000 para el tratamiento de riesgos de seguridad de la información, podemos identificar que los riesgos extremos representan un 6,74%, los riesgos altos representan un 24,72%, los moderados un 11.24% y bajos el 57.30, los extremos y altos corresponden a los que en pueden afectar la infraestructura de tecnologías de información de manera transversal a toda la ESE, y están concentrados en la aplicación de controles de la iso27002 relacionados con Falla en la operación, control de acceso físico al sitio, débil seguridad perimetral, puertas y divisiones débiles e inadecuadas, falta de detectores de humo, incendio, inundación y robo de servidores, seguridad perimetral física expuesta vulnerable, sin cumplimiento de los requisitos mínimos del centro de cómputo separación de puestos de trabajo, área centro de cómputo expuesta

Falta de mantenimiento a las baterías de las upss que soportan los 5 nodos de red, desconexión de servicios de ti de los puntos conectados a los nodos, riesgo de incendio, inundación y daño de equipos, control de acceso débil Operación de ti no soportada por una fuente regular de energía que garantice la disponibilidad del fluido eléctrico constante para soportar la continuidad del negocio, la infraestructura Servidores, base de datos, Centro de cómputo, nodos de red, Redes, UPSs y aplicaciones , riesgos unos mitigables con los relacionados con el fortalecimiento de la infraestructura como los nodos de red y centro de cómputo seguridad física perimetral y sistema de información panacea, y otros mitigables con la implementación de buenas prácticas de seguridad informática y seguridad de la información, el fortalecimiento está asociado a recursos los cuales están ya relacionados en el plan estratégico de ti PETI para cada vigencia y los mitigables en el plan de tratamiento a riesgos de seguridad de la información o sistema de gestión de seguridad de la información de la ese SGSI de acuerdo al siguiente detalle.

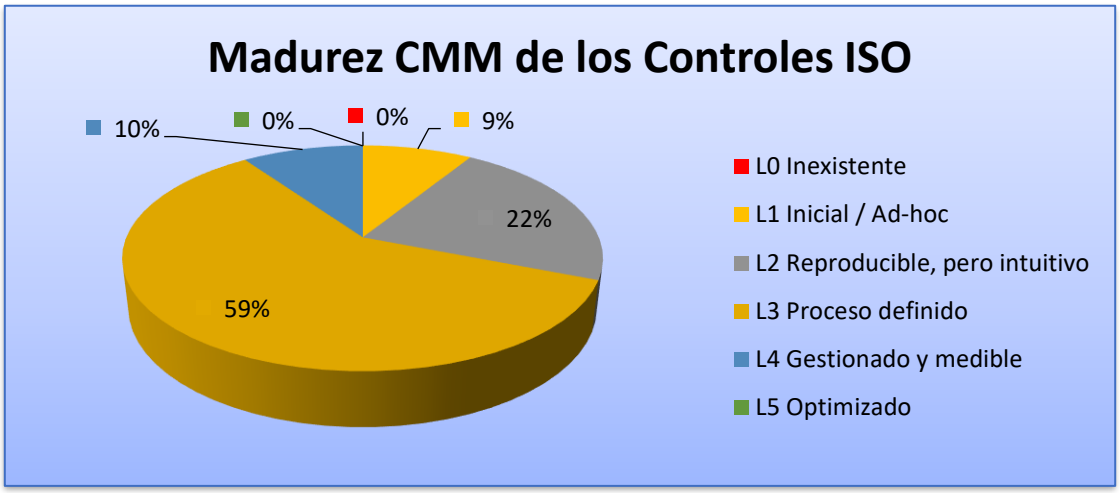
Falla en la operación, control de acceso físico al sitio, débil seguridad perimetral, puertas y divisiones débiles e inadecuadas, falta de detectores de humo, incendio, inundación y robo de servidores, seguridad perimetral física expuesta vulnerable, sin cumplimiento de los requisitos mínimos del centro de cómputo separación de puestos de trabajo, área centro de cómputo expuesta CENTRO DE COMPUTO

