PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PL-GI-02

2022-2024

Historial de Revisiones		
Fecha	Revisión	Concepto de modificación sobre la anterior revisión
30-sep-2022	01	Se elabora la creación del Plan de Seguridad y Privacidad de la Información
19-ene-2024	02	Se realiza revisión del plan y no se requiere hacer ajustes para 2024
Próxima revisión: cada año o antes si hay cambios que afecten al plan, lo que primero ocurra		

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Este documento describe el Plan estratégico de Seguridad de la Información para la E.S.E Hospital San Sebastián de Urabá en cumplimiento del marco legal que contempla la estructura y lineamientos dados por la política de gobierno digital 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. Con este documento se busca identificar las buenas prácticas para la gestión del plan de seguridad y privacidad de la información, incluyendo un diagnóstico de amenazas, para así planear estrategias y actividades que minimicen los riesgos de los activos.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer estrategias de seguridad y privacidad de la información, aplicando las políticas de seguridad digital y gobierno digital para proteger y preservar los activos de información, con el fin de garantizar su disponibilidad y confidencialidad en la E.S.E Hospital San Sebastián de Urabá.

2.2 OBJETIVOS ESPECIFICOS

- Proteger la información de la E.S.E Hospital San Sebastián de Urabá.
- Estudiar los Riesgos de seguridad para mantenerlos en niveles aceptables.
- Monitorear los riesgos de seguridad mediante herramientas de diagnóstico.
- Capacitar a empleados y contratistas de la institución, acerca de la seguridad y privacidad de la información y así fortalecer el nivel de concientización de los mismos en cuanto a la necesidad de salvaguardar los activos de la información críticos que se tengan en la E.S.E.
- Diseñar acciones preventivas y correctivas para mejorar la seguridad y privacidad de la información.
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales.

3. RESPONSABILIDADES

La responsabilidad en la elaboración del plan es del Líder de proceso de la dependencia de Sistemas-TIC, y la aplicación o ejecución del plan es del equipo directivo, líderes de la oficina de sistemas de información, líderes de los procesos y demás empleados.

4. DEFINICIONES

Activos. En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma.

Riesgo de seguridad de la información. Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

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).

Autorización. Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Ley de Transparencia y Acceso a la Información Pública. Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales. Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales

Vulnerabilidad. Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Datos Personales. Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3)

Datos Personales Públicos. Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos. Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Riesgo. El riesgo es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro.

Ciberespacio. Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Seguridad de la Información. Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información.

Seguridad de datos. La seguridad de los datos es la defensa de la información digital contra amenazas internas y externas, maliciosas y accidentales. Aunque la seguridad de los datos se centra específicamente en mantener los datos seguros, también incorpora la seguridad de la infraestructura.

Protección de Datos. La protección de datos es el proceso de salvaguardar información importante contra corrupción, verse comprometida o pérdida, La protección de datos se centra en la copia de seguridad y la recuperación.

Datos sensibles. aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación.

Amenazas. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema

Auditoria. Una auditoría es un proceso de verificación o validación del cumplimiento de una actividad según lo planeado y las directrices estipuladas

Derecho a la intimidad. Derecho a disfrutar de un ámbito propio y reservado para desarrollar una vida personal y familiar, plena y libre, excluida tanto del conocimiento como de las intromisiones de terceros.

5. META(S)

Lograr un cumplimiento mínimo de 80% del cumplimiento en la ejecución e implementación del plan de seguridad y privacidad de la información en 2024

6. DESARROLLO DEL PLAN

6.1 DESCRIPCIÓN

De acuerdo a la política y manual de seguridad y privacidad de la información aprobados por la E.S.E Hospital San Sebastián de Urabá, se realizan estudios de riesgos y así implementar estrategias que puedan minimizar los impactos que se tengan al momento de que se presente una eventualidad que afecte los activos de la institución.

