PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Versión 1.1 - 2025

ESE HOSPITAL REGIONAL MANUELA BELTRAN SOCORRO

Documento elaborado por:

Ing Roney Suárez-Coordinador DATIC

CONTENIDO

INTRODUCCION

La ESE Hospital Regional Manuela Beltrán Socorro en cumplimiento del marco legal Colombiano relacionado con la protección, seguridad y confidencialidad de la información, en especial el decreto 612 del 2018; además de la iniciativa propia de la empresa de diseñar un marco de referencia para proteger sus activos de información consciente de la vital importancia de los mismos para su funcionamiento, construye el presente Plan de Seguridad y Privacidad de la Información enfocado exclusivamente para su plataforma informática.

1. OBJETIVO 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

- Disminuir la probabilidad de ocurrencia e impacto de los incidentes de Seguridad y Privacidad de la Información de forma efectiva.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, y privacidad de la información de la ESE Hospital Regional Manuela Beltrán Socorro.
- Asegurar y hacer uso eficiente y seguro de los recursos de Tecnologías de Información y Comunicaciones, así como aquellos equipos biomédicos que almacena información referente a los servicios prestados, con el fin de garantizar la continuidad de la prestación de los servicios.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información, Seguridad Digital y protección de la información personal.
- Minimizar el riesgo de vulnerabilidad de la información en el desarrollo de los procesos.
- Mantener la confianza de sus clientes internos y externos.
- Asegurar la continuidad de funcionamiento de la plataforma informática
- Cumplir con la legislación nacional e institucional sobre seguridad de la información
- Garantizar la disponibilidad de la información para la eficiente toma de decisiones.
- Fortalecer la cultura de la seguridad de la información a nivel de clientes internos y externos.
- Proteger los activos tecnológicos y apoyar su desarrollo.

2. ALCANCE

Aplica a todos los niveles asistenciales y administrativos de la ESE Hospital Regional Manuela Beltrán Socorro, 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 y EAPB, que accedan ya sea interna, remotamente o vía internet a cualquier tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por la ESE Hospital Regional Manuela Beltrán Socorro en formato electrónico.

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 auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (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)

Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000) • Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 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.

Plan de tratamiento de Gestión de Riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación

Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

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).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de detección de intrusos: Es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no

autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red.

Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.

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.

4. DOCUMENTOS DE REFERENCIA

Decreto 338 de 2022 – MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
"Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"

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 1978 de 2019
"Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones."

Resolución 232 del 2015 – ESE Hospital Regional Manuela Beltrán Socorro
Por medio de la cual se adopta ley de protección de datos para usuarios de la ESE Hospital Regional Manuela Beltrán Socorro.

Resolución 355 del 2016 – ESE Hospital Regional Manuela Beltrán Socorro
Por medio de la cual se adopta la Política de Comunicaciones de la ESE Hospital Regional Manuela Beltrán Socorro.

Resolución 095 del 2018 – ESE Hospital Regional Manuela Beltrán Socorro
Por medio del cual se aprueba y expide la política para la Definición de políticas y niveles de acceso a la plataforma Informática de la ESE Hospital Regional Manuela Beltrán Socorro.

Resolución 045 del 2019 – ESE Hospital Regional Manuela Beltrán Socorro
Por medio del cual se aprueba el plan de gestión de riesgos plataforma informática de la ESE Hospital Regional Manuela Beltrán Socorro.

Resolución 166 del 2020 – ESE Hospital Regional Manuela Beltrán Socorro
Por medio del cual se establece la política de seguridad y privacidad de la información en la E.S.E Hospital Regional Manuela Beltrán Socorro.

Acuerdo 028 del 2009 – ESE Hospital Regional Manuela Beltrán Socorro
Por medio del cual se establece el Reglamento sobre las políticas para el uso de los servicios de Tecnologías de la Información y Comunicación ofrecidos por la E.S.E Hospital Regional Manuela Beltrán Socorro.

Acuerdo 007 del 2015 – ESE Hospital Regional Manuela Beltrán Socorro
Por medio del cual se realizan modificaciones al acuerdo 028 del 2009.

Procedimiento GIC-PC-39 – ESE Hospital Regional Manuela Beltrán Socorro
Gestión de Incidentes de Seguridad de la Información

5. METODOLOGÍA

La metodología usada para el diseño y desarrollo de este Plan de Seguridad y Privacidad de la Información, fue llevar a cabo las siguientes fases que 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.

