RESOLUCIÓN Nº 026
30 de enero de 2025

"POR MEDIO DE LA CUAL SE ADOPTA EL PLAN ESTRATEGICO DE TECNOLOGIAS DE INFORMACIÓN –PETI Y EL PLAN DE SEGURIDAD DE LA INFORMACIÓN DE LA ESE HOSPITAL PSIQUIÁTRICO SAN CAMILO, PARA LA VIGENCIA 2025"

La Gerente de la Empresa Social del Estado Hospital Psiquiátrico San Camilo, nombrada mediante Decreto 379 del 22 de marzo de 2025, expedido por el Gobernador de Santander y posesionada con Acta No. 017 del 01 de Abril de 2025, con efectos legales y fiscales, a partir del 01 de abril de 2025, en ejercicio de las atribuciones Constitucionales, legales, estatutarias y en especial las conferidas en el Acuerdo Nº 003 del 06 de febrero de 2006, y el Acuerdo N° 17 del 19 de diciembre de 2018, expedidos por la Junta Directiva de la Entidad, y

CONSIDERANDO:

Que la Empresa Social del Estado Hospital Psiquiátrico San Camilo, es una entidad prestadora de servicio de salud mental, descentralizada del orden departamental, dotada de personería jurídica, patrimonio propio y autonomía administrativa, de conformidad con lo dispuesto en el Decreto 0098 del 14 de agosto de 1995, *"Por medio del cual se transforma un Hospital Departamental en una Empresa Social del Estado"*, proferido por el Gobernador de Santander y el Acuerdo de Junta Directiva N° 003 de 2006, *"Por medio del cual se reforma el Estatuto de la Empresa Social del Estado Hospital Psiquiátrico San Camilo"*, expedido por la Junta Directiva de la Entidad.

Que la Ley Estatutaria 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013, y por el Decreto 1081 de 2015; por medio de la cual se dictan disposiciones generales para la protección de datos personales; *"tiene por objeto desarrollar el derecho constitucional que tienen todas las personas de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos".*

Consecuente a ello; el Decreto 1008 de 2018, *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"* tiene como finalidad lograr la prestación de servicios eficientes a los ciudadanos, así mismo, determinó que es función del Estado intervenir en el sector de las TIC, reglamentando consigo las condiciones en que se garantizará el acceso a la información en línea, de manera abierta, ininterrumpida y actualizada.

El Decreto 1078 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"* contempló en el artículo 2.2.9.1.2.2, los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI, de

www.hospitalsancamilo.gov.co ventanillaunica@hospitalsancamilo.gov.co (607) 7008391 Calle 45 N° 7- 18 Bucaramanga, Santander.

un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información.

Así mismo; el Decreto 2578 de 2012 *"Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto número 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los archivos del Estado"* consagra el deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles, entre otras disposiciones.

Por otra parte; el Decreto 2609 de 2012, compilado por el Decreto 1080 de 2015; *"... reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado"*, e incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

Aunado a ello; con ocasión a la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de la información y las comunicaciones; a través de la Ley 1273 de 2009; se modificó el código penal; creando un nuevo bien jurídico tutelado.

En esa misma línea; la Ley 1341 de 2009, define los principios y conceptos sobre la Sociedad de la Información y la Organización de las Tecnologías de la Información y Comunicaciones - TIC, crea la Agencia Nacional de Espectro, y se dictan otras disposiciones.

Que la Ley 599 de 2000, "*por la cual se expide el Código Penal*", creó el bien jurídico de los derechos de autor e incorporó conductas relacionadas con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y establece que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, hace incurrir en multa.

Que la norma ISO/IEC 27001:2005 establece la evolución certificable del Código de Buenas Prácticas ISO 17799, y define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Esta norma constituye la base para la gestión de la seguridad de la información.

Así mismo, a través del Decreto 612 del 04 de abril de 2018, fijó las directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, estableciendo en el artículo 1 *"Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos:*

> *"**2.2.22.3.14**.* **Integración de los planes institucionales y estratégicos al Plan de Acción.** *Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (...)*
>
> *10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI*
> *11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información*

N500

12. Plan de Seguridad y Privacidad de la Información".

Por su parte, es importante precisar que el proyecto de Acreditación en Salud emprendido por la ESE Hospital Psiquiátrico San Camilo, se encuentra regulado por los parámetros del Manual de Acreditación en Salud Ambulatorio y Hospitalario de Colombia Versión 3.1., dentro del cual se define como intencionalidad del grupo de estándares de Gerencia de la Información, *"Que la organización obtenga cada vez mejores resultados en el desempeño de la gestión de información. Para esto, la organización desarrolla un plan para la gerencia de la información, de manera sistemática con fundamento en el ciclo de mejoramiento continuo de la calidad".*

Finalmente, se advierte que el Estándar 143. Código: (GI2) del Manual de Acreditación en Salud Ambulatorio y Hospitalario de Colombia Versión 3.1. indica que, existe un proceso para planificar la gestión de la información en la organización, el cual debe estar documentado, implementado y evaluado en un plan de gerencia de la información, y deberá incluir criterios tales como: la identificación de las necesidades de la información, un proceso de implementación basado en prioridades, la recolección sistemática y permanente de la información necesaria y relevante que permita a la dirección y a cada uno de los procesos, la toma oportuna de decisiones, el uso, flujo, almacenamiento, conservación y depuración de la información, la recolección sistemática de las necesidades, las opiniones y los niveles de satisfacción de los clientes del sistema de información, cualquier difusión en el sistema de información es recolectada, analizada y resuelta, la seguridad y confidencialidad de la información, la identificación de espacios gerenciales y técnicos para el análisis de la información, la definición de indicadores corporativos que incluyan: seguridad del paciente, humanización, gestión del riesgo y gestión de la tecnología, la comparación con mejores prácticas y sistemas de medición, evaluación y mejoramiento del plan.

En ese orden de ideas, se hace necesario adoptar el plan estratégico de tecnologías de información –PETI, y el Plan de Seguridad de La Información de la ESE Hospital Psiquiátrico San Camilo para la vigencia 2025

En mérito de lo anterior,

RESUELVE:

ARTÍCULO PRIMERO: ADOPCIÓN: Adoptar el Plan Estratégico de Tecnologías de Información –PETI y El Plan de Seguridad de la Información de la ESE Hospital Psiquiátrico San Camilo y sus sedes para la vigencia 2025.

ARTÍCULO SEGUNDO: SEGUIMIENTO Y EVALUACIÓN: El seguimiento plan estratégico de tecnologías de información PETI y el Plan de Seguridad de la Información será realizado por el Área de TIC, bajo la supervisión de la Subdirección Administrativa y Planeación.

ARTÍCULO TERCERO: DIVULGACIÓN: La presente resolución será comunicada al correo institucional de los empleados, contratistas y colaboradores de la entidad por parte el profesional vinculado al proceso de gestión de la información y será publicada en la página web de la ESE Hospital Psiquiátrico San Camilo (www.hospitalsancamilo.gov.co).

ARTÍCULO CUARTO: AMBITO DE APLICACIÓN: El Plan ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACION-PETI y EL PLAN DE SEGURIDAD DE LA

INFORMACIÓN 2025, es de obligatorio cumplimiento para todos los empleados, contratistas, colaboradores y personal vinculado a la Empresa Social del Estado Hospital Psiquiátrico San Camilo, en cualquier nivel, en todas las áreas de la misma y sus sedes de acuerdo con los Convenios firmados.

ARTÍCULO QUINTO: VIGENCIA: La presente resolución rige a partir de la fecha de su expedición y deja sin efectos todos los actos administrativos que le sean contrarios.

Se expide en Bucaramanga, a los 30 días del mes de enero de dos mil Veinticinco 2025.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Natalia S. Ojeda O.