6.2 MARCO NORMATIVO

- CONPES 3854 de 2016. Política Nacional de Seguridad Digital
- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública.
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad.
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.
- Ley Estatutaria 1581 de 2012 - Protección de datos personales.
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública.
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- Decreto 2364 de 2012 - Firma electrónica.

- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales.
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
- Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.

6.3 CONTEXTO INSTITUCIONAL

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

Misión

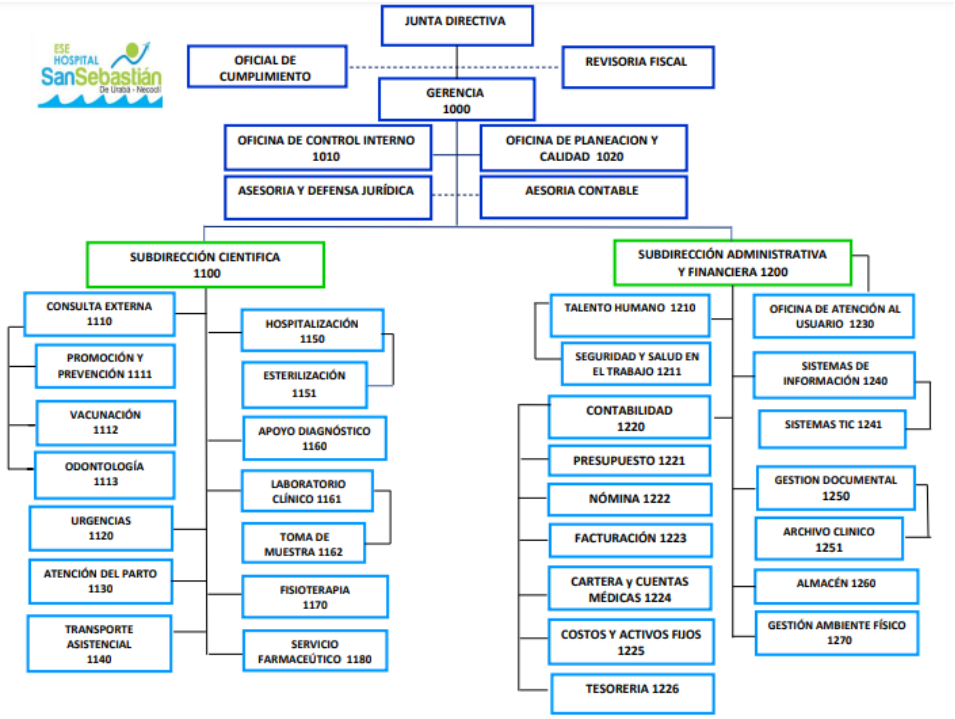
Somos la institución prestadora de servicios de salud de primer nivel de atención del municipio de Necoclí, que contribuye al bienestar y mejoramiento de las condiciones de salud de sus habitantes y visitantes; prestando servicios de salud de baja complejidad y otros de mediana, en la zona urbana y rural, a través de talento humano íntegro y competente que brinda trato humanizado.