Falta de mantenimiento a las baterías de las upss que soportan los 5 nodos de red, desconexión de servicios de ti de los puntos conectados a los nodos, riesgo de incendio, inundación y daño de equipos, control de acceso débil UPS COBERTURA

Operación de ti no soportada por una fuente regular de energía que garantice la disponibilidad del fluido eléctrico constante para soportar la continuidad del negocio CENTRAL DE TRASFERENCIA ELECTRICA Y PLANTA ELECTRICA

7.10. NIVEL DE MADUREZ DEL SGSI 2025

Estado de avance de la madurez de la seguridad esa norma técnica NTC-ISO 27001



En la evaluación se idéntica que, de los 14 Dominios, 34 Objetivos de control y 114 Controles de la norma de seguridad **NTC-ISO 27001 un 59% son controles ya procesos definidos,** un 10% gestionados y medibles, 22% reproducible e intuitivo y hace parte de la cultura organización de la ESE y un 9% está en etapa inicial

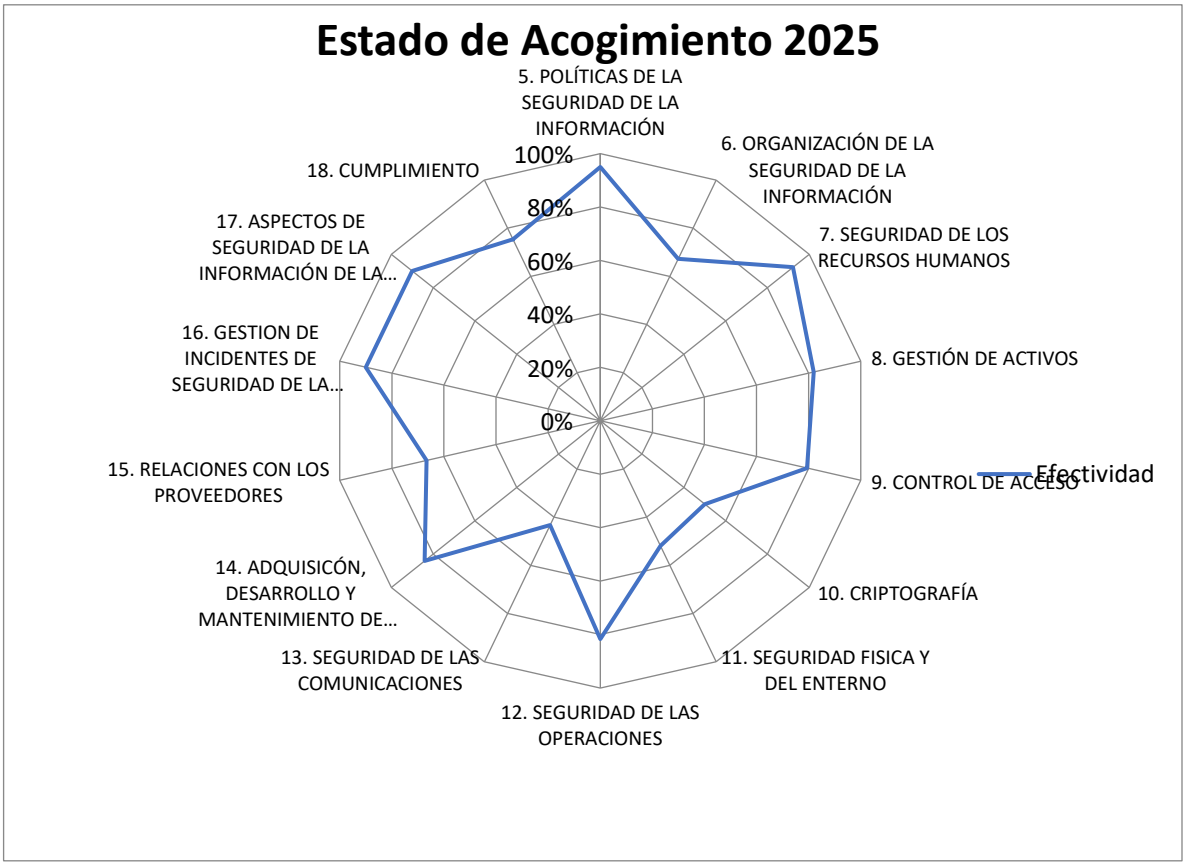
Porcentaje cumplimiento 14 controles de la norma técnica iso27001 2023

