PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FECHA DE ELABORACION	ELABORADO POR	REVISADO POR	APROBADO POR
13/01/2023	Ingeniero de Sistemas	Asesor de Calidad	Gerente

TABLA DE CONTENIDO

1. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4
2. ALCANCE 6
3. ROLES Y RESPONSABILIDADES 7
4. IMPLEMENTACIÓN DE PLANES DE SEGURIDAD DE LA INFORMACIÓN 8
4.1 Justificación 8
2.2 Objetivo 9
2.3 Roles y Responsabilidades 10
2.4 Cumplimiento 10
2.5 Comunicación 10
2.6 Monitoreo 11
5. 3. DESCRIPCIÓN DE LOS PLANES 11
3.1 Gestión de Activos 11
3.1.1 Plan para la identificación, clasificación y control de activos de información 11
Pautas para tener en cuenta 12
3.2 Control de Acceso 12
3.2.1 Plan de acceso a redes y recursos de red 12
Pautas para tener en cuenta 13
3.2.2 Plan de administración de acceso de usuarios 13
Pautas para tener en cuenta 13
3.2.3 Plan de control de acceso a sistemas de información y aplicativos 14
Pautas para tener en cuenta 14
3.2.4 Planes de seguridad física 15
Pautas para tener en cuenta 15
3.2.5 Plan de seguridad para los equipos 16
Pautas para tener en cuenta 16
3.2.6 Plan de uso adecuado de internet 18
Pautas para tener en cuenta 18
6. 4. PRIVACIDAD Y CONFIDENCIALIDAD 19
4.1 Plan de tratamiento y protección de datos personales 19

Pautas para tener en cuenta.....20
4.2 Disponibilidad del servicio e información.....21
4.2.1 Plan de continuidad, contingencia y recuperación de la información 21
Pautas para tener en cuenta.....22
7. SEGUIMIENTO Y EVALUACIÓN 23
8. SEGUIMIENTO CONTROL Y MEJORA 23

1. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección del HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, este plan aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus pacientes y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las Planes, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E
- Garantizar la continuidad del negocio frente a incidentes.
- El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E 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.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E:

1. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E 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.

2. Las responsabilidades frente a la seguridad de la información serán **definidas, compartidas, publicadas y aceptadas** por cada uno de los empleados, proveedores, socios de negocio o terceros.

3. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E **protegerá la información generada, procesada o resguardada** por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en subcontratación.

4. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E protegerá su información de las amenazas originadas por parte del personal.

6. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E implementará control de acceso a la información, sistemas y recursos de red.

9. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

12. El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

2. ALCANCE

El presente plan de Seguridad de la Información se dicta en cumplimiento de las disposiciones Jurídicas vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Hospital Departamental de Granada E.S.E.

En consecuencia, El HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E., en su búsqueda de fortalecer la seguridad de la información generada en el desarrollo de los procesos de la institución, con el fin de preservar la **INTEGRIDAD, CONFIDENCIALIDAD, DISPONIBILIDAD Y PRIVACIDAD DE LOS ACTIVOS DE INFORMACIÓN** mediante el Modelo de Seguridad y Privacidad de la Información **(MSPI)** paralelo con el Sistema de Gestión de Seguridad de la Información **(SGSI)**, para mejorar la prestación de los servicios. La PLAN de Seguridad de la Información es de obligatorio cumplimiento y aplica a todos los funcionarios, contratistas y demás partes interesadas en EL HOSPITAL DEPARTMENTAL DE GRANADA E.S.E., que en ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, tengan acceso a los activos de información de la entidad.

OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI

- Establecer Planes y procedimientos relacionados con la seguridad y privacidad de la información Implementando herramientas de seguridad informática que permitan proteger la información almacenada.

- Identificar los activos de información del HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E. y definir las responsabilidades de protección adecuadas.

- Definir los niveles adecuados de protección de la información de acuerdo con el grado de importancia para el HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E., teniendo en cuenta la integridad, confidencialidad, disponibilidad y privacidad de la misma.

- Establecer un plan de comunicación y sensibilización para fomentar una cultura de seguridad y privacidad de la información en los funcionarios, contratistas y demás partes interesadas de la entidad.

- Garantizar los procedimientos de archivo y custodia, para velar por el trámite y almacenamiento de datos.

- Establecer, mantener, documentar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información MSPI alineado al Sistema de Gestión de la Seguridad de la Información del HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E. de acuerdo con los requisitos legales y normativos.

- Identificar, analizar, valorar y tratar los riesgos de los activos de información, Promoviendo la gestión ética de la información y la confidencialidad de los datos derivados de las atenciones en salud.

- Implementar el Plan de tratamiento de riesgos de seguridad de la información para determinar los controles que mitiguen la materialización de riesgos de Seguridad de la Información.

3. ROLES Y RESPONSABILIDADES

Todos los funcionarios, contratistas y demás partes son responsables de la seguridad de la información; adicionalmente, se establecen los siguientes roles y responsabilidades:

El Comité Institucional COMUNICACIONES tiene la responsabilidad de impulsar la implementación del Modelo de Seguridad de la Información alineado al Sistema de Gestión de Seguridad de la Información SGSI en el HOSPITAL DEPARTAMENTAL DE GRANADA E.S.E., además de realizar el seguimiento y /o verificación de la implementación de este.

