PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023 - 2025

Revisado: Subgerente Administrativo y Financiero	Firma:	Fecha: 19 de abril de 2023
Aprobado: Gerente	Firma:	Fecha: 19 de abril de 2023

CONTENIDO

INTRODUCCIÓN

La ESE Hospital San Jerónimo de Montería dando cumplimiento del marco legal Colombiano construye el presente Plan de Seguridad y Privacidad de la Información, documento relacionado con la protección, seguridad y confidencialidad de la información, amparado específicamente en el decreto 612 del 2018; esto con el fin de contar con una guía que permita proteger los activos de información siendo consciente de la vital importancia de la información (Datos) para el funcionamiento de la Entidad.

1. OBJETIVOS DEL PLAN

Definir el conjunto de acciones necesarias para Diseñar, desarrollar e implementar de manera integral, la gestión de los riesgos de seguridad y privacidad de la información, con el objetivo de proteger los activos de información de la institución y garantizar la continuidad del funcionamiento de la plataforma informática.

1.1 Objetivos específicos

- Crear mecanismos de aseguramiento digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información en la E.S.E Hospital San Jerónimo de Montería.
- Brindar los medios tanto físicos como digitales necesarias que permitan asegurar el uso eficiente y seguro de los recursos tecnológicos de información y comunicación.
- Asegurar e incentivar en el personal asistencial el usos eficiente y seguro de aquellos equipos biomédicos que almacenen información sensible de los pacientes atendidos en la E.S.E Hospital San Jerónimo de Montería.
- Garantizar la disponibilidad de la información para la eficiente toma de decisiones.
- Disminuir las probabilidades de ocurrencia e impacto de incidentes de seguridad y privacidad de la información.
- Dar cumplimiento a los requisitos normativos en cuanto a seguridad y privacidad de la información.
- Asegurar la continuidad de funcionamiento de las diferentes bases de datos inherentes a los softwares que se utilicen en la institución.
- Incentivar la cultura de la seguridad de la información.

2. ALCANCE

Aplica a todos los niveles asistenciales y administrativos de la ESE Hospital San Jerónimo de Montería, sus funcionarios, contratistas, proveedores, usuarios, docentes, estudiantes que realicen prácticas, pasantías o trabajos de grado, bajo el marco de un contrato y/o convenio académico y cooperantes, adicionalmente todas aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la ESE compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, que accedan ya sea interna, remotamente o vía internet a cualquier tipo de información, independientemente de su ubicación. Así mismo, está lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por la ESE Hospital San Jerónimo de Montería, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

3. DEFINICIONES

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- Antivirus: Software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
- Ataques Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.
- Contraseña: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados.
- Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000).
- Encriptación: La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos
- Firewall: Es una aplicación de seguridad física y/o lógica diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.
- Malware: Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras.
- Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Vulnerabilidad: Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

4. DOCUMENTO DE REFERENCIA

- *Decreto 1078 de 2015 – MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.*

- *NTC / ISO 27001:2013 - ICONTEC Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.*

- *NTC/ISO 27002:2013- ICONTEC Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.*

- *Ley 1266 de 2008 "Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".*

- *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.*

- *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.*

5. METODOLOGIA

Para la realización del Plan de Seguridad y Privacidad de la Información se definieron una serie de fases, estas se detallan a continuación:

5.1. Identificación Del Contexto

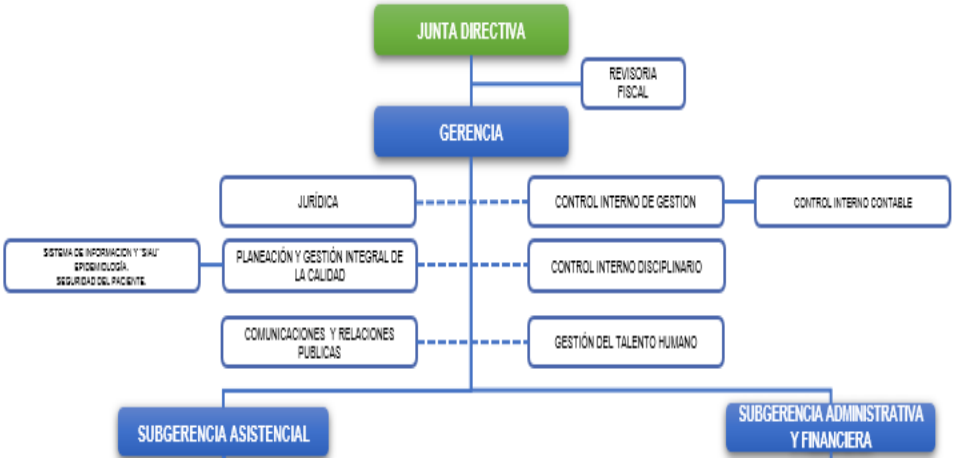
En esta fase se hace un reconocimiento de los principales aspectos, características, procesos y arquitectura funcional de la institución, para determinar un eficiente funcionamiento del plan propuesto en el presente documento.

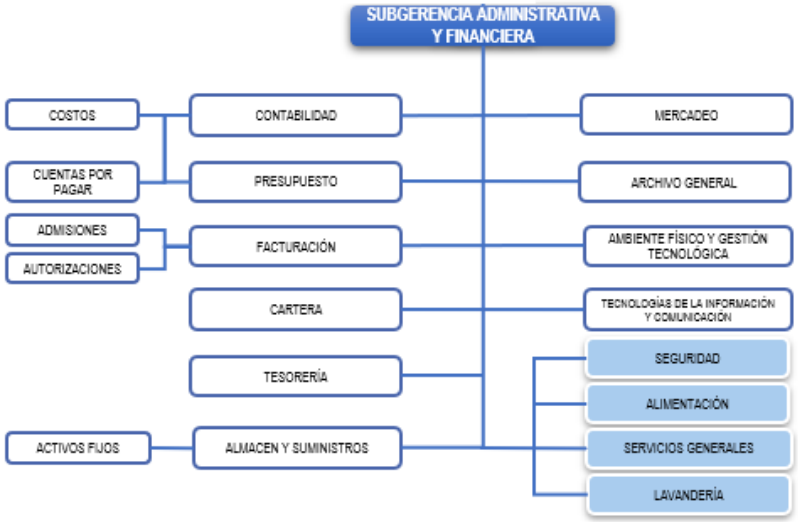
Misión.
Somos una empresa social del estado de mediana y alta complejidad que presta servicios de salud a la población del departamento de Córdoba y su área de influencia, con un equipo tecnológico y humano altamente calificado, con enfoque científico, universitario e investigativo, garantizando una atención integral, con calidad y trato humanizado, en armonía con el medio ambiente.

Visión.

Seremos en el 2025 la mejor Empresa Social del Estado prestadora de servicios de salud, con altos estándares de calidad proyectándonos a la acreditación.

Organigrama





Dentro de la estructura funcional de la Subdirección Administrativa y Financiera, se encuentra la oficina de Tecnologías de la Información y comunicaciones, quién es la responsable de la administración de la Plataforma informática de la ESE.

Mapa de procesos.

Mapa de E.S.E. Hospital San Jerónimo de Montería

6. POLITICAS

Se toma la decisión por parte de la E.S.E Hospital San Jerónimo de Montería de diseñar, implementar y operar un Sistema de Gestión de Seguridad de la Información, apuntando a la mejora continua de los procesos, soportado bajo los lineamientos normativos con el fin de salvaguardar uno de los activos más importantes – La Información -

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- La ESE Hospital San Jerónimo de Montería protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.
- La ESE Hospital San Jerónimo de Montería protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La ESE Hospital San Jerónimo de Montería protegerá las instalaciones de procesamiento y la infraestructura de redes de voz y datos que soporta sus procesos más críticos.
- La ESE Hospital San Jerónimo de Montería protegerá su información de las amenazas originadas por parte del personal.