Control	Efectividad
5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	95%
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	67%
7. SEGURIDAD DE LOS RECURSOS HUMANOS	92%
8. GESTIÓN DE ACTIVOS	82%
9. CONTROL DE ACCESO	79%
10. CRIPTOGRAFÍA	50%
11. SEGURIDAD FISICA Y DEL ENTERNO	52%
12. SEGURIDAD DE LAS OPERACIONES	82%
13. SEGURIDAD DE LAS COMUNICACIONES	43%
14. ADQUISICÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	84%

Control	Efectividad
15. RELACIONES CON LOS PROVEEDORES	67%
16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	90%
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	90%
18. CUMPLIMIENTO	75%

Hoja Radar cumplimiento de la norma técnica ISO27001

En la hoja radar se evidencia que los 14 controles de seguridad de la información de desplegaron del centro hacia los bordes del grafico evidenciando el desarrollo e implementación en la vigencia 2025.



Para este periodo4 trimestre del 2025 en la evaluación de la seguridad digital se continua con el deterioro de la seguridad y el hospital se expone más a la materialización de riesgos socializa la política de uso y tratamiento de datos personales, continuando con las actividades de gestión de seguridad de la información.

Al evaluar la calificación de los 34 objetivos de control 4 se encuentra gestionado y medible, 14 de los 34 están definidos y cuentan con la madurez en la implementación y la organización reconoce su desarrollo e implementación, 16 están en estado Reproducible, pero intuitivos, están en proceso de maduración y fortalecimientos y 0 son inexistentes en su implementación, de las medidas a fortalecer en a implementación del SGSI, el 50% de la red de energía del sistemas de información están conectadas a la red eléctrica no regulada, más la afectación que genera sobre la operación del sistema de información la sobre cargas en tableros eléctricos y la disfuncionalidad de la central de transferencia y la planta eléctrica del Hospital, en el 2025 logramos adquirir y renovar licencia y compra FIREWALL o UTM dispositivo de gestión unificada de amenazas , equipo que genero riesgos en un periodo significativo de la vigencia pero fue superado en el mes de noviembre, el hospital al cerrar la vigencia garantiza la seguridad informática renovando su FIREWALL y antivirus elementos claves y esenciales de la seguridad informática y eje primordial en la implementación de las normas ISO27000

NIVEL DE IMPLEMENTACION DE LOS OBJETIVOS DE CONTROL EN EL 2025

Orden	Objetivos de Control	Efectividad
1	5.1 Orientación de la dirección para la gestión de la seguridad de la información	95%
2	7.1 Antes de asumir el empleo	95%
3	8.1 Responsabilidad por los activos	93%
4	7.2 Durante la ejecución del empleo	92%
5	16.1 Gestión de incidentes y mejoras en la seguridad de la información	90%
6	7.3 Terminación y cambio de empleo	90%
7	8.2 Clasificación de la información	90%
8	9.3 Responsabilidades de los usuarios	90%
9	12.2 Protección contra códigos maliciosos	90%
10	12.3 Copias de respaldo	90%
11	12.5 Control de software operacional	90%
12	14.3 Datos de prueba	90%
13	17.1 Continuidad de seguridad de la información	90%
14	17.2 Redundancias	90%
15	14.2 Seguridad en los procesos de desarrollo y de soporte	86%
16	9.2 Gestión de acceso de usuarios	83%
17	6.1 Organización interna	82%
18	12.4 Registro y seguimiento	80%
19	14.1 Requisitos de seguridad de los sistemas de información	77%
20	18.2 Revisiones de seguridad de la información	77%
21	9.4 Control de acceso a sistemas y aplicaciones	74%