Visión

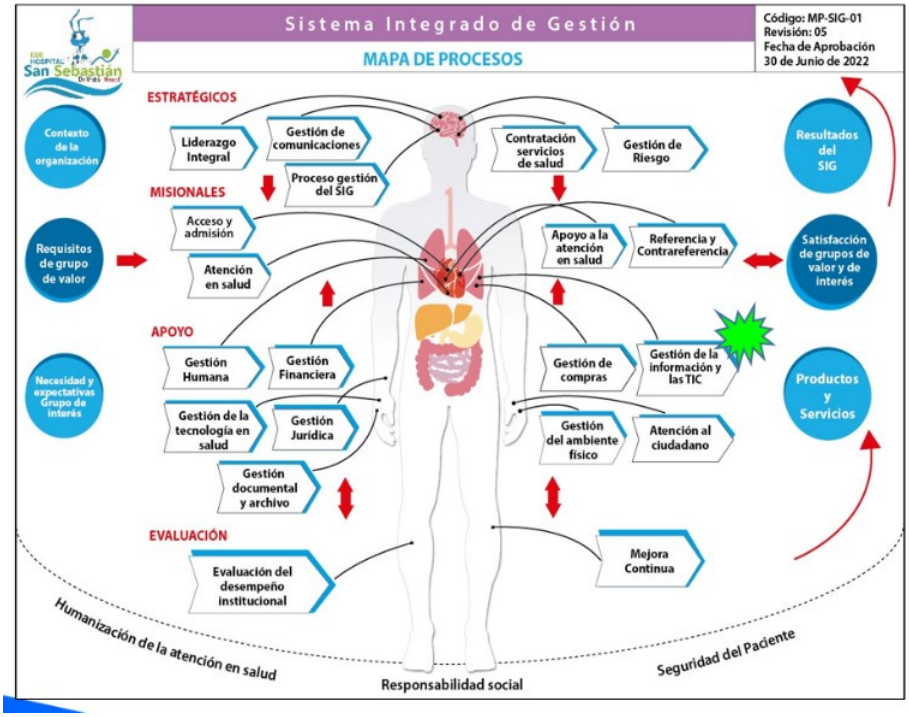
En 2024 seremos a nivel departamental un referente de entidad pública, que se destaca por ser sólida, solvente y competitiva, con un fuerte capital social, red de servicios de salud fortalecida en la zona rural y un alto sentido de la gobernanza para aunar esfuerzos; enmarcados en el respeto, la honestidad y el compromiso, para una mejor cobertura y resultados en salud, especialmente de la población más vulnerable como maternas, infantes, adolescentes y de riesgo cardiovascular.

6.3.1 Estructura Organizacional.

La E.S.E cuenta con una estructura organizacional que contiene las diferentes áreas, dependencia y oficinas mediante las cuales se busca garantizar el funcionamiento de la entidad. Entre estas dependencias se cuenta con la de Sistemas de información y Sistemas-TIC desde las que se lidera la implementación de la seguridad y privacidad de la información. Esta dependencia está ubicada en el área de la Subdirección Administrativa y Financiera. Esto con el fin de contar con una estructura funcional y de liderazgo.



3.2 Mapa De Proceso.



En relación con la gestión por procesos, la ESE ha identificado en el mapa de procesos, el proceso de gestión de la información y las TIC con el fin de desarrollar los procedimientos y actividades que se deben tener estandarizadas para un mejor desempeño en lo relacionado con el tratamiento de los activos de información.

6.3.3 SITUACIÓN ACTUAL (POLÍTICAS INSTITUCIONALES)

La E.S.E Hospital San Sebastián de Urabá actualmente cuenta documentos y políticas institucionales que nos motiva a mejorar y crear nuevas políticas que nos sirvan como marco de referencia para la garantizar la privacidad y seguridad de su información.

La E.S.E. Hospital San Sebastián de Urabá 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.

Así mismo ya se tienen definidas las políticas básicas para la seguridad y privacidad de la información, en las cuales se establecen los compromisos de acción como pilares para evidenciar su ejecución y aplicación en la entidad.

Entre las políticas establecidas en el sistema integrado de gestión desde la Gerencia de la E.S.E se tiene:

PO-LI-19 Política de Seguridad Digital
PO-LI-25 Política de Confidencialidad y Privacidad de la información
PO-L-07 Política de protección y tratamiento de datos

6.4 ACTIVOS DE INFORMACIÓN

- Todos los Líderes de proceso, en la actividad 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, el documento en el Sistema Integrado de Gestión
- La dependencia de almacén y activos fijos 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 dependencia de sus elementos de informática asignados.
- 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.

- No es permitida la instalación y desinstalación de software en el computador por cualquier persona diferente a los funcionarios de la dependencia de sistemas-TIC.
- Para el caso de computadores portátiles, el funcionario responsable del equipo está autorizado para la movilización de este, a los sitios tanto interno como externos que lo requiera, asumiendo las responsabilidades determinadas.