- La ESE Hospital San Jerónimo de Montería implementará control de acceso a la información, sistemas y recursos de red.
- La ESE Hospital San Jerónimo de Montería garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La ESE Hospital San Jerónimo de Montería garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La ESE Hospital San Jerónimo de Montería garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La ESE Hospital San Jerónimo de Montería garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6.1. Activos De Información

Todos los jefes de los servicios, en el proceso de creación de un nuevo documento, son los responsables de realizar el requerimiento a la oficina de calidad, quién se encargará de realizar la respectiva revisión y codificación; posteriormente esta última oficina informará a oficina de Tecnologías de la Información y comunicaciones la creación del nuevo documento para ser incluido en el inventario de activos de información.

La oficina de Tecnologías de la Información y comunicaciones es la responsable del control del inventario de los activos de información a nivel de hardware, redes y comunicaciones; para lo cual debe realizar mínimo una vez al año una revisión por cada unidad funcional de sus elementos de informática asignados.

En las políticas para el uso de los servicios de Tecnologías de la Información y Comunicación de la E.S.E – Se definen las normas para el uso de equipos de cómputo personales que no son propiedad de la ESE, las cuáles se detallan a continuación:

a) Para el ingreso de equipos de informática a la institución es obligatorio consultar su existencia en la lista de equipos autorizados, la cual será suministrada semanalmente por La oficina de Tecnologías de la Información y comunicaciones, y para su inclusión en ella se debe entregar una carta dirigida al mismo, especificando las características técnicas del equipo, el funcionario responsable y el área al cual pertenece este último.

b) El hospital no se hace responsable en caso de pérdida o robo del computador en el interior de sus instalaciones.

c) El hospital se reserva el derecho de revisar el software instalado en el computador como medida de protección de su plataforma informática.

d) El software instalado en el computador es responsabilidad de su propietario, por lo tanto la E.S.E. recomienda el cumplimiento de las normas referentes al respeto de la propiedad intelectual del software.

e) El software institucional no será instalado en computadores que no sean propiedad de la E.S.E.

f) Los servicios técnicos requeridos por el computador serán responsabilidad de su propietario.

En las políticas para el uso de los servicios de Tecnologías de la Información y Comunicación de la E.S.E – Se definen las normas para el uso de equipos de informática institucionales, las cuáles se detallan a continuación:

a) El uso de los equipos de cómputo de la institución es exclusivo para el desarrollo de las actividades laborales propias de cada funcionario relacionadas con los procesos institucionales, y su utilización solo es permitida por funcionarios activos de la ESE, y personal que temporalmente este realizando alguna actividad relacionada con la ESE, bajo supervisión permanente de un funcionario activo.

b) No es permitida la instalación y desinstalación de software en el computador por cualquier persona diferente a los funcionarios de La oficina de Tecnologías de la Información y comunicaciones.

c) Para el caso de computadores portátiles, el funcionario responsable del equipo está autorizado para la movilización de este, a los sitios tanto internos como externos que lo requiera, asumiendo las responsabilidades relacionadas a la salida del activo. la salida del activo solo podrá ser autorizados por la oficina de Tecnologías de la Información y comunicaciones.

En lo referente a la información generada por la plataforma informática de la ESE, En las políticas para el uso de los servicios de Tecnologías de la Información y Comunicación de la E.S.E, determina las normas para su manejo, las cuáles se detallan a continuación:

a) La información institucional no puede ser utilizada para fines diferentes a los requeridos en los procesos de la ESE, y para su uso externo se debe contar con la previa autorización de la Gerencia.

b) La información clínica de un paciente es estrictamente confidencial por lo tanto solo tiene acceso el personal debidamente autorizado.

d) El acceso a la Dinámica Gerencial (Software de gestión Hospitalaria – Integrado por módulos asistenciales y administrativos) y demás software de uso institucional está basado en los roles de usuario y/o permisos de acceso asignados bajo previa autorización del jefe de área a la oficina de Tecnologías de la Información y comunicaciones, quien es la encargada de la administración de los diferentes softwares de usos institucional.