Orden	Objetivos de Control	Efectividad
22	18.1 Cumplimiento de requisitos legales y contractuales	74%
23	9.1 Requisitos del negocio para control de acceso	70%
24	12.1 Procedimientos operacionales y responsabilidades	70%
25	12.6 Gestión de la vulnerabilidad técnica	70%
26	15.2 Gestión de la prestación de servicios de proveedores	70%
27	15.1 Seguridad de la información en las relaciones con los proveedores	63%
28	8.3 Manejo de medios	63%
29	11.2 Equipos	61%
30	6.2 Dispositivos móviles y teletrabajo	53%
31	10.1 Controles criptográficos	50%
32	13.2 Transferencia de información	50%
33	11.1 Áreas seguras	43%
34	13.1 Gestión de la seguridad de las redes	37%
	CALIFICACION PROMEDIO	**76,65%**

Modelo de Madurez de la Capacidad (CMM - Capability Maturity Model)

CMM	Significado
L0	Inexistente
L1	Inicial / Ad-hoc
L2	Reproducible, pero intuitivo
L3	Proceso definido
L4	Gestionado y medible
L5	Optimizado

8. INDICADORES

NOMBRE DEL INDICADOR	FORUMULA
Seguridad Digital	(avance de seguridad digital / criterios de seguridad digital) *100
Grado de avance de gobierno digital	(cumplimiento actividades de gestión gobierno digital / actividades de gestión de gobierno digital definidas en mipg) *100

9. RECURSOS

Si se cuenta especificados lo recursos para llevar a cabo el programa
Todo aquello que vamos a necesitar durante el proceso:

- ✓ Personal
- ✓ Equipos biomédicos
- ✓ Insumos
- ✓ Medicamentos
- ✓ Dispositivos médicos

10. CRONOGRAMA

CICLOS	ETAPAS	N°.	ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	RESPONSABLES	PRODUCTO O RESULTADO ESPERADO
PLANIFICACIÓN	ETAPA 1. DEFINICIÓN DEL ALCANCE	1.1	Creación el comité de seguridad de la información	03/05/2021	16/05/2021	Representante Legal	Resolución de comité se seguridad de la información con funciones y responsabilidades
		1.2	diagnóstico y análisis del contexto y exigencias del negocio	19/05/2021	30/06/2021	Miembros del comité de seguridad de la información	Documento con las necesidades organizaciones y de procesos a fortalecer en la implementación del Sistema de Gestión de Seguridad de la información
		1.3	Definición de procesos del Negocio, críticos y claves para la implementación del proyecto SGSI	01/07/2021	09/07/2021	Miembros del comité de seguridad de la información	Procesos del negocio priorizados para la implementación
		1.4	Identificación los Stalholders del Proyecto	12/07/2021	16/07/2021	Miembros del comité de seguridad de la información	Identificar los involucrados en la implementación que generan un efecto sobre el proyecto y que deben ser tenidos en cuenta
		1.5	Definición de los objetivos estratégicos del proyecto SGSI	19/01/2021	20/08/2021	Miembros del comité de seguridad de la información	Metas esperadas en la implementación del sistema de gestión de seguridad de la información

CICLOS	ETAPAS	N°.	ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	RESPONSABLES	PRODUCTO O RESULTADO ESPERADO
		1.6	Articular y alinear los objetivos estratégicos del proyecto SGSI con los objetivos del plan de desarrollo	23/01/2021	31/06/2021	Miembros del comité de seguridad de la información y Planeación	Identificar como impactan los objetivos de la implementación dentro del microsistema de la organización
		1.7	Construir aprobar y socializar la Política de seguridad de la información y los acuerdos de confidencialidad	01/02/2021	31/12/2021	Miembros del comité de seguridad de la información, planeación y comunicaciones	Marco de directriz y gestión, intensión de construcción
		1.8	Definir los Frameworks para la implementación, evaluación y seguimiento del Proyecto SGSI	13/01/2021	28/03/2021	Miembros del comité de seguridad de la información	Contar con herramientas sistematizadas y lógicas para apoyar la implementación, evaluación y resultados
		1.9	Elaborar, aprobar y socializar el Plan de gestión de la seguridad de la información	01/02/2021	31/03/2021	Miembros del comité de seguridad de la información, Planeación y comunicaciones	Guía de implementación de Sistema de gestión de seguridad de la información
		1.10	Aprobar por la alta gerencia de los recursos financieros, personas, responsabilidades y tiempos para la	01/02/2021	31/12/2021	Representante legal	Contar con los recursos disponibles para la viabilidad financiera del Plan de gestión de Seguridad de la Información