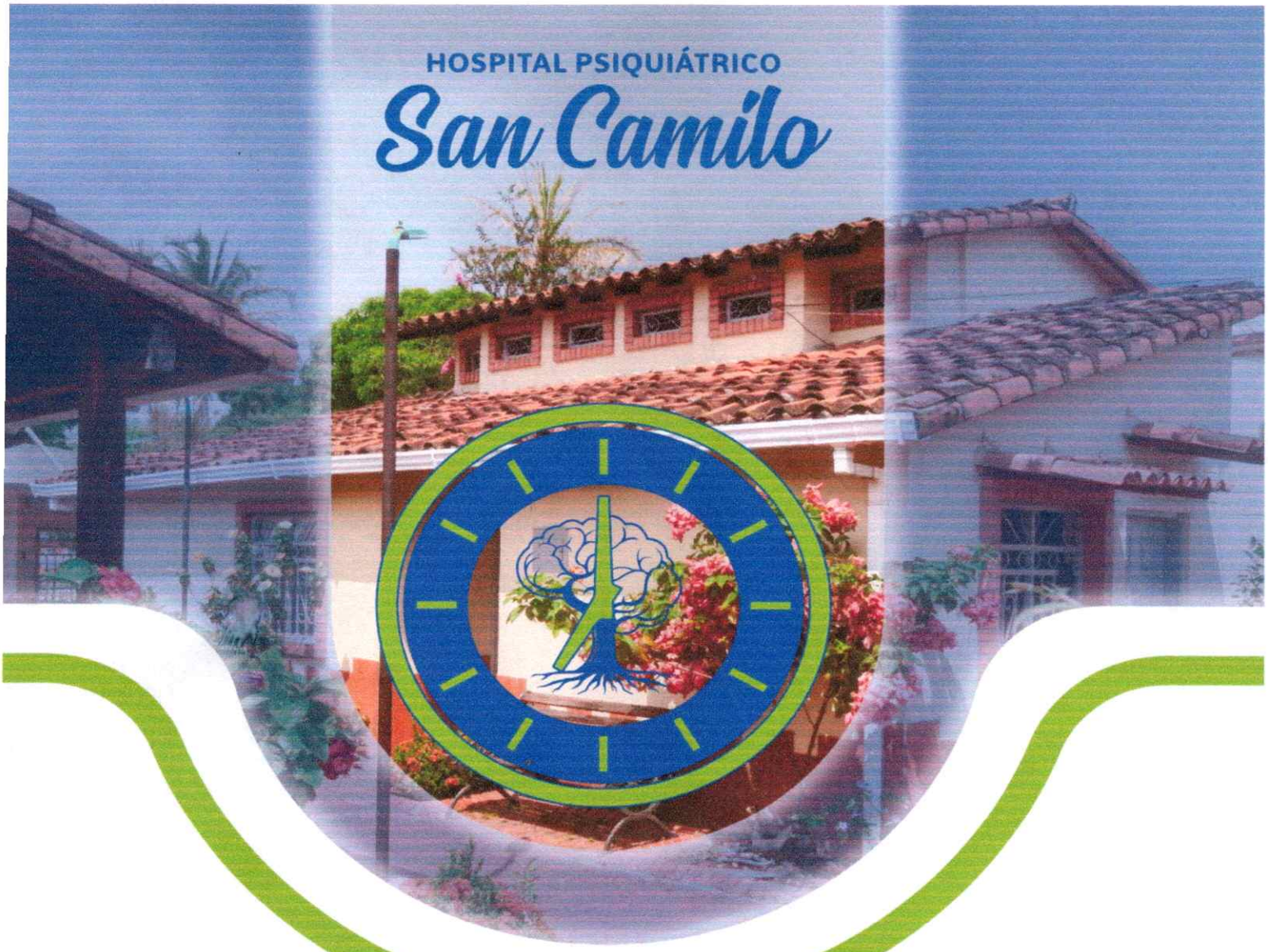
NATALIA SOFIA OJEDA ORTIZ
Gerente

Revisó Aspectos Jurídicos: Yennifer Ximena Mayorga A.
Abogada Apoyo Oficina Jurídica.

Proyectó: Erwing Jesid Dávila García
Apoyo Profesional II

Revisó Aspectos Técnicos: Margarita María Pinto Díaz
Profesional Proceso de Planeación

N500



Tipo de proceso: PLAN DE SEGURIDAD DE LA INFORMACIÓN

Proceso: Gestión de la Información

Subproceso: Tecnologías de la Información y las Telecomunicaciones

Código: AD-GIT-TIC-PL-22

Versión: 04

Fecha de aprobación: 30/01/2025

TABLA DE CONTENIDO

HOSPITAL PSIQUIÁTRICO San Camilo

N500

1. INTRODUCCIÓN

En un mundo cada vez más digitalizado, la información se ha convertido en uno de los activos más valiosos para las organizaciones. En la ESE Hospital Psiquiátrico San Camilo; la protección de datos sensibles, la confidencialidad de la información y la seguridad contra ciberamenazas son factores clave para garantizar la estabilidad y la confianza en nuestras operaciones.

Este plan de seguridad de la información tiene como objetivo establecer políticas, procedimientos y controles para salvaguardar la integridad, disponibilidad y confidencialidad de la información dentro de nuestra organización. A través de una gestión proactiva y la aplicación de buenas prácticas, buscamos minimizar los riesgos asociados a la manipulación, almacenamiento y transmisión de datos.

La implementación de este plan nos permitirá no solo cumplir con las regulaciones en materia de seguridad informática, sino también fortalecer nuestra reputación y garantizar la continuidad del negocio ante posibles incidentes de seguridad.

2. JUSTIFICACION

Este plan tiene como finalidad mitigar los posibles riesgos a los cuales está expuesta la institución en cuanto al manejo de seguridad de la información; y se realiza por medio de las políticas establecidas en la institución.

Con el plan propuesto en este documento, el proceso de Gestión de la información, contará con un instrumento que permita a la institución conocer y actuar ante los riesgos que se puedan presentar en la ESE Hospital Psiquiátrico San Camilo y sedes.

Este Plan de Seguridad de la Información inicia con la descripción de la Políticas aprobadas en la ESE Hospital Psiquiátrico San Camilo para la seguridad de la información y finaliza con los controles de modificaciones.

3. OBJETIVO GENERAL

El objetivo principal del plan de seguridad de la información es mantener un ambiente razonablemente seguro alineado a la misión de la Entidad, que permita proteger los activos de información que componen la estrategia de La ESE Hospital Psiquiátrico San Camilo y sus sedes, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información, y el aseguramiento de su continuidad.

Como objetivos del plan de seguridad de la información se plantean los siguientes:

- Cumplir con la política y principios de seguridad de la información, con el fin de administrar adecuadamente los riesgos.
- Asegurar la información y los sistemas de información, contra la divulgación, modificación, apropiación y/o uso no autorizado que comprometan los servicios de la Entidad.
- Concienciar a los funcionarios de los beneficios frente a las buenas prácticas de seguridad de la información.
- Garantizar la continuidad de la información, los servicios y recursos Esenciales, frente a la ocurrencia de un incidente de seguridad de la información, que pueda afectar la operatividad de La ESE Hospital Psiquiátrico San Camilo.
- Brindar elementos de trazabilidad de las actividades desarrolladas por la ESE Hospital Psiquiátrico San Camilo, dentro de los eventos que puedan comprometer la seguridad de los activos de información o ante la presencia de un incidente de seguridad de la información.

3.1 Objetivos específicos

- Proteger la información asegurando su confidencialidad, confiabilidad y disponibilidad.
- Garantizar la preservación y conservación de la información física y digital.
- Fortalecer la administración de la información para la correcta valoración, análisis y evaluación.
- Actualizar las tecnologías, herramientas y estrategias para el procesamiento y almacenamientos de la información.
- Gestionar los planes de contingencia para garantizar la continuidad e integridad de los sistemas de información.

4. PARTES INTERESADAS

- Los funcionarios del Área de Sistemas serán los encargados de realizar el seguimiento para el respectivo cumplimiento del Plan de Seguridad de la Información de La ESE Hospital Psiquiátrico San Camilo.
- De igual forma el plan aplica para todos los funcionarios y las sedes de La ESE Hospital Psiquiátrico San Camilo.

N500

5. POLÍTICAS

5.1 Política de seguridad de la información

La ESE Hospital Psiquiátrico San Camilo garantiza la protección, preservación y administración eficiente de la información haciendo uso de las tecnologías adecuadas, herramientas y estrategias para mitigar amenazas internas, externas, deliberadas y accidentales.

Alcance

La política de seguridad de la información cubre todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y usuarios que laboren o tengan relación con La ESE Hospital Psiquiátrico San Camilo, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

Indicadores de gestión

- Evaluar los riesgos de seguridad a los que está expuesta cada Unidad Administrativa.
- Evaluar iniciativas, proyectos y planes institucionales de Seguridad de la Información.
- Evaluar y seleccionar las herramientas de seguridad informática.

Acciones estratégicas

- Desarrollar un Plan de Seguridad de la Información para que sea adoptado por las diferentes áreas institucionales, que conlleve a la protección de los activos de información, su confidencialidad, integridad y disponibilidad.
- Gestionar y coordinar esfuerzos, por crear un plan de contingencia, que de sustento o solución, a problemas de seguridad dentro de la institución.
- Impulsar y promover la implantación de controles tecnológicos para proteger la información.
- Informar sobre problemas de seguridad a la alta gerencia.

5.2 Política de uso de dispositivos móviles

Alcance

Garantizar la seguridad de la información cuando se utilizan dispositivos móviles.

Objetivo

Adoptar medidas de seguridad apropiadas para la protección de la información contra los riesgos introducidos por el uso de los dispositivos móviles.

Detalle

Teniendo en cuenta los riesgos en el uso de dispositivos móviles (computadores portátiles, tabletas, tarjetas inteligentes, teléfonos celulares, entre otros), La ESE Hospital Psiquiátrico San Camilo implementará mecanismos de protección física, claves de acceso, cifrado de información, copias de respaldo, instalación de antivirus y autenticación en la conexión remota a la red de la Entidad. Así mismo, se realizarán campañas de sensibilización a los usuarios para concienciarlos y asesorarlos acerca de las buenas prácticas de seguridad, equipos desatendidos y aseguramiento de los dispositivos.