e) En el caso de que la información sea de dominio público y de interés general para el funcionamiento de la ESE, el usuario generador de esta debe asegurar los mecanismos para su disponibilidad, utilizando los servicios que la oficina de Tecnologías de la Información y comunicaciones le brinde.

f) Los usuarios son responsables por la información local almacenada en sus equipos de cómputo, y por la definición de los mecanismos de protección y confidencialidad. Los respaldo y recuperación en caso de incidentes será la oficina de Tecnologías de la Información y comunicaciones la encargada.

g) La oficina de Tecnologías de la Información y comunicaciones es el responsable por la información institucional almacenada en sus servidores, y por la definición de los mecanismos de protección, confidencialidad, respaldo y recuperación en caso de incidentes, mediante la implementación de su Plan de Recuperación de Desastres.

h) En el caso de ser requerida la eliminación de información institucional este proceso debe seguir las indicaciones establecidas por La oficina de Tecnologías de la Información y comunicaciones.

6.2. Seguridad De La Información En El Talento Humano

Todos los funcionarios de la ESE Hospital San Jerónimo de Montería, independiente del tipo de vinculación laboral o contractual, o de los procesos al que pertenezca y del nivel de funciones o actividades que desempeñe deben contar con un perfil de uso de los recursos de información, de acuerdo la política para la Definición de políticas y niveles de acceso a la plataforma Informática.

La responsabilidad de custodia de cualquier documento o archivo generado dentro de la entidad, usado o producido por algún funcionario y/o contratista que se retira, recae en los subdirectores Científico y Administrativo para el personal de planta y en el supervisor del contrato para el resto de personal, la oficina Tecnologías de la Información y comunicaciones es la encargada de la realización de las copias de seguridad para el caso de información electrónica que repose en los computadores; aclarando que el proceso de cadena de custodia de la información debe hacer parte integral de un procedimiento de terminación de la relación contractual o de cambio de cargo.

6.3. Seguridad Física Y Del Entorno

Los servidores que contengan información institucional deben estar ubicados en el Data center principal ubicado en la oficina de Tecnologías de la Información y comunicaciones: protegidos con seguridad física, sistemas eléctricos regulados, respaldados por fuentes de potencia ininterrumpida (UPS) y con circuitos alternos de entrada de corriente.

Las estaciones de trabajo que contengan información institucional deben estar en un ambiente seguro y protegido por lo menos con Cuentas de administrador solamente uso exclusivo para la oficina de Tecnologías de la Información y comunicaciones, antivirus, sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Los documentos físicos con conservados en el archivo central de la institución, de acuerdo con los lineamientos definidos en el PINAR.

6.4. Reporte Y Revisión De Incidentes De Seguridad

El personal vinculado a la ESE Hospital San Jerónimo de Montería debe realizar el reporte de todas las presuntas violaciones de seguridad detectadas, mediante correo electrónico al correo coord.sistemas@esesanjeronimo.gov.co, dirigido a la Coordinación de la oficina de Tecnologías de la información y comunicaciones.
En el caso de no tener acceso a correos electrónicos se debe realizar el reporte inmediato al supervisor del proceso, quién lo realizará a su notificación al Coordinador de la oficina de Tecnologías de la información y comunicaciones.

6.5. Protección Contra Malware Y Hacking

Todos los equipos de informática de la ESE deben estar protegidos de amenazas de malware, instalación de software no autorizado y hackeo mediante un conjunto de acciones que se describen a continuación y cuyo objetivo es el de disminuir la probabilidad de un evento que genere daños en la plataforma informática.

a) Cada equipo está bajo la administración de un software de dominio y cada usuario que accede a los diferentes equipos de cómputo se registra en el dominio asignándole un usuario y contraseña de acceso, así se permite administrar por usuario los diferentes equipos brindado seguridad a la información que reposa en cada usuario. El dominio permite configurarán dos tipos de usuario administrador y usuario normal. la cuenta de perfil administrador es de exclusivo manejo de la oficina de Tecnologías de la información y comunicaciones, el usuario normal es para el ingreso de los funcionarios que usan el equipo.
b) Cada equipo contará con software antivirus, el cual será actualizado en cada mantenimiento preventivo que se realiza al mismo, buscando un máximo de 6 meses para cada actualización.