Políticas de seguridad

Con estas políticas se deben definir 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 la dependencia de sistemas, 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.

Normas para el manejo de la información generada por la plataforma informática de la ESE.

- 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.
- La información clínica de un paciente es estrictamente confidencial por lo tanto a ella solo tiene el personal debidamente autorizado.
- El acceso a la información institucional está basado en los perfiles de cuenta de cada usuario de acuerdo al software aplicativo que se use.
- 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.

- 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.
- E 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.
- En el caso de ser requerida la eliminación de información institucional este proceso debe seguir las indicaciones establecidas por el DATIC

6.5 SEGURIDAD DE LA INFORMACIÓN EN EL TALENTO HUMANO

Todos los funcionarios de la E.S.E Hospital San Sebastián de Urabá, 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.

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.

6.6 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 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 la dependencia de sistemas, controles de acceso y seguridad física, 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 a los lineamientos definidos por la institución.

6.7 PROTECCIÓN CONTRA MALWARE Y HACKING

Todos los equipos de informática de la ESE Hospital San Sebastián de Urabá deben estar protegidos de amenazas de malwar, tiene instalado el antivirus Kaspersky el cual les bloque el uso de dispositivos usb y el ingreso a paginas sospechosas, además instalación de software no autorizado cuyo objetivo es el de disminuir la probabilidad de un evento que genere daños en la plataforma informática.

- En la mayor parte de los equipos se configurarán dos tipos de cuentas para el sistema operativo la cuenta de perfil administrador es de exclusivo manejo de la dependencia de sistemas, la cuenta de usuario normal es para el ingreso de los funcionarios que usan el equipo.

- Cada equipo cuenta con software antivirus, el cual es actualizado semanalmente de manera automática.
- Se cuenta con un dispositivo endpiont o Firewall Fortinet un dispositivo de seguridad que permiten la creación de redes seguras y proporcionan una protección amplia, integrada y automatizada contra amenazas emergentes y sofisticadas, además controla el acceso a través del sistema de filtrado, protección y control de todo el tráfico de redes internas y externas.

6.8 COPIAS DE SEGURIDAD

Las copias de seguridad se hacen en la plataforma de backup **Acronis** ofrece protección de datos, para garantizar las copias de seguridad y la recuperación simple y fiable. Se cuenta además con un sistema de almacenamiento en RED NAS para la realización de copias de seguridad de la información de los usuarios más relevante, copias de la base de datos del software xenco.

- El proceso se realiza de forma automática, está configurado para realizar tareas de forma inmediata a los equipos de la entidad.
- La oficina de Sistemas debe verificar que se esté realizando la copia de seguridad, además de garantizar que se tenga suficiente espacio en el servidor de almacenamiento.
- Se tiene configurado tres copias automáticas de la de base de datos diariamente, se ejecutan una a las 4:30, 1:00, y 20:30 las cuales se guardan en el servidor NAS y una se guarda en la nube.
- Se guarda una copia en el equipo de escritorio de la oficina de a la cual se le hace cada 15 días la validación de integridad.

6.9 INTERCAMBIO DE INFORMACIÓN CON ENTIDADES EXTERNAS

Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por la Gerencia previamente, quién determinará las personas responsables del manejo y custodia dicha información. Todo requerimiento debe haber sido previamente radicado l. La información entregada será de acuerdo a la clasificación de confidencialidad establecida en el inventario de activos de información.

6.10 SERVICIO DE COMUNICACIÓN DE DATOS INTERNET

Este servicio será administrado por la dependencia de sistemas, 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 acceso 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.

- 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 dependencia de sistemas, como potencialmente dañinos para la seguridad informática de la ESE.
- Como página de inicio de los navegadores debe ser establecida la página web institucional www.hospitalnecocli.gov.co.
- 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.
- 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.
- Solo se debería usar el servicio de correo institucional para los procesos e intercambio de información institucional y no los de dominio público o personales.