Condiciones obligatorias

- Se deberá tener especial cuidado al utilizar dispositivos móviles en lugares públicos, salas de reuniones u otros entornos sin la debida protección por parte de la Entidad.
- Se deberán proteger física y lógicamente los dispositivos móviles para evitar el hurto, acceso o la divulgación no autorizada de la información, cifrar la información en caso de ser necesario y tener copias de respaldo.
- se deberá bloquear los servicios de conexión y servicios compartidos cuando no se estén usando.
- Los dispositivos móviles del nivel directivo y sistemas, solamente podrán conectarse a la red interna de La *ESE* Hospital Psiquiátrico San Camilo, pero en caso de detectarse alguna actividad no autorizada, se restringirá el uso del servicio.
- Una vez los funcionarios hayan culminado su relación laboral con la entidad, el Área de Sistemas con la información suministrada del Área de Talento humano

N500

denegará el acceso a la información o sistemas de información accedidos desde los dispositivos móviles.

En caso tal se presente el extravió o hurto de un dispositivo móvil que contengan información crítica o sensible de la entidad, el funcionario será el responsable de reportar de forma inmediata al Responsable de Seguridad de la Información, quien identificará conforme la información contenida, las medidas de seguridad adecuadas para la protección de la información.

Usos no autorizados

- Los dispositivos móviles que manejen o administren información confidencial o crítica de la entidad, no se podrán conectar a una red pública, y deberán ser transportados y usados con cautela para evitar el daño o manipulación no autorizada de la información, así mismo, será necesario evitar dejar el equipo desatendido.
- No se deberán realizar instalaciones de aplicaciones de dudosa procedencia que puedan afectar la confidencialidad, integridad y/o disponibilidad de la información almacenada o transmitida por el dispositivo.
- Está prohibido almacenar y transferir información sensible de la Entidad en dispositivos móviles personales de los usuarios, y aquellos dispositivos que sean de propiedad de la entidad deberán garantizar la debida protección de la información contenida en ellos.

Responsabilidades

- Todos los funcionarios, colaboradores y terceros que tengan acceso a la información por medio de dispositivos móviles deberán cumplir la presente política.
- El Área de Sistemas, deberá adoptar las medidas y mecanismos de seguridad adecuados para proteger la seguridad almacenada y transmitida en los dispositivos móviles de la Entidad.
- El Responsable de Seguridad de la Información o delegado en coordinación con el Área de Talento Humano deberán realizar capacitaciones periódicas a todo el personal de La ESE Hospital Psiquiátrico San Camilo para el uso adecuado de los dispositivos móviles.

Procedimientos del área

- Procedimiento de creación, modificación, cancelación de cuentas de Usuario y privilegios.
- Procedimiento de control de cambios.
- Procedimiento Mantenimiento de Equipos.

Controles por área

- Antes de realizar actividades que involucren el uso de dispositivos móviles, se deberá identificar los requisitos mínimos de seguridad, la sensibilidad de la información y las vulnerabilidades y amenazas existentes.
- Para la transmisión de información de la Entidad haciendo uso de dispositivos móviles, se deberá establecer canales de comunicación segura para preservar la integridad y confidencialidad de la información.
- Capacitar periódicamente al personal de la Entidad en buenas prácticas de seguridad en el uso de dispositivos móviles.

5.3 Política de control de acceso a la información

Alcance

Controlar el acceso de la información y restringirla sólo al personal autorizado conforme el perfil de acceso.

Objetivo

Generar mecanismos para controlar el acceso a la información, medios de procesamiento y sistemas de información alineados a la misión de la entidad.

Detalle

Esta política tiene como fin controlar el acceso a los sistemas de información de la ESE hospital psiquiátrico san camilo, teniendo en cuenta mecanismos de protección para la red, datos y la información, así como la implementación de perímetros de seguridad para la protección de áreas con instalaciones de procesamiento de información, suministro de energía eléctrica, aire acondicionado, y cualquier otra área considerada crítica para la operatividad de la entidad.

El emplazamiento y la fortaleza de cada barrera estarán definidas por el responsable o encargado de seguridad de la información con el asesoramiento del responsable de seguridad física, de acuerdo al resultado de la evaluación de riesgos efectuada.
El control de acceso a la información deberá estar previsto para controlar el acceso tanto lógico como físico y se deberán considerar en conjunto.

Condiciones obligatorias

- Los funcionarios y contratistas de la ESE hospital psiquiátrico san camilo y sedes son responsables de la información que manejan y deberán cumplir los lineamientos establecidos por la entidad, con el fin de evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la información. así mismo no deberán suministrar información de la entidad a ningún ente o persona externa sin la debida autorización.
- Todo funcionario que utilice la información y los sistemas de información de la ESE hospital psiquiátrico san camilo, tiene la responsabilidad de velar por la integridad, confidencialidad y disponibilidad de la información, especialmente si dicha información está clasificada como confidencial y/o crítica.
- Todos los funcionarios y contratistas que laboran para la ESE hospital psiquiátrico san camilo tendrán acceso sólo a la información necesaria para el desarrollo de sus labores.
- Las claves de acceso compartidas asignadas a los funcionarios de los sistemas de información de la entidad tendrán únicamente carácter de consulta, estas no permiten modificación de la información, se modificarán periódicamente o cuando se requiera y exclusivamente se utilizarán para la gestión de la entidad.
- Todos los accesos y claves de usuario para el uso de los sistemas de información de la ESE hospital psiquiátrico san camilo, deberán ser desactivados o cambiados después de que un funcionario cese de prestar sus servicios en la ESE hospital psiquiátrico san camilo, dicha información será emitida por el área de talento humano al área de sistemas, una vez el funcionario culmine sus actividades laborales
- El acceso a la información y los sistemas de información deberá ser consistente con el procedimiento de clasificación y etiquetado de la información, y así mismo, el acceso estará otorgado con respecto al rol y responsabilidad de cada uno de

los funcionarios dentro de la entidad, basándose en la premisa "en general, todo está prohibido, a menos que esté expresamente permitido".

- Los funcionarios de la ESE hospital psiquiátrico san camilo, terceras personas y contratistas que tengan acceso a la información deberán firmar un acuerdo de confidencialidad de la información, en donde se establezcan las obligaciones y responsabilidades contractuales relacionadas con la protección del acceso a los datos o los servicios y sistemas de información.
- Se deberán atender los requerimientos establecidos de los lineamientos de gobierno en línea, respecto a la publicación de información de la entidad en la página web.
- Cuando se identifique la necesidad de trabajar con partes externas y se necesite acceso a la información y/o sistemas de información, se deberá realizar una evaluación de riesgos para determinar las implicaciones de seguridad y los requisitos de control.
- En las instalaciones de la entidad deberán existir elementos de control de incendio, inundación, alarmas, circuito cerrado de televisión, y de igual forma deberán estar demarcados como zona restringida.
- Los equipos de cómputo (computadores, servidores, impresoras, equipos de comunicación, entre otros) no deberán moverse o reubicarse sin la aprobación previa.

Responsabilidades

- Todos los funcionarios, colaboradores y terceros que tengan acceso a la información y sistemas de información deberán cumplir la presente política.
- El responsable de seguridad de la información o delegado en coordinación con el área de talento humano deberá realizar capacitaciones periódicas a todo el personal de la ESE hospital psiquiátrico san camilo para el uso adecuado de los la presencia de desconocidos no escoltados o cualquier persona que no exhiba una identificación visible recursos tecnológicos y las responsabilidades de los funcionarios frente a la seguridad de la información.
- Los funcionarios se comprometen a no utilizar la red regulada de energía (tomacorrientes naranja o ups) para conectar equipos eléctricos diferentes a su computador o demás equipos autorizados por los administradores de la red.

- Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

Procedimientos por área

- Procedimiento de creación, modificación y cancelación de cuentas de usuario y privilegios.

Controles por área

Controles físicos: las áreas críticas se protegerán mediante el empleo de controles de acceso físico determinados por el responsable del área de sistemas, a fin de permitir el acceso sólo al personal autorizado. Estos controles tendrán, por lo menos, las siguientes características:

- Controlar y limitar el acceso a la información y sistemas de información, exclusivamente a las personas autorizadas, utilizando controles de autenticación y registros de acceso.
- La ESE hospital psiquiátrico san camilo implementará el uso de identificación visible para los funcionarios y se concienciará al personal acerca de comunicar.
- Se revisará y actualizará periódicamente la lista de funcionarios autorizados para acceder a las áreas críticas, los cuales serán generados y firmados por el responsable del área.

Control de acceso lógico

- Los usuarios sólo tendrán acceso a los servicios para cuyo uso están específicamente autorizados conforme el procedimiento de creación, modificación y cancelación de usuario y privilegios.
- El Área de Sistemas de La ESE Hospital Psiquiátrico San Camilo., velará por la protección del acceso lógico y físico a los puertos de configuración y diagnóstico de los equipos de red y demás que sean considerados como críticos.
- Se implementarán controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información, correspondan los lineamientos definidos por la entidad.
- Todos los sistemas automáticos que operen y administren información sensible, valiosa o crítica para la entidad como son los sistemas de bases de Datos y

telecomunicaciones deben generar un libro con la bitácora de auditoría de la tareas principales (adición, modificación, borrado). El libro de bitácora de auditoría debe proporcionar suficiente información para apoyar el monitoreo, control y auditorías.

5.4 Política de escritorio limpio y pantalla limpia

Alcance

Preservar la seguridad de la información de La ESE Hospital Psiquiátrico San Camilo y sedes por medio de buenas prácticas en el manejo de documentos, medios de almacenamiento removibles y pantalla de los dispositivos de procesamiento de información.