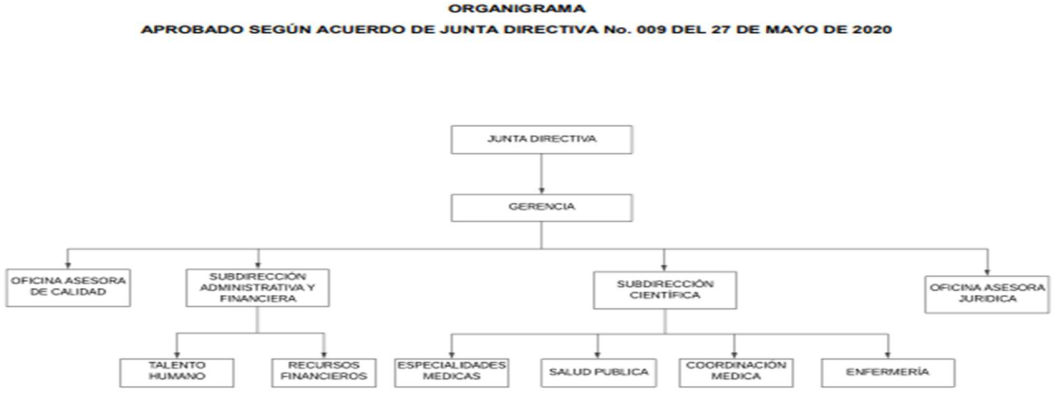
Misión

La ESE Hospital Manuela Beltrán del Socorro Referente para el Sur de Santander, presta servicios de salud de alta calidad, apoyados en un talento humano idóneo, vocación académica, infraestructura física y tecnológica; que garantiza la atención en la baja, media y alta complejidad para nuestros usuarios, sus familias y la comunidad en general, orientados hacía una atención Humanizada incluyente y participativa.

Visión

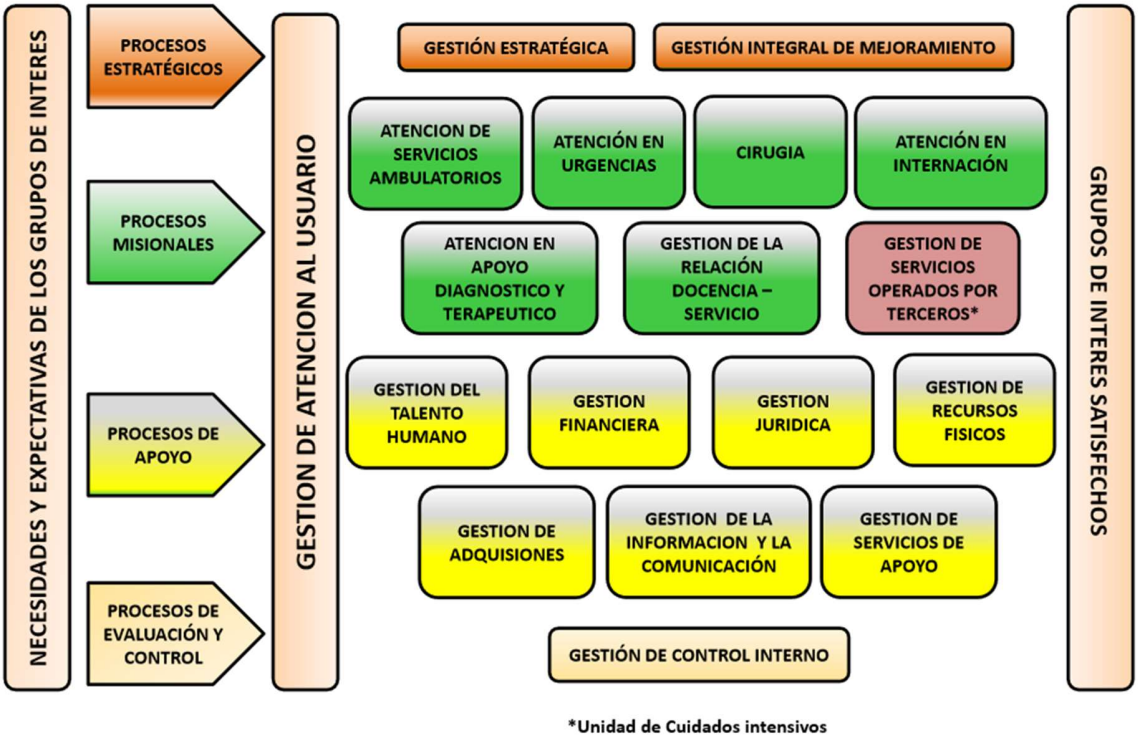
La ESE Hospital Regional Manuela Beltrán para el año 2027, será reconocida como el Centro de Referencia del sur de Santander en la prestación de los servicios de salud de mediana y alta complejidad, con un compromiso ético y practicas sostenibles, que impacten de forma Efectiva la Salud de la población de la Región con la implementación de estándares superiores de Calidad para lograr experiencias positivas en nuestros usuarios, colaboradores y demás actores del sistema de salud.