.6.11 PLAN DE IMPLEMENTACIÓN

6.11.1 CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Diseñar estrategias para sensibilizar a funcionarios y contratistas de acuerdo a su rol dentro de la institución sobre la importancia de la seguridad de la información, la confidencialidad del dato y así minimizar los riesgos.

6.11.2 INDUCCIÓN AL PERSONAL QUE INGRESA LABORAR A LA INSTITUCIÓN

Verificar antecedentes de cada profesional que ingresa a realizar labores a la institución, además dar a conocer el tratamiento de datos personales y mantener la confidencialidad de los datos sensibles.

6.11.3 IDENTIFICAR Y CLASIFICAR ACTIVOS

Realizar inventarios detallados de los activos que se tienen en la institución, clasificando los que requieren confidencialidad. Dar a conocer el proceso para las bajas de inventario cuando los activos ya no se requieran por obsolescencia o presenten daños irreparables.

6.11.4 CONTROL EN EL INGRESO AL SISTEMA DE INFORMACIÓN

Crear perfiles, roles y asignarlos a cada funcionario dependiendo su especialidad para así restringir el acceso a los datos, de esta manera solo podrán acceder a la información necesaria para realizar sus labores.

Esto bajo el manual de procedimiento para usuarios y en el manual de manejo y custodia de historias clínicas, manuales que han sido aprobados por la institución

6.11.5 PROTECCIÓN DE ACTIVOS

Para la protección de los activos y mitigar los daños causados ante cualquier fenómeno, desastre, riesgo o vulnerabilidad se debe implementar acciones que minimicen el impacto y tiempo de respuesta para restablecer los servicios en la institución, para eso se tiene creada y aprobada la política de copias de seguridad y recuperación de la información, además, el manual para la migración de la información y así asegurar la integridad de los datos.

Se tienen controles de seguridad en los dispositivos de red como firewall para filtrar los datos que entran y salen de la institución, con esto se busca proteger los activos de ataques informáticos con software maliciosos.

6.11.6 PLAN DE MANTENIMIENTOS DE EQUIPOS

Para el plan de mantenimiento de equipos de pretender actualizar gradualmente la infraestructura tecnológica, adquiriendo equipos, repotenciando los que estén en mejores condiciones e ir actualizado los sistemas operativos ya que hay unos que no tienen soporte de Microsoft como lo son Windows 7 y Windows 8, y así mismo evitar incidentes que expongas nuestra seguridad. Además, se cuenta con un plan de mantenimiento de equipos que se realiza cada seis meses a nivel general y soporte continua para las eventualidades.

6.11.7 MAPA DE RUTA

ESTRATEGIA	ACTIVIDAD	OBJETIVO	PLAZO	PRIORIDAD
Capacitación Y Sensibilización Del Personal En Seguridad Y Privacidad De La Información	Crear ayudas didácticas para que cada colaborador sepa la importancia de la seguridad de la información y de cómo evitar que sea vulnerable a ataques cibernéticos o daños en los equipos informáticos.	Fortalecer el Modelo de seguridad y privacidad de la información de la institución, como habilitador fundamental, para dar cumplimiento a lo estipulado en la Política de Gobierno Digital.	CORTO PLAZO	ALTA
Inducción Al Personal Que Ingresa Laborar A La Institución	Al personal que ingresa como nuevos funcionarios, darle a conocer las restricciones que se tienen con los sitios web prohibidos, software no licenciado y tips para cuidar la integridad de los activos.	Fortalecer el Modelo de seguridad y privacidad de la información de la institución, como habilitador fundamental, para dar cumplimiento a lo estipulado en la Política de Gobierno Digital.	CORTO PLAZO	ALTA
Identificar Y Clasificar Activos	Realizar periódicamente inventario de todos los activos y llevar un control de cada cambio que se realice en cada sistema informático.	Garantizar la continuidad del negocio mediante el fortalecimiento de seguridad y privacidad de la información	CORTO PLAZO	ALTA
Control En El Ingreso Al Sistema De Información	Asignar a cada usuario un rol para ingresar solo a los módulos autorizados a realizar sus funciones y restringir	Fortalecer el Modelo de seguridad y privacidad de la información de la institución, como	CORTO PLAZO	ALTA