Objetivo

Generar controles para que los funcionarios de la ESE hospital psiquiátrico san camilo y sedes conserven el escritorio limpio de documentos, medios de almacenamiento removibles y pantalla limpia en sus dispositivos de almacenamiento y procesamiento de información.

Condiciones obligatorias

Para el aseguramiento de la información sensible de la entidad, los funcionarios deberán adoptar buenas prácticas al momento de manejar y administrar la información de la ESE hospital psiquiátrico san camilo y sedes, teniendo en cuenta los niveles de clasificación de la información, los riesgos identificados. Para ello se deberá tener en cuenta:

- El fondo de pantalla de los equipos de cómputo, será el configurado por la oficina de sistemas el cual está guardado en uno de los servidores de la institución y será modificado previa solicitud del área responsable.
- Fomentar las buenas prácticas con los funcionarios de la institución para no guardar información en el escritorio del equipo de cómputo en el cual solo deberán permanecer los accesos directos a los programas utilizados por cada servicio.
- Se limitará en lo posible, el uso de fotocopiadoras y tecnologías de reproducción, con el fin de conservar la confidencialidad y evitar la pérdida o fuga de información de la entidad.
- Los datos sensibles almacenados en los equipos o sistemas de información, deberán encontrarse ubicados en rutas que no sean de fácil acceso.

Responsabilidades

- Los funcionarios de la ESE hospital psiquiátrico san camilo y sedes, serán los encargados de hacer buen uso de la información tanto física como lógica, y de cumplir los lineamientos descritos en la presente política

Procedimientos por área

- Procedimiento de control de cambios.

Controles por área

- El Área de Sistemas, limitará el acceso de los dispositivos de impresión o fotocopiadoras, con el fin de impedir que una persona no autorizada duplique información sensible o confidencial de la Entidad.
- Los equipos serán configurados, para el no cambio del fondo de escritorio y dispositivos de acceso removibles.
- El Responsable de Seguridad de la Información o delegado en coordinación con el Área de Talento Humano serán los encargados de capacitar a todos los funcionarios de La ESE Hospital Psiquiátrico San Camilo en buenas prácticas de seguridad.

5.5 Política de gestión de cambios

Alcance

Asegurar que los cambios en los medios y sistemas de procesamiento de la información se encuentren acordes con las necesidades y requerimientos de la ESE hospital psiquiátrico san camilo.

Objetivo

Controlar los cambios en los medios y sistemas de procesamiento de la información, por medio de mecanismos de seguridad adecuados.

Detalle

- los cambios sólo se deberán realizar cuando existe una razón válida para hacerlo, como un incremento en el riesgo para el sistema, sin embargo siempre se deberá

evaluar las posibles implicaciones debido al riesgo de introducir nuevas vulnerabilidades e inestabilidad en el sistema.

- todo requerimiento de mejora (creación y modificación de programas, pantallas) o reporte de falla que afecte los sistemas de información de la ESE hospital psiquiátrico san camilo, deberá ser solicitado por los usuarios del sistema y para su seguimiento el área de sistemas.
- cualquier tipo de cambio en la plataforma tecnológica deberá quedar formalmente documentado desde su solicitud hasta su implantación en el formato. este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.
- todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros deberá realizarse sin la alteración de la seguridad.
- el área de sistemas deberá verificar que los cambios sean propuestos por usuarios autorizados y se encuentren alineados a la licencia de uso y necesidades de la entidad.
- el responsable de seguridad de la información revisará las solicitudes de cambio y realizará un análisis de impacto, para garantizar que no se violen los requerimientos de seguridad, al mismo tiempo velará por la implementación de mecanismos de control adecuados para el aseguramiento de la información y la continuidad de las operaciones.
- el área de sistemas deberá mantener un control de versiones para todas las actualizaciones de software y los cambios realizados, con el fin de realizar rollback en el caso que sea necesario.
- el área de sistemas garantizará que la implementación de los cambios se lleve a cabo sin generar discontinuidad de las actividades operativas, la alteración de los procesos y la operatividad de la entidad para el cumplimiento de la misión institucional
- los responsables de los cambios, deberán informar antes de la implementación de un cambio a las áreas o usuarios que puedan verse afectados, con el fin de evitar indisposición y falta de operatividad.
- una vez realizado un cambio, el responsable deberá documentar las actividades realizadas, la información relevante y los resultados obtenidos después de realizado el cambio.

Responsabilidades

- los funcionarios y usuarios autorizados deberán velar porque los cambios se encuentren alineado a las necesidades operativas y el cumplimiento de la misión de la entidad.
- el responsable de seguridad de la información o persona delegada en coordinación con el área de sistemas, serán los responsables de controlar los cambios y prever el impacto que puedan ocasionar a la seguridad de la información.
- el funcionario encargado del cambio, deberá documentar detalladamente las actividades realizadas, así como los resultados obtenidos y los mecanismos de mitigación del impacto en el caso que aplique

Procedimientos por área

- procedimiento de control de cambios.

Controles por área

- La solicitud de cambios, sólo será realizada por usuarios autorizados.
- Los cambios deberán ejecutarse, una vez han sido identificados y controlados los riesgos de seguridad de la información, y de igual forma antes de ejecutarlos se deberán encontrar autorizados por el responsable.
- Los cambios serán documentados para realizar su respectivo seguimiento y auditoría, y al mismo tiempo, se realizará un control de versiones para tener como contingencia un rollback en caso de ser necesario.

5.6 Política de generación y restauración de copias de respaldo

Alcance

Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información críticos de la ESE hospital psiquiátrico san camilo a través de copias de respaldo.

Objetivo

Realizar copias de respaldo para preservar la disponibilidad de la información y revisarlas regularmente para asegurar la restauración de la información en caso que sea necesario.

Detalle

La información que es soportada por la infraestructura de tecnología informática de la ESE hospital psiquiátrico san camilo deberá ser almacenada y respaldada de tal forma que se garantice su disponibilidad.

El almacenamiento de la información se deberá realizar internamente en la entidad, de acuerdo con su importancia. La información de copias de respaldo, estará bajo custodia por la oficina de sistemas de tal forma que garantice que la información no sea de condiciones obligatorias manipulada por ninguna persona externa o interna durante su creación, estas copias de seguridad permitirán hacer seguimiento de control en una auditoría o en caso de requerirse recuperar la información de los procesos.

Condiciones obligatorias

- se deberá identificar el nivel necesario de valor y criticidad de la información de respaldo, así como la frecuencia en donde deberán reflejarse los requisitos de seguridad de la información involucrada y la importancia de la operación continua de la institución.
- los respaldos se deberán almacenar en un sitio lejano con protección física, lógica y ambiental, a una distancia suficiente para escapar a cualquier daño causado por desastres.
- los procedimientos de restauración como los medios de respaldo, se verificarán y probarán periódicamente para garantizar la disponibilidad de la información en caso de contingencia o desastre.
- los funcionarios del área de sistemas serán los responsables de generar las copias de respaldo de los servidores de red y bases de datos, o demás servicios identificados como críticos, en horas no laborables para la entidad.
- la copia de respaldo deberá tener el mismo tratamiento y manejo conforme el nivel de clasificación de la información contenida.

Usos no autorizados

Cada funcionario de la ESE hospital psiquiátrico san camilo y sedes será el responsable de mantener la información de su computador en las carpetas creadas para el almacenamiento, para garantizar la disponibilidad y copias de seguridad de la información de la entidad.

Responsabilidades

La oficina de sistemas serán los encargados de custodiar adecuadamente los medios de almacenamiento en donde se alojada la información de respaldo, así como de realizar las pruebas para asegurar la disponibilidad de la información en caso de una contingencia.

Los funcionarios de cada dependencia deberán mantener depurada la información de las carpetas compartidas, como buena práctica para la optimización de recursos de la entidad.

Procedimientos por área

Procedimiento de copias de respaldo.

Controles por área

La oficina de sistemas realizara el procedimiento de copias de respaldo (BackUp) en el cual se establecen los pasos a llevar a cabo para la extracción de las copias de respaldo, así como un registro de control de BackUp, en donde se registran las actividades realizadas y el consecutivo de las copias.

5.7 Política de transferencia de información

Alcance

Mantener la seguridad en el intercambio de información y sistemas dentro de la entidad y con cualquier otra organización.

Objetivo

Proteger el intercambio de información a través del uso de los medios de comunicación y transferencia de información de la entidad.

Detalle

La información de La ESE Hospital Psiquiátrico San Camilo relacionada con la topología de la red, el direccionamiento interno, así como las configuraciones y demás datos relacionados con las redes y sistemas de comunicación de la entidad, deberá ser información confidencial y estará bajo la responsabilidad del Área de Sistemas.

Todo intercambio de información o interacción entre sistemas de información con otras entidades, deberá estar soportado con el visto bueno del responsable de Seguridad de la Información y el Área de Sistemas.

Condiciones obligatorias

El Área de Sistemas se encargará de implementar herramientas de detección y protección para salvaguardar adecuadamente la información, garantizando así la confidencialidad, integridad y autenticidad de la información.