Organigrama



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

Mapa de Procesos



*Unidad de Cuidados intensivos

Identidad Organizacional

Calidad Y Seguridad: Priorizaremos la seguridad del paciente evitando errores médicos, garantizando una atención con calidad en la promoción de prácticas seguras en la higiene y la esterilización de los ambientes hospitalarios.

Empatía: Estaremos comprometidos en reconocer las necesidades del usuario y su familia, escucharemos sus preocupaciones y garantizaremos una explicación clara y entendible en los procedimientos de manera comprensible vinculando de forma activa la participación del usuario en la toma de decisiones.

Ética e Integridad: Actuaremos con honestidad y transparencia en la información al usuario sobre costos, riesgos y alternativas de tratamiento; Garantizando el acceso y oportunidad a la atención medica sin discriminación y con igualdad de oportunidades.

Trabajo en Equipo: Trabajaremos en conjunto para brindar una atención integral y coordinada, que permitirá la comunicación abierta y el respeto mutuo entre todos los colaboradores de la ESE.

Sostenibilidad: Generaremos una conciencia en los impactos ambientales y sociales de manera responsable, eficiente y comprometida en la prestación de los servicios que ofrece la ESE en la provincia Comunera y Sur de Santander.

5.2. SITUACION ACTUAL

La institución actualmente cuenta con un buen grupo de documentos institucionales que sirven como marco de referencia para la garantizar la privacidad y seguridad de su información, los cuáles fueron relacionados en el capítulo 5 de este mismo documento.

6. POLITICAS

En el Artículo 6 de la resolución 166 del 2020, ya se tienen definidas las políticas básicas para la seguridad y privacidad de la información, las cuáles se mencionan a continuación:

"La E.S.E. Hospital Regional Manuela Beltrán ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- 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 Regional Manuela Beltrán protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- La ESE Hospital Regional Manuela Beltrán 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 Regional Manuela Beltrán protegerá su información de las amenazas originadas por parte del personal.
- La ESE Hospital Regional Manuela Beltrán protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La ESE Hospital Regional Manuela Beltrán controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La ESE Hospital Regional Manuela Beltrán implementará control de acceso a la información, sistemas y recursos de red.
- La ESE Hospital Regional Manuela Beltrán garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La ESE Hospital Regional Manuela Beltrán 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 Regional Manuela Beltrán 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 Regional Manuela Beltrán Socorro 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 DATIC por medio de gestión documental, la creación del nuevo documento para ser incluido en el inventario de activos de información.

La oficina de inventarios 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 el artículo 6 del Acuerdo 028 del 2009 – Se definen las normas para el uso de equipos 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 el DATIC, 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, el hospital 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 del hospital.
f. Los servicios técnicos requeridos por el computador serán responsabilidad de su propietario.

En el artículo 7 del Acuerdo 028 del 2009 – 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 informática 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 del DATIC.

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 determinadas en ítem b del artículo 4.

En lo referente a la información generada por la plataforma informática de la ESE, el Artículo 9, del Acuerdo 028 del 2009, 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 a ella solo tiene el personal debidamente autorizado.
c. El acceso a la información institucional está basado en los perfiles de cuenta de cada usuario de acuerdo al software aplicativo que se use.
d. 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 de los servidores de almacenamiento.
e. Los usuarios son responsables por la información local almacenada en sus equipos de trabajo, y por la definición de los mecanismos de protección, confidencialidad, respaldo y recuperación en caso de incidentes.
f. El DATIC 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.
g. En el caso de ser requerida la eliminación de información institucional este proceso debe seguir las indicaciones establecidas por el DATIC.

6.2. SEGURIDAD DE LA INFORMACIÓN EN EL TALENTO HUMANO

Todos los funcionarios de la ESE Hospital Regional Manuela Beltrán Socorro, 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 a la resolución institucional 095 del 2018 (no se incluye el personal de servicios generales).

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 DATIC 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.

La asignación de los perfiles de los usuarios estará determinada por la Resolución institucional 095 del 2018. La creación de los usuarios en la plataforma se encuentra definido en el procedimiento PC11038.