	acceso a módulos no autorizados, también hacer restricciones de sitios web no autorizados por la institución	habilitador fundamental, para dar cumplimiento a lo estipulado en la Política de Gobierno Digital.		
Protección De Activos	Tener en cuenta las recomendaciones y cuidados que se deben tener al momento de trabajar con los equipos informáticos, al ingresar datos en el sistema de información, para extender la vida útil de los equipos y garantizar la confiabilidad, veracidad e integridad de la información. Evitar el uso de correos de dominio público o personales para el intercambio de información institucional, implementar el uso de correo institucional.	Garantizar la continuidad del negocio mediante el fortalecimiento de seguridad y privacidad de la información	CORTO PLAZO	ALTA
Plan De Mantenimientos De Equipos	Realizar y ejecutar un plan de mantenimiento preventivo a equipos informáticos para minimizar los mantenimientos correctivos y así conservar los equipos en condiciones aptas para desarrollar las actividades diarias en las labores designadas en cada área	Fortalecer el Modelo de seguridad y privacidad de la información de la institución, como habilitador fundamental, para dar cumplimiento a lo estipulado en la Política de Gobierno Digital.	CORTO PLAZO	ALTA

7. RECURSOS (FINANCIEROS, FÍSICOS, TECNOLOGÍA)

Para la ejecución de éste plan existe un recurso tecnológico que cumple todas las características para la seguridad y protección de la información, además, se cuenta con un rubro en cada vigencia para cubrir los gastos e inversiones a futuro y así mejorar la infraestructura que se tiene, equipos de seguridad, firewall, Antivirus licenciado, software licenciado, hardware licenciado, servicio de backup en la nube.

8. MECANISMO DE SEGUIMIENTO Y MEDICIÓN

Indicador	Fórmula	Meta	Frecuencia
Porcentaje de cumplimiento en la meta para la vigencia 2024	Actividades proyectadas en la vigencia /Actividades ejecutadas en la vigencia	80%	Anual

9. DOCUMENTOS DE REFERENCIA

Internos:

Política de Seguridad y Privacidad de la Información
Manual de seguridad y privacidad de la información
Manual de del usario
Manual de manejo y custodia de historias clínica
PL-GI-01 PETI
PL-GI-04 Plan de acción Sistemas

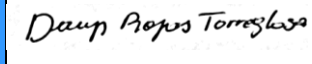
Externos:

ISO/IEC 27000
Decreto único reglamentario 1078 de 2015
Ley 594 de 2000, art 3
Ley 1581 de 2012, art 3
CONPES 3701
Resolución CRC 2258 de 2009
Ley 1712 de 2014, art 6
Decreto 1377 de 2013, art 3
Ley 1581 de 2012, art 3 literal h
Ley Estatutaria 1266 de 2008
Ley 1581 de 2012, art 25

10. CONTROL DE SOCIALIZACIÓN

Proceso/servicio/dependencia	Cargo(s) a los que se debe desplegar
Todos los procesos	Gerente, Subdirectores y Líderes de proceso

11. ANEXO

	Elabora	Revisa	Aprueba
Nombre	Danis Rojas Torreglosa	Damaris Isabel Doria C. Carrascal	Neyder Pupo Negrete
Cargo	Ingeniera de Sistemas	Asesora de Planeación y Calidad	Gerente
Firma			
Fecha	2-ene-2024	17-ene-2024	19-ene-2024