- Los usuarios serán responsables de no abandonar información sensible o crítica en los equipos de impresión, facsímiles, entre otros medios de reproducción.
- La ESE Hospital Psiquiátrico San Camilo establecerá acuerdos formales para el intercambio de información y de sistemas de información con otras entidades. Estos acuerdos serán de obligatorio cumplimiento.
- Cuando se requiera conectar la red o los sistemas de información de La ESE Hospital Psiquiátrico San Camilo con la red o sistemas de otra entidad, esta solicitud deberá ser estudiada y avalada por el Responsable de Seguridad de la Información, incluyendo un análisis de los posibles riesgos asociados y posteriormente debe escalarse con el Comité de Seguridad para su respectiva aprobación, considerando siempre la necesidad de apoyar la misión de La ESE Hospital Psiquiátrico San Camilo

Responsabilidades

- todos los funcionarios, colaboradores y terceros que transmitan información deberán cumplir la presente política.
- el responsable de seguridad de la información o persona delegada en coordinación con el área de sistemas, serán los responsables de implementar todos los controles de seguridad identificados para proteger la integridad, disponibilidad y confidencialidad de la información a ser transferida.
- el funcionario encargado de la transmisión de la información, velará porque se generen registros de las actividades realizadas, especialmente en los casos de tratarse de información confidencial o crítica de la entidad.

Procedimientos por área

Procedimiento de transferencia de información.

Controles por área

- Se implementarán herramientas y dispositivos de seguridad que permitan proteger la integridad, disponibilidad y confidencialidad de la información en el momento de ser transferida.
- La firma de los acuerdos de confidencialidad entre las partes, garantiza la total reserva de la información, así como los Alcances frente al tratamiento y divulgación de la información.

5.8 Política de desarrollo seguro de software

Alcance

Mantener la seguridad del software y sistemas de información desarrollados en La ESE Hospital Psiquiátrico San Camilo.

Objetivo

Establecer y aplicar reglas para el desarrollo de software y de sistemas de información, desarrollados al interior de la ESE hospital psiquiátrico san camilo.

Detalle

Para el desarrollo del software y de los sistemas de información seguro, es importante que los responsables y personas involucradas dentro del proceso tengan en cuenta lineamientos y buenas prácticas que permitan un adecuado manejo de la información y la preservación de un nivel de seguridad óptimo.

Condiciones obligatorias

Se planeará la metodología a utilizar y el cronograma de etapas del desarrollo del software o sistema de información, teniendo en cuenta los requerimientos de la Entidad y las necesidades para el cumplimiento misional institucional de La ESE Hospital Psiquiátrico San Camilo.

- Se deberá generar por parte de los usuarios autorizados las especificaciones funcionales y no funcionales de los sistemas de información, definiendo los requisitos sobre la calidad, seguridad y funcionalidad del código.
- Una vez se haya realizado el desarrollo del código, se deberá validar las condiciones y tipos de pruebas a realizar, con el fin de revisar la funcionalidad y requerimientos descritos, entre ellos los de seguridad

- La oficina de sistemas deberá validar los criterios de aceptación, con sus respectivas pruebas para detectar códigos maliciosos o troyanos, puertas traseras, entre otros.
- La ESE Hospital Psiquiátrico San Camilo realizará los acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual con respecto al desarrollo de los códigos fuentes y usabilidad contratados o desarrollados internamente.
- Todo cambio que se realice, deberá cumplir con la política de gestión de cambios, y así mismo con el procedimiento de control de cambios.

Responsabilidades

- El área de sistemas será la encargada de realizar la supervisión del desarrollo conforme a los parámetros planeados, requerimientos realizados, y criterios de aceptación.
- Los usuarios del software o sistemas de información, deberán realizar las solicitudes de desarrollo o modificación de manera formal al área de sistemas.

Procedimientos por área

- procedimiento de control de cambios.

Controles por área

- Se establecerá una metodología y cronograma de desarrollo, con el fin de conocer el Alcance y requerimientos detallados.
- El Área de Sistemas realizará la respectiva revisión de funcionamiento y documentación del código, así como los criterios de aceptación, con el fin de evitar vulnerar la seguridad de la Entidad.
- Se llevará a cabo un control de versiones por parte del desarrollador y las pruebas de funcionamiento necesarias, para asegurar el buen funcionamiento del software o sistema de información.

5.9 Política de seguridad de la información para relaciones con proveedores

Alcance

Minimizar los riesgos asociados al acceso de los activos de información por parte de los proveedores de la entidad.

Objetivo

Asegurar que los controles de seguridad asociados al acceso de los proveedores a los activos de información de la entidad, se implementen, operen y mantengan.

Detalle

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la entidad, el responsable de seguridad de la información o delegado y el propietario de la información, llevarán a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos.

Condiciones obligatorias

Para brindar el acceso a la información de la entidad por parte de proveedores, se deberá tener en cuenta los siguientes parámetros:

- El tipo de acceso requerido (físico/lógico y a qué recurso). o Los motivos para los cuales se solicita el acceso. o El valor de la información y su clasificación. o Los controles empleados por la tercera parte. o La incidencia de este acceso en la seguridad de la información. o Los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables, restringiendo los permisos a otorgar.
- En ningún caso se otorgará acceso a proveedores a las instalaciones de procesamiento o áreas críticas, hasta no haber implementado los controles de seguridad y se haya firmado un contrato o acuerdo que defina las condiciones de acceso.
- El responsable de la información, realizará un monitoreo y revisión de los servicios de proveedores para asegurar que se cumplan los términos y condiciones acordados
- Dentro de los contratos o acuerdos celebrados con los proveedores que requieran acceder a la información de la entidad, se deberá establecer el cumplimiento de

las políticas de seguridad, protección de activos, protección de datos, autorización de acceso, administración de cambios o aquellas consideradas relevantes para garantizar un adecuado aseguramiento de la información.

Responsabilidades

- todos los funcionarios, colaboradores y proveedores que tengan acceso a la información deberán cumplir con la presente política.
- el responsable de la información, deberá velar por el cumplimiento de los servicios contratados, así como requerimientos de controles específicos del resultado de la valoración de riesgos.
- No se permitirá el acceso a la información y sistemas de información de los proveedores antes de la firma del contrato o acuerdo que defina las condiciones para la conexión o acceso, así mismo, posterior a la implementación de los controles identificados como necesarios para la protección de la información.

Procedimientos por área

- procedimiento de transferencia de información

Controles por área

- Se implementarán los controles de seguridad identificados en el estudio de riesgos para asegurar la protección de la información.
- Se firmará los acuerdos de confidencialidad entre las partes, que garantiza la confidencialidad de la información, así como los Alcances frente al tratamiento y divulgación de la información.
- Se realizará monitoreo y revisión de los servicios para asegurar que se cumplan los términos y condiciones de seguridad, y el manejo apropiado de la información

5.10 Política de protección de datos personales

Alcance

Establecer las medidas necesarias para garantizar la seguridad de los datos de carácter personal, evitando su posible adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Objetivo

Garantizar la privacidad y protección adecuada de las bases de datos, los centros de tratamiento de información, equipos, sistemas, programas y personas que intervengan en el tratamiento de datos personales por medio de mecanismos de seguridad.

Detalle

Para el tratamiento de la información, donde se recopila la información de datos personales:

Atención: al ser atendido dentro de la institución, la primera información que se le solicitara, serán los datos personales para la creación de su atención.

Página web: es la información recopilada en los diferentes formularios existentes en la página web (quejas y reclamos, contratación, contáctenos, etc.).

Condiciones obligatorias

Los funcionarios deberán acceder únicamente a los datos que se requieran para el desarrollo de las funciones, guardando estricta reserva y no divulgarlos más allá de lo estrictamente necesario.

- Los funcionarios de la ESE hospital psiquiátrico san camilo no deberán retirar de la entidad ninguna clase de datos sin autorización expresa del responsable de seguridad y del responsable del archivo.
- Se deberán borrar periódicamente los archivos que contengan datos de carácter personal y que no sean requeridos para el desarrollo de las actividades dentro de la entidad.
- Los archivos que contengan datos de carácter personal, que vayan a ser desechados o reutilizados, deberán proteger la información mediante mecanismos de destrucción óptimos que impidan la recuperación de la información.
- Antes de generar archivos que contengan datos personales se deberá gestionar la autorización (evidenciable) de los titulares de los datos, en donde se establezca la finalidad y tipos de datos.
- El responsable de la información, será el encargado de decidir sobre la finalidad, contenido y uso de los datos personales, así como el tratamiento fuera de las instalaciones.

- El responsable de seguridad verificará que las medidas de seguridad física y lógica implementadas para proteger los datos de carácter personal sean acordes con las necesidades de la entidad y los riesgos identificados.

Responsabilidades

- Conocer y cumplir las políticas internas en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.
- Utilizar los controles y medidas que se hayan establecido para proteger tanto los datos de carácter personal como los propios sistemas de información y sus componentes.
- No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos, informar de posibles debilidades en los controles.

Procedimientos por área

- procedimiento de transferencia de información

Controles por área

- Los datos personales no se deberán transmitir a terceros o entidades que no proporcionen niveles adecuados de protección de datos, y los cuales no hayan sido autorizados para su tratamiento.
- Se realizarán auditorías periódicas para verificar el cumplimiento de los controles de seguridad, así como el cumplimiento de la presente política.
- La firma de los acuerdos de confidencialidad entre las partes, que garantiza la total reserva de la información, así como los Alcances frente al tratamiento de los datos personales.