6.6. Copias De Seguridad

Es responsabilidad de la oficina de tecnologías de la Información y comunicación realizar la copia de seguridad de la información en cada equipo propiedad de la E.S.E, Este proceso se realiza con cada mantenimiento preventivo y/o correctiva o a solicitud exclusiva del jefe de área y/o supervisor del contratista. Las copias de seguridad reposaran en la oficina de tecnologías de la Información y comunicación, en Discos Duros Externos destinados para tal fin.

Para las copias de seguridad de los correos electrónicos, se debe notificar con previa antelación a la oficina de tecnologías de la información y comunicación para que sea los funcionarios de esta dependencia quien realicen la respectiva copia y se resguarde en el equipo de cómputo del funcionario que tiene asignada dicha cuenta de correo institucional.

Las copias de seguridad de las bases de datos y documentos almacenados en los servidores ubicados en el Datacenter principal de la institución, son realizadas por la oficina de tecnologías de la Información y comunicación, de acuerdo al procedimiento ya definido.

6.7. Intercambio De Información Con Entidades Externas

Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por la Gerencia previamente por la gerencia, quién determinará las personas responsables del manejo y custodia dicha información. Todo requerimiento debe haber sido previamente radicado por Ventanilla Única, cumpliendo los procedimientos institucionales establecidos para la gestión documental. La información entregada será de acuerdo con la clasificación de confidencialidad establecida en el inventario de activos de información.

6.8. Servicio De Comunicación De Datos Internet

Este servicio será administrado por la oficina de tecnologías de información y comunicación, el acceso de los usuarios a internet estará definido de acuerdo con el tipo de usuario y privilegios de acceso otorgados.

Se debe garantizar una conexión mínima para los procesos vitales, por lo tanto, se debe contar con dos proveedores diferentes que permitan realizar un respaldo de cada uno por fallo.

En las políticas para el uso de los servicios de Tecnologías de la Información y Comunicación, determina las normas para su uso, las cuáles se detallan a continuación:

a) No se permite la descarga de videos o música, el acceso a sitios cuyo contenido involucre compras, pornografía, canales de televisión o radio en línea, actos delictivos y aquellos considerados por la oficina de tecnologías de la información y comunicación, como potencialmente dañinos para la seguridad informática de la ESE.

b) Los servicios de correo no pueden ser utilizados como soporte al desarrollo de actividades ilegales, ni pueden ser utilizados como herramientas de publicidad institucional sin la debida autorización de la gerencia.

c) En el caso de utilización de los servicios de correo para el intercambio de información con otras empresas, se debe colocar el nombre completo del funcionario y su cargo en los datos del remitente.

Para la red de datos institucional se cuenta con un firewall que tiene un Sistema de reportes mensuales que nos permite identificar las páginas a las que acceden los usuarios, desde que computador se excede el consumo del ancho del canal y adicionalmente el firewall nos protege de las amenazas externas. Actualmente es equipos hace parte de los servicios prestados por el proveedor del canal principal de internet y su administración es compartida.

7. PLAN DE IMPLEMENTACIÓN

La ESE Hospital San Jerónimo de Montería viene aumentando la automatización de sus procesos y su oferta de servicios electrónicos a sus usuarios mediante el crecimiento de su plataforma informática, mediante adquisición de aplicativos externos, tanto en ambiente cliente servidor como en la web.