CICLOS	ETAPAS	N°.	ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	RESPONSABLES	PRODUCTO O RESULTADO ESPERADO
			ejecución del proyecto SGSI				
IMPLEMENTACIÓN	ETAPA 2.- GESTIÓN DE ACTIVOS DE INFORMACIÓN	2.1	Construir y Actualizar y aprobar instrumentos de identificación de activos de información	15/07/2021	30/07/2021	Miembros del comité de seguridad de la información, Planeación y comunicaciones	Instrumentos de identificación de activos de información
		2.2	Socializar Instrumentos de activos de información	01/09/2021	10/12/2021	Miembros del comité de seguridad de la información, Planeación y comunicaciones y líder SGSI	Página Web, correos instituciones, drive institucional
		2.3	Realizar Mapeo e inventario de Activos de información por mapa de procesos y responsables	13/12/2021	31/01/2022	Jefes de Procesos y líder del SGSI	Inventario y matrices de Activos de información por procesos
		2.4	Realizar análisis de criticidad de la información por proceso CID (Confiabilidad, Integridad, Disponibilidad)	01/02/2022	30/03/2022	Comité de Seguridad, jefes de procesos y líder SGSI	Matrices y resultados de criticidad

CICLOS	ETAPAS	N°.	ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	RESPONSABLES	PRODUCTO O RESULTADO ESPERADO
		2.5	Establecer responsabilidades ley 1712 transparencia y del derecho de acceso a la información pública nacional	01/07/2021	30/03/2022	Planeación, comunicaciones y líder SGSI	Matrices de activos de información pública que administre la empresa
		2.6	Establece la responsabilidad ley 1581 de 2012 protección de datos personales	01/07/2021	30/03/2022	Planeación, comunicaciones y líder SGSI	Informe de identificación de datos personales
	ETAPA 3.- LEVANTAMIENTO E IDENTIFICACIÓN DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN	3.1	Construir, Actualizar y aprobar instrumentos de identificación de Riesgos de activos de información y reporte de incidentes de seguridad de la información	01/05/2022	30/05/2022	Comité de Seguridad, y líder SGSI	Instrumentos de identificación de riesgos de activos de información
		3.2	Socializar Instrumentos de identificación de riesgos de activos de información	01/06/2022	15/06/2022	Comité de Seguridad y líder SGSI y procesos	Página Web, correos instituciones, drive institucional

CICLOS	ETAPAS	N°.	ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	RESPONSABLES	PRODUCTO O RESULTADO ESPERADO
		3.3	Realizar Análisis de vulnerabilidades sobre 3 pilares PPT (Personas, Procesos y Tecnología)	16/06/2022	15/08/2022	Comité de Seguridad y líder SGSI y procesos	Matrices y resultados de vulnerabilidades
		3.4	Identificación de Brechas de Seguridad de la información PPT	16/06/2022	15/08/2022	Comité de Seguridad y líder SGSI y procesos	Matriz Análisis de brechas
		3.5	Identificación de Amenazas de seguridad de la información PPT	16/06/2022	15/08/2022	Comité de Seguridad y líder SGSI y procesos	Matriz Análisis de amenazas
		3.6	Análisis y evaluación de Riesgos Seguridad de la información vulnerabilidades, brechas y amenazas	16/08/2022	16/09/2022	Comité de Seguridad y líder SGSI y procesos	Matriz análisis de riesgos
		3.7	Tratamiento de Riesgos Seguridad de la Información	17/09/2022	16/12/2022	Comité de Seguridad y líder SGSI y procesos	Informe tratamiento a riesgos
		3.8	Informe de Seguimiento a Riesgos y revisión de seguridad de la información	15/12/2022	31/12/2022	Comité de Seguridad y líder SGSI y procesos	Informe de riesgos