5.11 Política de uso de internet

Alcance

Proteger la información de la entidad haciendo uso de buenas prácticas de seguridad en el uso del internet.

Objetivo

Generar los mecanismos apropiados para el buen uso del servicio de internet por parte de los funcionarios de la ESE hospital psiquiátrico san camilo, para la protección de la información de la entidad.

Detalle

Condiciones obligatorias

Las nuevas amenazas cibernéticas son uno de los principales riesgos de seguridad para los sistemas de información, por tal razón se deberán tomar las siguientes precauciones de seguridad sobre la utilización de internet:

- Todos los funcionarios de la ESE hospital psiquiátrico san camilo y sedes, tendrán la obligación a dar cumplimiento a la ley 679 de 2001, acatando las prohibiciones que le han sido impuestas. por consiguiente se obligan a no utilizar los servicios, redes y sistemas de la ESE hospital psiquiátrico san camilo que impliquen directa o indirectamente, bajar o consultar información de actividades sexuales y/o material pornográfico.
- El spam o correo basura son los mensajes no deseados que hacen referencia a publicidad pudiendo además contener virus; estos mensajes deberán eliminarse sin ser leídos para evitar el aumento de la cantidad del correo basura en el buzón así como la posibilidad de intrusión de virus en el sistema.
- Se usará regularmente el antivirus para revisar la información procedente de internet y se verificará periódicamente su actualización, con la colaboración del área de sistemas, quienes prestarán apoyo para tal fin.
- El área de sistemas activará las actualizaciones de los sistemas de información de forma automática, las cuales contribuyen con la protección de los equipos ante ataques de virus provenientes de internet.

Usos no autorizados

- No se utilizará canales de chat o grupos sociales como Facebook, YouTube, Google+, etc., en horario laboral con fines personales sin previa autorización del ESE hospital psiquiátrico san camilo.
- no se descargará de internet, ni se alojará en los discos duros de los equipos de cómputo información como música, videos, ni software sin licencia (a nombre de la ESE hospital psiquiátrico san camilo).
- No se descargará información de sitios web de los que no se tenga referencias de seriedad, o que no sean medianamente conocidos. si se descarga información, archivos, los mismos se deberán revisar con el antivirus actualizado antes de realizar cualquier tipo de actividad.

- No se podrá realizar el intercambio de información de propiedad de la ESE hospital psiquiátrico san camilo y/o de sus funcionarios con terceros, a menos que exista una autorización por parte del responsable del archivo o en su defecto el responsable de seguridad de la información o contrato de por medio que autorice el intercambio de información.

Responsabilidades

- Los funcionarios de la ESE hospital psiquiátrico san camilo son responsables del uso adecuado de los recursos y en ningún momento pueden realizar prácticas ilícitas o mal intencionadas que atenten contra terceros o contra los lineamientos de seguridad de la información.
- El área de sistemas, serán los encargados de velar por el cumplimiento de la presente política haciendo uso de monitoreo del servicio e implementación de los mecanismos de seguridad adecuados.
- El área de sistemas en coordinación con el área de talento humano serán los encargados de capacitar a todos los funcionarios de la ESE hospital psiquiátrico san camilo y sedes en buenas prácticas de seguridad

Procedimientos por área

- Procedimiento de creación, modificación y cancelación de usuarios y privilegios.

Controles por área

- Monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros.
- Se contará con las herramientas adecuadas para controlar el acceso y navegación de Internet.
- Eliminación periódica de las cookies y archivos temporales almacenados en los navegadores de los funcionarios de La ESE Hospital Psiquiátrico San Camilo.

5.12 Política de uso de correo electrónico

Alcance

Asegurar la integridad, disponibilidad y confidencialidad de la información contenida o emitida del correo electrónico institucional de los funcionarios de la ESE hospital psiquiátrico san camilo.

Objetivo

Generar los controles necesarios para preservar la disponibilidad, integridad y disponibilidad de la información de la entidad transmitida, recibida y/o almacenada en el correo electrónico.

Detalle

Condiciones obligatorias

- El usuario y contraseña del correo electrónico de cada funcionario de La ESE Hospital Psiquiátrico San Camilo es personal e intransferible, por lo tanto el uso y manejo es responsabilidad absoluta del funcionario.
- La información emitida y transmitida por el correo electrónico de cada funcionario es responsabilidad única y exclusiva del usuario.
- En el caso de que a cualquier usuario le llegue una comunicación o correo electrónico sospechoso, de alguien desconocido o spam, deberá reportarlo de inmediato, sin abrirlo, al correo electrónico de soporte de La ESE Hospital Psiquiátrico San Camilo.
- La ESE Hospital Psiquiátrico San Camilo y sedes e reserva el derecho a auditar y vigilar los correos electrónicos institucionales para garantizar que sea utilizada sólo para propósitos laborales. Estas auditorías se realizarán periódicamente, al azar o cuando exista una investigación sobre una situación en particular.
- En caso que un usuario olvide su contraseña deberá notificarlo al área de sistemas para su recuperación o cambio.
- El servicio de correo electrónico sólo estará vigente mientras los funcionarios tengan relación laboral con la entidad, una vez culmine la relación el Área de Sistemas eliminará los accesos después de recibido el comunicado del área de Talento Humano.

Usos no autorizados

- Se prohíbe el envío por fuera de la Entidad de información confidencial por medio del correo electrónico sin autorización o el consentimiento del remitente original.
- No se utilizará la cuenta de correo electrónico suministrada por el La ESE Hospital Psiquiátrico San Camilo, para asuntos personales.
- Se prohíbe el envío de mensajes de correo electrónico en donde se divulgue, comente o exprese hechos, opiniones o asuntos internos del La ESE Hospital Psiquiátrico San Camilo que puedan afectar la reputación, seguridad e imagen de la Entidad.
- No se permitirá a terceras personas leer, revisar, interceptar, modificar o destruir información relacionado con los funcionarios o la entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación.
- Se prohíbe el envío de correos electrónicos con material ofensivo, ilegal o pornográfico o de cualquier otra índole no autorizada.
- Se prohíbe a los funcionarios suscribirse a listas de correo electrónico o grupos de noticias que divulguen información o mensajes ajenos a las funciones y deberes de la Entidad sin la debida autorización.
- No se podrá hacer uso de comunicaciones para propósito personal o asunto privado del funcionario o para el recibo y envío de mensajes en cadena, redes sociales, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro asunto o servicio no oficial o ajeno a las funciones laborales de La ESE Hospital Psiquiátrico San Camilo

Responsabilidades

- Los funcionarios de La ESE Hospital Psiquiátrico San Camilo deberán conocer y cumplir la presente política y las buenas prácticas de seguridad relacionadas con el uso del correo electrónico institucional.
- No se deberá ceder ni comunicar a otros la contraseña; los funcionarios serán responsables ante la entidad de todos los accesos y actividades que se puedan haber realizado con su usuario y contraseña.
- Cada uno de los usuarios será el encargado de hacer copias de respaldo o Backus en su buzón de correo electrónico, así como depurar periódicamente la información contenida en el mismo.

Procedimientos por área

- Procedimiento de Creación de correo electrónico institucional

Controles por área

- Se realizarán auditorías periódicas para verificar el cumplimiento de los controles de seguridad, así como el cumplimiento de la presente política.
- El Área de Sistemas realizara la asignación de contraseñas, garantizando un nivel de complejidad para la generación de las mismas.
- Se realizarán capacitaciones de buenas prácticas del uso de los recursos de la entidad, en donde se desarrollen temas acerca del uso adecuado del correo electrónico institucional.

5.13 Política de acceso y redes sociales

Alcance

Minimizar los riesgos asociados al acceso o emisión de información no autorizada de la entidad por medio de redes sociales.

Objetivo

Asegurar que los controles de seguridad asociados al uso de las redes sociales brinden la protección adecuada a los activos de información de la entidad

Detalle

Usos no autorizados

- No se utilizará canales de chat o grupos sociales como Facebook, YouTube, Google+, etc., en horario laboral con fines personales sin previa autorización del ESE hospital psiquiátrico san camilo, el área de comunicación será el responsable de manejar los canales de redes sociales con la imagen institucional de la entidad.
- No se deberá publicar información confidencial o perteneciente a la ESE hospital psiquiátrico san camilo que pueda afectar la imagen de la entidad.
- Si algún funcionario de la ESE hospital psiquiátrico san camilo observa información pública de la entidad que pueda estar afectando la imagen de la ESE hospital psiquiátrico san camilo, se deberá comunicar al área de comunicaciones para que realice los trámites pertinentes frente a la misma.

- Los funcionarios beberán ser cauteloso en el uso de las redes sociales, teniendo en cuenta que son fuentes usadas para hurto de información, y de explotación de vulnerabilidades de seguridad.
- Cuando un funcionario de la ESE hospital psiquiátrico san camilo se encuentre navegando en una red social autorizada, deberá ser cuidadoso al dar clic en enlaces publicados en los muros, teniendo en cuenta que allí se albergan la mayoría del software malicioso, acción que puede poner en peligro la información de la entidad

Responsabilidades

- Todos los funcionarios deberán cumplir la presente política.
- Todo empleado está obligado a informar por escrito la oficina de sistemas, sobre cualquier situación, incidente o problema de seguridad identificado.