La Oficina **GESTION DE LA INFORMACION** será la responsable del funcionamiento del Modelo de Seguridad y Privacidad de la Información y tendrá la responsabilidad de coordinar la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información MSPI

Los **Propietarios de la Información** son responsables de clasificarla de acuerdo con el grado de sensibilidad de esta, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El **responsable del Área de Recursos Humanos** o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa, de sus obligaciones respecto del cumplimiento del plan de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.

El **Usuario de la Información**, es el funcionario, contratista y/o tercero autorizado para utilizar la información en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales o vigencia del respectivo contrato y es el responsable del buen uso de los activos de información durante el cumplimiento de sus labores o compromisos, según de quien se trate.

4. IMPLEMENTACIÓN DE PLANES DE SEGURIDAD DE LA INFORMACIÓN

4.1 Justificación

El Hospital Departamental de Granada E.S.E. con el propósito de salvaguarda la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve un plan de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

a) **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

b) **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

c) **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

a) **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

b) **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

c) **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

d) Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

e) Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes definiciones:

a) Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

b) Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

c) Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2 Objetivo

Definir los mecanismos y todas las medidas necesarias por parte del Hospital Departamental de Granada E.S.E., tanto técnica, lógica ,física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2.2 Alcance

Este Plan de Seguridad y Privacidad de la Información y su PLAN, son aplicables a todos los funcionarios del Hospital Departamental de Granada E.S.E., a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

2.3 Roles y Responsabilidades

Es responsabilidad del *Comité de Gestión y Desempeño* del Hospital Departamental de Granada E.S.E., la implementación, aplicación, seguimiento y autorizaciones del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso del plan de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

El Comité de Gestión y Desempeño cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

1. El Gerente de Hospital Departamental de Granada E.S.E., quien lo presidirá.
2. Subgerente Administrativo, quien actuará como secretario técnico.
3. Subgerente de Atención al Usuario
4. Subgerente Asistencial
5. Asesor de Planeación o quien haga sus veces
6. Asesor de Calidad
7. Gestor de Talento Humano
8. Asesor de Control Interno quien tendrá voz pero no voto

Este comité deberá revisar y actualizar este plan anualmente presentando las propuestas a la alta dirección para su aprobación.

2.4 Cumplimiento

El cumplimiento del plan de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este Plan, El Hospital Departamental de Granada E.S.E. se reserva el derecho de tomar las medidas correspondientes.

2.5 Comunicación

Mediante socialización a todos los funcionarios del Hospital Departamental de Granada E.S.E. se dará a conocer el contenido del documento de las Planes de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al Plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las Planes, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Calidad para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.hospitalgranada.gov.co

2.6 Monitoreo

Se crearán los mecanismos y los indicadores correspondientes al plan de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

5. 3. DESCRIPCIÓN DE LAS PLANES

Generalidades

El Hospital Departamental de Granada E.S.E. en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo con este plan se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la PLAN de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en El Hospital Departamental de Granada E.S.E.

3.1 Gestión de Activos

3.1.1 PLAN para la identificación, clasificación y control de activos de información

El Hospital Departamental de Granada E.S.E. a través del Comité de Gestión y Desempeño realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a Gestión de la Información y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

La subgerencia Administrativa tendrá la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.

Pautas para tener en cuenta

a) Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

b) La información física y digital del Hospital Departamental de Granada E.S.E. debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo con la disposición final definida por la entidad.

c) Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; así mismo, recoger de las impresoras, escáneres, fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionado.

d) Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

e) La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

3.2 Control de Acceso

3.2.1 PLAN de acceso a redes y recursos de red

El Ingeniero de sistemas del Hospital Departamental de Granada E.S.E., como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico y físicos.

Pautas para tener en cuenta

a) El proceso Gestión de la Información debe asegurar que las redes inalámbricas del Hospital Departamental de Granada E.S.E. cuenten con métodos de autenticación que evite accesos no autorizados.

b) El proceso Gestión de la Información debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red del Hospital Departamental de Granada E.S.E., así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Planes de Seguridad de la Información por parte de estos.

c) Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos del Hospital Departamental de Granada E.S.E., deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de Confidencialidad firmado previamente.

d) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos del Hospital Departamental de Granada E.S.E. deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

3.2.2 PLAN de administración de acceso de usuarios

El Hospital Departamental de Granada E.S.E. establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Pautas para tener en cuenta

a) El proceso Gestión de la información, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información del Hospital Departamental de Granada E.S.E.; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

b) El proceso Gestión de la información, debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera

oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

c) El proceso Gestión de la información debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

d) Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, juntamente con el proceso Gestión de la información, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

e) Los propietarios de los activos de información deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

3.2.3 PLAN de control de acceso a sistemas de información y aplicativos

El Hospital Departamental de Granada E.S.E. como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El proceso Gestión de la información, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Pautas para tener en cuenta

a) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

b) Los propietarios de los activos de información deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

c) El proceso Gestión de la información debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos del Hospital Departamental de Granada E.S.E.

d) El proceso Gestión de la información debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

e) El proceso Gestión de la información debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

f) Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

g) Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

h) Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el daño.