CICLOS	ETAPAS	N°.	ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	RESPONSABLES	PRODUCTO O RESULTADO ESPERADO
	ETAPA 4.- IMPLEMENTACIÓN DE CONTROLES Y REQUISITOS DE LA SEGURIDAD DE LA INFORMACIÓN	4.1	Construir, Actualizar y aprobar instrumentos para elaborar procedimientos para administrar controles registros y Riesgos de seguridad de la información	01/01/2023	30/04/2023	Comité de Seguridad y líder SGSI, planeación y calidad	Instrumentos para elaborar procedimientos para administrar controles, registros y riesgos
		4.2	Socializar Instrumentos para elaborar procedimientos para la implementación y administración de controles y riesgos de seguridad de la información	01/05/2023	30/08/2023	Comité de Seguridad y líder SGSI, comunicaciones, calidad y planeación	Página Web, correos instituciones, drive institucional
		4.3	Elaborar, socializar e Implementar procedimientos para la gestión de controles, riesgos y registros de seguridad de la información	01/09/2023	31/12/2023	Comité de Seguridad, calidad, planeación, líder SGSI y procesos	Procedimientos para la administración y seguimiento a controles de seguridad de la información
VALIDACIÓN	ETAPA 5.- PRUEBA DE SEGURIDAD DE LA INFORMACIÓN	5.1	Elaborar, aprobar y socializar plan de auditoria al sistema de gestión de	01/01/2024	31/01/2024	Comité de Seguridad, planeación, líder SGSI	Plan de Auditorias al SGSI

CICLOS	ETAPAS	N°.	ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	RESPONSABLES	PRODUCTO O RESULTADO ESPERADO
			seguridad de la información				
		5.2	Implementar escenarios de pruebas de seguridad de la información	01/02/2024	30/04/2024	Líder SGSI Y jefe de TI	Escenario seguro de Pruebas
		5.3	Implementar Escaneo de Activos de Información con frameworks definidos en la etapa uno (1)	01/05/2024	30/08/2024	líder SGSI Y jefe de TI	Información escaneada de activos de la empresa para general Análisis
		5.4	Implementar evaluación independiente del sistema de gestión de seguridad de la información por empresa especializada	01/09/2024	31/10/2024	Comité de Seguridad de la información, líder SGSI, jefe TI y Evaluador independiente	Evaluar independiente del estado seguridad de la información de la empresa
		5.5	Implementar buenas prácticas de Hacking Ético e ingeniería Social al sistema de gestión de seguridad	01/11/2024	31/12/2024	Comité de Seguridad de la información, líder SGSI y jefe TI	Evaluación interna del estado de seguridad la información de la empresa

CICLOS	ETAPAS	N°.	ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	RESPONSABLES	PRODUCTO O RESULTADO ESPERADO
	ETAPA 6.- CAPACITACION Y SENSIBILIZACION	6.1	Elaborar, aprobar y socializar Plan de sensibilización y capacitación en Seguridad y Privacidad de la información	01/01/2026	31/01/2026	Comité de Seguridad de la información, líder SGSI, talento humano y comunicaciones	Documento Plan de Concienciación en Seguridad y Privacidad
		6.2	implementar Plan de sensibilización y capacitación del Sistema de Gestión de Seguridad de la información	01/02/2026	30/03/2026	Comité de Seguridad de la información, líder SGSI, talento humano y comunicaciones	Informe de ejecución Plan de Concienciación en Seguridad y Privacidad
		6.3	Análisis de resultados del Plan de sensibilización y capacitación del Sistema de Gestión de Seguridad de la información	01/04/2026	30/04/2026	Comité de Seguridad de la información, líder SGSI, talento humano y comunicaciones	Informe de resultados Plan de Concienciación en Seguridad y Privacidad
REVISIÓN Y ACTUALIZACIÓN	ETAPA 7.- MANTENIMIENTO Y ACTUALIZACION	7.1	Elaborar, aprobar y socializar programa para la evaluación y seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información	01/05/2026	30/05/2026	Comité de Seguridad de la información, líder SGSI y planeación	Programa de auditoria