Procedimientos por área

- Procedimiento de creación, modificación y cancelación de usuarios y privilegios.

Controles por domino

El Área de Sistemas realizará auditorías y supervisión del uso de los recursos tecnológicos.

5.14 Política de actualización de hardware

Alcance

Generar una planeación de la infraestructura del conforme los requerimientos funcionales y misionales de la institución.

Objetivo

Asegurar el buen funcionamiento de la infraestructura tecnológica de la ESE hospital psiquiátrico san camilo en un escenario futuro, acorde con el cumplimiento de la misión y procesos críticos institucionales.

Detalle

- Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, monitor, teclado, mouse, adición de memoria o tarjetas)

debe tener previamente una evaluación técnica del área de sistemas, el supervisor de mantenimiento y la autorización del responsable de manejo de bienes para la actualización de seriales y hojas de vida de mantenimiento de los equipos

- La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal capacitado, previa autorización.
- Los equipos de cómputo (pc, servidores, comunicaciones, etc.) no deben moverse o reubicarse sin previa autorización de la oficina de sistemas.

Responsabilidades

- Todos los funcionarios deberán cumplir la presente política.
- Todo empleado está obligado a solicitar por escrito a la oficina de sistemas, cualquier movimiento o modificación que se lleve a cabo con los equipos.
- Los funcionarios y contratistas que realicen las labores de administración del recurso informático son responsables por la implementación y permanencia de los controles sobre los recursos tecnológicos.
- El área de sistemas, deberá velar por la seguridad de todos los equipos de la entidad.
- El área de sistemas está encargada de diseñar y ejecutar planes de mantenimiento preventivo a los equipos de la ESE hospital psiquiátrico san camilo.

Procedimientos por área

- Procedimiento de mantenimiento de equipos

Controles por área

- Se llevará a cabo un inventario actualizado de bienes tecnológicos, en donde se establezca por lo menos la ubicación, responsable y características generales del Equipo.
- Se desarrollarán planes de mantenimiento preventivo de los equipos con motivo de identificar posibles fallas de funcionamiento.

5.15 Política de gestión de medios removibles

Alcance

Establecer el uso adecuado de los medios removibles durante la vida útil del equipo en la entidad.

Objetivo

Asegurar el uso, reutilización y eliminación de medios removibles, con el fin de garantizar que la información se salvaguarde adecuadamente.

Detalle

- El uso de medios de dispositivos removibles (ejemplo: CD, DVD, Blu-ray, USB, discos duros externos, celulares) en La ESE Hospital Psiquiátrico San Camilo, solo serán autorizados por la Gerencia para los funcionarios cuyo perfil del cargo y funciones lo requiera, y serán controlados por el Área de sistemas.
- El contenido de medios reutilizables que contengan información crítica o sensible de la Entidad que se van a retirar de las instalaciones se les deberá realizar un borrado seguro con el fin de evitar recuperación de información. Para el retiro de dichos medios se debe contar con la autorización del Área de Sistemas.
- Los funcionarios de ESE Hospital Psiquiátrico San Camilo no podrán utilizar los puertos USB para guardar o extraer información de los equipos de la institución sin previa autorización de la Gerencia.

Responsabilidades

- Todos los funcionarios deberán cumplir la presente política.
- Los funcionarios del Área de Sistemas serán los encargados de efectuar las copias de respaldo frente a la solicitud realizada por los funcionarios de La ESE Hospital Psiquiátrico San Camilo frente a la reutilización y eliminación de los medios removibles.

Procedimientos por área

- Procedimiento de Mantenimiento de Equipos.

Controles por área

- Se realizará un borrado seguro a los equipos al momento de reutilizar o eliminar medios removibles.
- El Área de Sistemas controlará la distribución y uso de los medios removibles de La ESE Hospital Psiquiátrico San Camilo.

- Se desactivaran los puertos USB de los equipos para la lectura y escritura de medios USB removibles.

5.16 Política de Cambio de Contraseñas

Alcance

Esta política aplica a todos los usuarios que tienen acceso a los sistemas de información del Hospital Psiquiátrico San Camilo, incluyendo empleados, contratistas, proveedores y cualquier otra persona con credenciales de acceso.

Objetivos

- Garantizar la confidencialidad, integridad y disponibilidad de la información del hospital.
- Reducir el riesgo de acceso no autorizado a los sistemas y datos.
- Promover una cultura de seguridad de la información entre los usuarios.
- Cumplir con las normativas y estándares de seguridad aplicables al sector salud.

Detalles de Acciones

Requisitos de complejidad:

- Las contraseñas deben tener una longitud mínima de 12 caracteres.
- Deben incluir una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
- No se permiten contraseñas basadas en información personal (nombres, fechas de nacimiento, etc.) o palabras comunes.
- No se permite la reutilización de contraseñas anteriores.

Cambio periódico:

- Las contraseñas deben cambiarse cada 90 días como máximo.
- Se requerirá un cambio inmediato en caso de sospecha de compromiso de la cuenta.

Bloqueo de cuentas:

- Las cuentas se bloquearán después de 5 intentos fallidos de inicio de sesión.
- El desbloqueo requerirá la intervención del personal de soporte técnico.

Gestión de contraseñas:

- Se recomienda el uso de gestores de contraseñas para generar y almacenar contraseñas seguras.
- Las contraseñas no deben compartirse ni almacenarse en lugares inseguros (notas adhesivas, documentos no cifrados, etc.).

Autenticación Multifactorial (MFA):

- Implementar MFA siempre que sea posible para agregar una capa adicional de seguridad.

Responsabilidades

Usuarios:

- Cumplir con esta política y cambiar sus contraseñas según lo requerido.
- Proteger sus contraseñas y no compartirlas con nadie.
- Reportar cualquier incidente de seguridad o sospecha de compromiso de la cuenta.

Departamento de TIC:

- Implementar y mantener los sistemas de gestión de contraseñas.
- Monitorear el cumplimiento de esta política.
- Proporcionar soporte técnico a los usuarios.
- Realizar auditorías periódicas de las políticas de seguridad.

Oficial de Seguridad de la Información (CISO):

- Desarrollar y mantener esta política.
- Realizar evaluaciones de riesgos y auditorías de seguridad.
- Capacitar a los usuarios en seguridad de la información.

Procedimientos

Cambio de contraseña:

- Los usuarios pueden cambiar sus contraseñas a través del portal web del hospital o contactando al departamento de TI.
- El sistema guiará a los usuarios a través del proceso y verificará el cumplimiento de los requisitos de complejidad.

Restablecimiento de contraseña:

- En caso de olvido de la contraseña, los usuarios pueden solicitar un restablecimiento a través del portal web o contactando al departamento de TI.
- El proceso de restablecimiento requerirá la verificación de la identidad del usuario.

Reporte de incidentes:

- Los usuarios deben reportar cualquier incidente de seguridad o sospecha de compromiso de la cuenta al área de TIC.

Controles

Auditorías periódicas:

- Se realizarán auditorías periódicas para verificar el cumplimiento de esta política y la efectividad de los controles.

Monitoreo de registros:

- Se monitorearán los registros de acceso a los sistemas para detectar actividades sospechosas.

Pruebas de penetración:

- Se realizarán pruebas de penetración periódicas para identificar vulnerabilidades en los sistemas.

Capacitación y concientización:

- Se proporcionará capacitación y concientización continua a los usuarios sobre seguridad de la información y buenas prácticas de contraseñas.

Consideraciones Adicionales:

- Es crucial que esta política se comunique claramente a todos los usuarios y que se proporcione capacitación sobre su implementación.
- Se recomienda revisar y actualizar esta política periódicamente para adaptarla a las nuevas amenazas y tecnologías.
- Es importante que la ESE Hospital Psiquiátrico San Camilo, se apegue a la normatividad Colombiana vigente, con respecto a la protección de datos personales, y las normas que regulan la seguridad informática en el sector de la salud.

5.17 Política de Redes

Alcance

Esta política se aplica a todas las redes de datos del Hospital Psiquiátrico San Camilo, incluyendo redes cableadas, inalámbricas, VPN y cualquier otro medio de conexión a la infraestructura de red del hospital. También aplica a todos los dispositivos conectados a estas redes, ya sean propiedad del hospital o de los usuarios.

Objetivos

- Garantizar la disponibilidad, integridad y confidencialidad de la información transmitida a través de las redes del hospital.
- Proteger la infraestructura de red contra accesos no autorizados, ataques cibernéticos y otras amenazas.
- Establecer lineamientos claros para el uso adecuado de los recursos de red.
- Cumplir con las normativas y estándares de seguridad aplicables al sector salud.

Detalles de Acciones

Segmentación de la red:

- Implementar segmentación de la red para separar el tráfico de diferentes áreas funcionales (por ejemplo, red de pacientes, red administrativa, red de investigación).
- Utilizar Blas y firewalls para controlar el acceso entre segmentos de red.

Acceso inalámbrico:

- Implementar redes Wi-Fi seguras con cifrado WPA2/WPA3.
- Utilizar autenticación fuerte para el acceso a la red Wi-Fi.
- Establecer una red Wi-Fi separada para invitados.

Acceso remoto:

- Utilizar VPNs seguras para el acceso remoto a la red del hospital.
- Implementar autenticación multifactorial (MFA) para el acceso VPN.
- Restringir el acceso remoto a los recursos necesarios.