Estos aplicativos pueden estar expuestos a amenazas, como malware o hacking, entre otros, pero también a riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde cualquier origen o los causados accidentalmente por fallas técnicas y desastres naturales, por lo que se considera de vital importancia continuar con la implementación del modelo de seguridad y privacidad de la información (MSPI), debido a que este sistema ayuda a la entidad a gestionar de manera eficaz la seguridad de la información, con el objetivo de definir y aplicar medidas, procesos y procedimientos para el apropiado control, tratamiento y mejora continua.

A continuación, se detallan las fases y sus correspondientes actividades que se van a desarrollar teniendo en cuenta lo definido descrito en los lineamientos del documento “Modelo de Seguridad y Privacidad de la Información (MSPI)” del MinTIC alineados con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI (MRAE), la Estrategia de Gobierno en Línea (GEL) y la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013.

7.1. Fases Implementación MSPI

FASE I: ANÁLISIS DE BRECHA

Elaborar el análisis GAP (análisis de brecha) frente a la norma ISO 27000 y el Modelo de seguridad y privacidad de la información MSPI de la ESE Hospital San Jerónimo de Montería.

FASE II: ESTABLECIMIENTO DEL SGSI

Diseñar políticas y procedimientos de seguridad conforme la estructura propuesta por la norma ISO 27000 alineados al Sistema Integrado de Gestión de la Entidad.

Determinar la estructura y ubicación en el organigrama institucional de la función de seguridad de la información ajustada al contexto interno de la ESE Hospital San Jerónimo de Montería y teniendo en cuenta sus necesidades.

Definir y documentar formalmente el proceso de gestión de incidentes del SGSI

Crear, definir e implementar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información Se deberá tener como referencia la norma ISO 27004:2016.

FASE III: ANÁLISIS DE RIESGOS

Actualizar los activos de información de la institución y ajustar su clasificación de acuerdo con los requerimientos de confidencialidad definidos y establecer los requerimientos exigidos por la norma ISO27001:2013 y normas relacionadas ISO 27002 e ISO 27005.

Actualizar el plan de gestión de riesgos de la ESE basados en los lineamientos establecidos en la norma ISO 31000 e ISO 27005:2008, y en la actualización de los activos de información.

FASE IV: PRUEBAS DE SEGURIDAD

Desarrollo de pruebas para determinar las vulnerabilidades que existen dentro de la configuración física y lógica de la plataforma informática de la entidad.

Realización de pruebas de Ingeniería social buscando evidenciar las vulnerabilidades que existen dentro de la ESE, mediante la obtención de información de personas y procesos claves del negocio mediante acceso físico a la misma o con información de acceso facilitada por el personal de la organización, el cual ha sido objeto de engaño.

Construir el Plan Estratégico de Seguridad de la Información PESI.

FASE V: SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN

Establecer las acciones necesarias para implementar el programa de capacitación requerido por la organización en lo referente a seguridad de la información tomando como insumo los resultados de las pruebas de ingeniería social y a lo definido en el Plan Estratégico de Seguridad de la Información PESI

FASE VI: AUDITORIA INTERNA

Diseñar y desarrollar las actividades preparatorias que busquen orientar a la organización para afrontar el proceso de auditoría por parte de un ente certificador el cual comprenderá efectuar una revisión y cumplimiento del SGSI frente a los requerimientos exigidos para la certificación ISO 27001:2013.

7.1. CRONOGRAMA IMPLEMENTACION MSPI

Fases	2023	2024	2025
Fase 1			
Fase 2			
Fase 3			
Fase 4			
Fase 5			
Fase 6			

CUADRO DE REVISIONES

Versión	***Elaboró***	***Revisó***	***Aprobó***
01	Profesional Universitario Sistemas de Información y comunicaciones	Planeación y Gestión de Calidad	Gerente

CONTROL DE COPIAS

Versión	***Tipo de Copia***	***Área o Sección***	***Fecha Elaboración***	***Fecha Revisión***
01	Controlada	Tecnología de la Información y Comunicaciones	Abril 2023	Abril 2024

Versión	***Descripción del Cambio***
01	Elaboración del documento PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
02	
03	
04	