CICLOS	ETAPAS	N°.	ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	RESPONSABLES	PRODUCTO O RESULTADO ESPERADO
		7.2	Evaluar Acciones Correctivas y Acciones de Mejora del Sistema de Gestión de Seguridad de la Información	01/06/2026	30/06/2026	Comité de Seguridad de la información, líder SGSI y planeación	Actas de reunión / correos electrónicos
		7.3	Revisar y gestionar e intervenir resultados de las Auditorías al Sistema de Gestión de Seguridad de la Información	01/07/2026	30/07/2026	Comité de Seguridad de la información, líder SGSI y planeación	Actas de participación en el Plan de auditoria
		7.4	Revisar, gestionar e intervenir los reportes de Incidentes de Seguridad de la Información	01/08/2026	30/09/2026	Comité de Seguridad de la información, líder SGSI y planeación	Aplicativo para Incidentes de Seguridad de la información.
		7.5	Evaluar los resultados y tendencias de los indicadores trazadores del Sistema de Gestión de Seguridad de la Información	01/10/2026	31/12/2026	Comité de Seguridad de la información, líder SGSI y planeación	Evidencia para evaluación de los indicadores

10.1. CARGA DE LA IMPLEMENTACIÓN POR ETAPAS, ACTIVIDADES Y TIEMPO

ORDEN	ETAPAS	NO. DE ACTIVIDADES
1	Definición del alcance del proyecto	10
2	Gestión de inventario de activos de información	6
3	Levantamiento e identificación de riesgos de los activos de información	8
4	Implementación de controles y requisitos de la seguridad de la información	3
5	Pruebas de seguridad de la información	5
6	Capacitación y sensibilización	3
7	Mantenimiento y actualización	5
Totales		**40**

La Implementación y mantenimiento del Sistema de Gestión de la Información (SGSI) en el Hospital Mario Correa Rengifo ESe, genera como resultado la ejecución para las 7 etapas con 40 actividades, en un tiempo promedio de 3 a 6 años, como s e revela en la tabla de la carga de la implementación. Aquí, se identifica que la etapa inicial de planeación del proyecto son 10 actividades superiores a las siguientes, debido a que esta es la etapa más importante para garantizar la ejecución del proyecto.

De igual manera, es importante resaltar que la implementación de este plan plantea grandes desafíos al interior del Hospital, debido a que no se limita a solo implementar un proyecto, sino, que tiene una ejecución proyectada a 3 a 6 años de duración. Por lo que se requiere del compromiso de la alta gerencia y todos los procesos, de la asignación de los recursos requeridos en cada etapa, así como la designación de un patrocinador, un líder del proyecto y un oficial de seguridad, pero, sobre todo, en la concentración de una apuesta por trabajar en la transformación de la cultura organizacional de la empresa, para la adopción de este proceso estricto de gestión de la información.

11. ANEXOS

Matriz de evaluación de controles norma técnico Icontec ISO27002.

12. BIBLIOGRAFIA

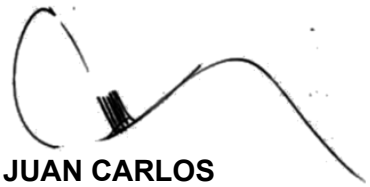
- Compendio de Seguridad de la Información segunda edición Icontec Internacional agosto de 2015

- guía para la administración del riesgo y el diseño de controles en entidades Públicas, Riesgo de gestión, Corrupción y Seguridad Digital Versión 4, Dirección de gestión y Desempeño Institucional Función Pública octubre de 2018

13. CONTROL DE REGISTROS

VERSIÓN	FECHA	MODIFICACIONES O CAMBIOS
1	Enero 2022	Cambio en el formato institucional
2	Enero 2023	actualización del Plan
3	Enero 2024	actualización del Plan
4	Enero 2025	actualización del Plan
5	Enero 2026	actualización del Plan

14. ELABORÓ, REVISÓ Y APROBÓ

Elaborado por:	Revisado por:	Aprobado por:
		
MARIO GONZÁLEZ HERNÁNDEZ Jefe De Gestión De Sistemas De Información	**AEJANDRA NAVARRETE S.** Jefe Oficina asesora de Planeación	**JUAN CARLOS CORRALES BARONA** Gerente General