Firewalls e IDS/IPS:

- Implementar firewalls para controlar el tráfico de red entrante y saliente.

- Utilizar sistemas de detección y prevención de intrusiones (IDS/IPS) para detectar y bloquear ataques cibernéticos.

Monitoreo de la red:

- Implementar herramientas de monitoreo de red para detectar anomalías y actividades sospechosas.
- Registrar y analizar los registros de eventos de seguridad.

Actualizaciones y parches:

- Mantener actualizados todos los dispositivos de red y software con los últimos parches de seguridad.

Uso aceptable:

- Definir políticas de uso aceptable de la red que prohíban actividades ilegales, no autorizadas o que puedan comprometer la seguridad de la red.

Responsabilidades

Departamento de TI:

- Implementar y mantener la infraestructura de red.
- Monitorear la seguridad de la red.
- Responder a incidentes de seguridad.
- Aplicar parches y actualizaciones.

Usuarios:

- Cumplir con las políticas de uso aceptable de la red.
- No conectar dispositivos no autorizados a la red.
- Reportar cualquier incidente de seguridad o actividad sospechosa.

Oficial de Seguridad de la Información (CISO):

- Desarrollar y mantener las políticas de seguridad de la red.
- Realizar evaluaciones de riesgos y auditorías de seguridad.
- Capacitar a los usuarios en seguridad de la red.

Procedimientos

Gestión de cambios:

- Implementar un proceso de gestión de cambios para cualquier modificación en la infraestructura de red.

Respuesta a incidentes:

- Desarrollar un plan de respuesta a incidentes de seguridad de la red.
- Realizar simulacros de respuesta a incidentes.

Evaluación de vulnerabilidades:

- Realizar evaluaciones de vulnerabilidades periódicas de la infraestructura de red.

Controles

Auditorías de seguridad:

- Realizar auditorías de seguridad periódicas de la red para verificar el cumplimiento de las políticas y la efectividad de los controles.

Pruebas de penetración:

- Realizar pruebas de penetración periódicas para identificar vulnerabilidades en la red.

Monitoreo de registros:

- Monitorear los registros de eventos de seguridad de la red para detectar actividades sospechosas.

Consideraciones Adicionales:

- Es fundamental que esta política se comunique claramente a todos los usuarios y que se proporcione capacitación sobre su implementación.
- Se recomienda revisar y actualizar esta política periódicamente para adaptarla a las nuevas amenazas y tecnologías.

6. PROCESOS RELACIONADOS

Aplica para todos los Procesos Institucionales, de la ESE Hospital Psiquiátrico San Camilo.

7. REQUISITOS LEGALES APLICABLES

a. Ley 599 DE 2000 la cual expide el Código Penal. crea el bien jurídico de los derechos de autor e incorporo conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.
b. Norma ISO/IEC 27001:2005 establece la evolución certificable del código de buenas prácticas ISO 17799 y Define cómo organizar la seguridad de la información en cualquier

tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Esta norma constituye la base para la gestión de la seguridad de la información.

c. Ley 1273 DE 2009 por medio de la cual se modificó el Código Penal, Crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
d. Ley 1341 DE 2009, la cual define principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
e. Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013 tiene por objeto desarrollar el derecho constitucional que tienen todas las personas de conocer, actualizar y rectificar las informaciones que se hallan recogido sobre ellas en bases de datos o archivos, y los demás derechos Por la cual se dictan disposiciones generales para la protección de datos personales.
f. Decreto 2693 de 2012 la cual establece los Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, reglamenta parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
g. Decreto 2578 de 2012 que reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones.
h. Decreto 2609 de 2012 mediante el cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos

8. DESCRIPCION DEL PLAN

El Plan de Seguridad de la Información de La ESE Hospital Psiquiátrico San Camilo, tiene como fin primordial brindar las herramientas apropiadas para dar cumplimiento a los principios integridad, disponibilidad y confiabilidad de la información, por medio de las políticas de seguridad de la información, en donde se describen las responsabilidades de los usuarios,

custodios y propietarios de la información, al igual que objetivos de protección que permitan reducir el impacto en caso tal que ocurra un incidente de seguridad de la información.

La implementación del presente plan tiene como fin minimizar las vulnerabilidades y amenazas accidentales o intencionales que puedan facilitar la divulgación, modificación, destrucción o uso ilícito o indebido de los activos de información, y al mismo tiempo, son lineamientos de uso para las áreas responsables de los servicios, activos y sistemas de la Entidad.

8.1 Matriz de seguridad de la información

La coordinación del proceso de gestión de la información, el área de sistemas (TIC) y el subproceso de gestión documental, realizaron la elaboración de la matriz de seguridad de la información conforme a los lineamientos establecidos en la norma internacional ISO 27001;2020, incluyendo las mejores prácticas de seguridad para la institución apoyado en los controles de seguridad allí establecidos.

Anexo: Matriz de riesgos de seguridad de la información Código: AD-GIT-TIC-P-02-R-

8.2 Acerca de la seguridad de la información

En la ESE Hospital Psiquiátrico San Camilo la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, en la ESE Hospital Psiquiátrico San Camilo implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

8.3 Organización para la seguridad de la información

El Comité de Seguridad tendrá la potestad de modificar la Política Global o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

8.4 Alcance del plan de gestión de seguridad de la información

La ESE Hospital Psiquiátrico San Camilo a través de su política de seguridad de la información, dicta el cumplimiento de disposiciones que tienen con objeto gestionar adecuadamente la seguridad de la información, la gestión de activos, la gestión de riesgos y Continuidad del negocio, por tal motivo deberán ser conocida y cumplida por todo el personal (funcionarios, colaboradores y terceros) que accedan a la información de la entidad, sistemas de información e instalaciones físicas

8.5 Definiciones

Seguridad Informática: Procesos, actividades, mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

Seguridad de la información: Son todos los controles técnicos y metodológicos que permiten mitigar los riesgos a los que se expone la información

Confidencialidad: La propiedad que esa información esté disponible y no sea divulgada a personas o procesos no autorizados.

Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos.

Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Activo: Cualquier cosa que tenga valor para la organización

Amenaza: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir daño (material o inmaterial) sobre los elementos (activos, recursos) de un sistema.

Vulnerabilidad: Son la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

Activos de información: Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

8.6 Orientación de la dirección para la gestión de seguridad de la información

El Plan de Seguridad de la Información de la ESE Hospital Psiquiátrico San Camilo, tiene como objetivo principal, establecer los lineamientos, procedimientos y buenas prácticas para conservar la integridad, confidencialidad y disponibilidad de la información, características Esenciales de Seguridad. Por tal motivo, La ESE Hospital Psiquiátrico San Camilo, para la prestación de sus servicios y conforme los requisitos y funciones determinados por el Estado y la satisfacción de las partes interesadas (usuarios, entidades de control, sociedad y terceras partes), busca por medio del liderazgo y compromiso de la Alta Dirección y su equipo de trabajo, asegurar la mejora continua de la eficacia, eficiencia y efectividad del plan de seguridad de la información.

Para tal fin, la Alta Dirección deberá apoyar los siguientes aspectos:

- Asegurar que los objetivos de la seguridad de la información se encuentren alineados con los objetivos de la ESE Hospital Psiquiátrico San Camilo.
- Revisar y aprobar periódicamente la política de seguridad de la información de la ESE Hospital Psiquiátrico San Camilo y sedes
- Velar porque las acciones de seguridad de la información sean ejecutadas de acuerdo a las políticas y lineamientos establecidos. Las mismas serán monitoreadas, reportadas y registradas en caso tal que exista una violación a las políticas y/o controles.
- Proporcionar los recursos necesarios para el desarrollo e implementación de iniciativas de seguridad de la información.

Conformar un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del plan de Seguridad de la Información de la ESE Hospital Psiquiátrico San Camilo.

9. SEGUIMIENTO Y EVALUACIÓN

El área de sistemas será el responsable por la revisión anual del presente plan, para lo cual deberá oportunamente informar a la oficina de Sistemas integrados de gestión las modificaciones propuestas, con base en las necesidades de actualización que surjan de la operación del día y teniendo en cuenta las sugerencias presentadas por los colaboradores de la ESE Hospital Psiquiátrico San Camilo.

Una vez aprobadas las modificaciones se autorizará la puesta en vigencia de la nueva versión del presente plan.

El presente Plan entrará en vigencia en la fecha de su aprobación, por parte de sistemas y deroga y sustituye todas las políticas anteriores vigentes hasta la fecha de aprobación del presente manual. El Plan de Seguridad de la Información tendrá seguimiento a través de indicadores de eficacia en cada una de las metas propuestas para la vigencia, y control para el desarrollo de las actividades por medio de la matriz de actividades

Anexo: Matriz Programación De Actividades Planes Institucionales Código: CODIGO: ES-PLI- P-01-R-03

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Erwing Jesid Dávila García **Profesional Grado II** Juan Gabriel Rojas Gómez **Coordinador de Archivo**	Edgar Albarracín Cogollo **Subdirector Administrativo**	Natalia Sofía Ojeda Ortiz. **Gerente**
FECHA:30/01/2025	FECHA:30/01/2025	FECHA:30/01/2025