6.3. SEGURIDAD FÍSICA Y DEL ENTORNO

Los servidores que contengan información institucional deben estar ubicados en Datic-DataCenter: protegidos con controles de acceso y seguridad física, sistemas eléctricos regulados, respaldados por fuentes de potencia ininterrumpida (UPS) y con circuitos alternos de entrada de corriente; además con monitoreo permanente de sensores de humo y temperatura.

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 Datic, controles de acceso y seguridad física, sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

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

6.4. REPORTE Y REVISIÓN DE INCIDENTES DE SEGURIDAD

En el caso de un incidente de seguridad de la información, el personal vinculado a la ESE Hospital Regional Manuela Beltrán Socorro deberá cumplir el procedimiento GIC-PC-39.

La oficina DATIC es la responsable de actualizar el procedimiento GIC-PC-39 para el reporte de incidentes de seguridad informática, y su respectiva socialización.

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. En cada equipo se configurarán dos tipos de cuentas para el sistema operativo: la cuenta de perfil administrador es de exclusivo manejo de la oficina DATIC, la cuenta de usuario normal es para el ingreso de los funcionarios que usan el equipo.

b. Cada equipo contará con software de seguridad, el cual será actualizado en cada mantenimiento preventivo que se realiza al mismo, buscando un máximo de 6 meses para cada actualización.

c. Instalación de un software tipo congelador en los equipos buscando restaurar su estado original simplemente con un reinicio.

d. Instalación de firewall para cada una de las dos conexiones de internet que posee el hospital, en especial la conexión que soporta las dos VPN con los nodos.

6.6. COPIAS DE SEGURIDAD

Es responsabilidad de todo funcionario realizar la copia de seguridad de la información manejada en cada equipo asignado, para este proceso se encuentra disponible el aplicativo de copias ubicado en Gestión Documental. Estas copias reposaran en la oficina DATIC, en un servidor destinado para este propósito. Este proceso será sujeto de auditoría por parte de la oficina DATIC, quien informará a las respectivas subdirecciones sobre el incumplimiento en estas actividades.

Las copias de seguridad de las bases de datos y documentos almacenados en los servidores ubicados en el datacenter de la institución, son realizadas por la oficina DATIC, 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 a 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 DATIC, el acceso de los usuarios a internet estará limitado solo para aquellos procesos en donde es requerido y mediante el uso de diferentes perfiles, los cuáles restringirán el horario, páginas visitadas y posibilidad de descarga de información, buscando mitigar el riesgo de un ataque web.

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.

El Artículo 10, del Acuerdo 028 del 2009, determina las normas para su uso, las cuáles se detallan a continuación:

a. El acceso a internet está restringido solamente a funcionarios de la institución que en el normal desarrollo de sus procesos lo requieran, y será administrado por medio de un servidor proxy y filtros de control de navegación. El número de usuarios por área será determinado de acuerdo a la capacidad del servicio contratado por la empresa con su proveedor externo de conectividad.

b. 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 el DATIC, como potencialmente dañinos para la seguridad informática de la ESE.

c. Como página de inicio de los navegadores debe ser establecida la página web institucional www.hospitalmanuelabeltran.gov.co.

d. 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.

e. 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.

f. El proceso DATIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

Para la red de datos institucional se debe contar con un Sistema de Detección de intrusos que permita estarla monitoreando permanentemente, de igual manera un firewall de altas prestaciones para la protección contra amenazas externas.

6.9. COMUNICACIONES INTERNAS Y EXTERNAS

Todo lo referente a la generación de comunicaciones tanto internas como externas, estará regida por “Política de Comunicaciones de la ESE Hospital Regional Manuela Beltrán Socorro”, establecida mediante resolución 355 del 2016.

7. PLAN DE IMPLEMENTACIÓN

La ESE Hospital Regional Manuela Beltrán Socorro viene aumentando la automatización de sus procesos y su oferta de servicios electrónicos a sus usuarios mediante el crecimiento de su plataforma informática, mediante desarrollo propio y 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 IMPLEMENTACION 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 Regional Manuela Beltrán Socorro.

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

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 Regional Manuela Beltrán Socorro y teniendo en cuenta sus necesidades.

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.

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.

7.2. CRONOGRAMA DESARROLLO

	2025-1	2025-2	2026-1	2026-2	2027-1	2027-2
Fase 1						
Fase 2						
Fase 3						
Fase 4						
Fase 5						
Fase 6						