3.2.4 Planes de seguridad física

El Hospital Departamental de Granada E.S.E. provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

El proceso Gestión la información mantiene las normas, controles y registros de acceso a dichas áreas.

Pautas para tener en cuenta

a) Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por funcionarios que apoyan el proceso Gestión de la

información autorizada; no obstante, los visitantes siempre deberán estar acompañados de un funcionario.

b) El proceso Gestión de la información debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

c) La Subgerencia Administrativa debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones del Hospital Departamental de Granada E.S.E.

d) La Subgerencia Administrativa debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.

e) Los ingresos y egresos de personal a las instalaciones del Hospital Departamental de Granada E.S.E. en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

f) Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones del Hospital Departamental de Granada E.S.E.; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.

g) Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

3.2.5 PLAN de seguridad para los equipos

El Hospital Departamental de Granada E.S.E. para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Pautas para tener en cuenta

a) El proceso Gestión de la información debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones del Hospital Departamental de Granada E.S.E.

b) El proceso Gestión de la información debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.

c) El proceso Gestión de la información en conjunto con el facilitador del proceso Gestión de Suministros debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.

d) El proceso Gestión de la información debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.

e) El proceso Gestión de la información debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condicione con la lista de chequeo de Planes de Seguridad de la Información ***HDG-PO-L1***, antes de conceder a estos equipos acceso a los servicios de red.

f) El proceso Gestión de la información debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.

g) El proceso Almacén debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones del Hospital Departamental de Granada E.S.E. cuente con la autorización documentada y aprobada previamente por el área.

h) El proceso Gestión de la información es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos del Hospital Departamental de Granada E.S.E.

i) Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione el proceso Gestión de la Información.

j) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad del Hospital Departamental de Granada E.S.E., el usuario responsable debe informar al facilitador del proceso Gestión de la información, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

k) La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los técnicos de apoyo al proceso Gestión de la información.

l) Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

m) Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

n) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos

o) En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

p) Los funcionarios de la entidad y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

3.2.6 PLAN de uso adecuado de internet

El Hospital Departamental de Granada E.S.E. consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad

Pautas para tener en cuenta

a) El proceso Gestión de la información debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

b) El proceso Gestión de la información debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

c) El proceso Gestión de la información debe monitorear continuamente el canal o canales del servicio de Internet.

d) El proceso Gestión de la información debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

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

f) Los usuarios del servicio de Internet del Hospital Departamental de Granada E.S.E. deben hacer uso de este en relación con las actividades laborales que así lo requieran.

g) Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

h) No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o Planes establecidas en este documento.

i) Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del Hospital Departamental de Granada E.S.E.

j) No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de la información o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

k) No está permitido el intercambio no autorizado de información de propiedad del Hospital Departamental de Granada E.S.E., de los funcionarios, con terceros.

6. 4. PRIVACIDAD Y CONFIDENCIALIDAD

4.1 PLAN de tratamiento y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, El Hospital Departamental de Granada E.S.E. a través del Comité de Gestión y Desempeño, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establece los términos, condiciones y finalidades para las cuales El Hospital Departamental de Granada E.S.E., como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, El Hospital Departamental de Granada E.S.E. exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Pautas para tener en cuenta

a) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.

b) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

c) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

d) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

e) Las Unidades de Gestión que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos

establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

f) El Comité de Gestión y Desempeño debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros del Hospital Departamental de Granada E.S.E. de los cuales reciba y administre información.

g) El proceso Gestión de la información debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

h) Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

i) Es deber de los usuarios y funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por correo electrónico o por correo certificado, entre otros.

4.2 Disponibilidad del servicio e información

El Hospital Departamental de Granada E.S.E. con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, a decidió crear un plan para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

4.2.1 PLAN de continuidad, contingencia y recuperación de la información

El Hospital Departamental de Granada E.S.E. proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

4.2.1.1 Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Gestión y Desempeño. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias del Hospital Departamental de Granada E.S.E. deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

El proceso Gestión de la información debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad. La (el) profesional especializado con funciones de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

Pautas para tener en cuenta

a) El Comité de Gestión y Desempeño, debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

b) El Comité de Gestión y Desempeño, debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres

c) El Comité de Gestión y Desempeño debe realizar los análisis de impacto a la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el Plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

d) El Comité de Gestión y Desempeño debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información

e) El Comité de Gestión y Desempeño, debe asegurar la realización de pruebas periódicas del Plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

7. SEGUIMIENTO Y EVALUACIÓN

Se realizará seguimiento trimestral por parte de la oficina de sistemas y Planeación al cumplimiento de las Planes de seguridad y privacidad de la información en la institución.

8. SEGUIMIENTO CONTROL Y MEJORA

CONTROL DE CAMBIOS		
VERSION	**FECHA**	**DESCRIPCION DE LA MODIFICACION**
Versión 1	07/01/2022	Nuevo
Versión 2	13/01/2023	Modificación Ítem 1 Presentación.