POLÍTICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

La gerencia de la ESE Hospital Universitario de Santander y sus colaboradores se comprometen a desarrollar procesos institucionales que cuenten con información segura, confiable, asertiva, cumpliendo con los criterios de oportunidad, integridad disponibilidad, confidencialidad, promoviendo la continuidad de la prestación de servicios de salud.

VALORES

- Honestidad
- Responsabilidad
- Respeto
- Compromiso

PRINCIPIOS

- Transparencia
- Compromiso Social
- Trabajo en Equipo

OBJETIVOS

1. Desarrollar procesos institucionales que cuenten con información segura, confiable, asertiva
2. Cumplir con los criterios de oportunidad, integridad disponibilidad, confidencialidad
3. Promover la continuidad de la prestación de servicios de salud.

INDICADORES

Cumplimiento a:

Proporción de cumplimiento al Manual de Seguridad de la Información (SIS-03)
Proporción de Caída del del sistema de información por fallas en el Aplicativo (SIS-01)
Proporción de Caída del sistema de información por Otras fallas (SIS-02)
Proporción de respuesta de las solicitudes de datos administrativos (GEI-02)
Proporción de respuesta de las solicitudes de datos asistenciales (GEI-03)

Objeto: Desarrollar procesos institucionales que cuenten con información segura, confiable, asertiva, cumpliendo con los criterios de oportunidad, integridad disponibilidad, confidencialidad, promoviendo la continuidad de la prestación de servicios de salud.

Alcance: Esta política es aplicable a cada uno de los procesos institucionales establecidos por la Empresa Social del Estado Hospital Universitario de Santander con las alianzas estratégicas y finaliza con el seguimiento a la aplicación de la política.

Definiciones

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: Es el elemento de información que cada entidad territorial recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentra en forma expresa escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos de cómputo incluyendo datos contenidos en registros, archivos, bases de datos, videos e imágenes.

Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos del negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardo en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para la E.S.E. HUS.

Amenaza: Una causa potencial de un incidente no deseado, el cual puede producir un daño a un sistema o a la Organización.

Antivirus: Es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones: Es todo el software que se utiliza para la gestión de la información.

Autenticación: Garantía de que una parte de una transacción informática no es falsa. La autenticación normalmente lleva consigo el uso de una contraseña, un certificado, un número de identificación personal u otra información que se pueda utilizar para validar la identidad en una red de equipos.

Comité de Gestión y Desempeño: Instancia de nivel superior, que debe validar las políticas de seguridad de información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos de la E.S.E HUS.

Confidencialidad: Propiedad de la información que determina que esté disponible a personas autorizadas.

Control de acceso: Es el proceso de conceder permisos a usuarios o grupos de acceder a objetos tales como ficheros o impresoras en la red.

Copia de respaldo: Es un duplicado de nuestra información más importante, que realizamos para salvaguardar los documentos, archivos, fotos, etc., de nuestro ordenador.

Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la E.S.E HUS.

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Evento de Seguridad de la Información: Se considera un evento de seguridad de la información a cualquier situación identificada que indique una posible brecha en la política de seguridad y confidencialidad de la información o falla en los controles y/o protecciones establecidas.

Hardware: Son todos los equipos utilizados para gestionar la información y las comunicaciones.

Incidente de Seguridad de Información: Se considera como incidente de seguridad de información, un acceso, el uso, divulgación, modificación o destrucción no autorizada de la información de la E.S.E HUS y de sus usuarios, un impedimento en la operación normal de las redes, sistemas informáticos o cualquier otro que implique una violación a la política de seguridad informática.

Instalaciones: Son todos los lugares en los que se alojan los sistemas de información.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.

Minería de Datos: Es el estudio y tratamiento de datos masivos para extraer conclusiones e información relevante de ellos.

Política de seguridad: Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad de la información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias [NTC-ISO/IEC 27000:2013]

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas. [NTC-ISO/IEC 27002:2013]

Sistema de Información: conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos.

Tratamientos de Datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración,

modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consulta, interconexiones y transferencias.

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la E.S.E HUS, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la E.S.E HUS y a quienes se les otorga un nombre de usuario y una clave de acceso.

TIC: Las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Art.6 Ley 1341 de 2009).

La dirección de la Empresa Social del Estado Hospital Universitario de Santander, 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 la Empresa Social del Estado Hospital Universitario de Santander, 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 la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política 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 determinados por las siguientes objetivos:

- Minimizar los riesgos asociados a la información del SGSI descritos en el plan de tratamiento de riesgos para 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 clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, 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 de la Empresa Social del Estado Hospital

Universitario de Santander Garantizar la continuidad del negocio frente a incidentes.

- La Empresa Social del Estado Hospital Universitario de Santander 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.

La Empresa Social del Estado Hospital Universitario de Santander establece 12 principios de seguridad que soportan el SGSI:

1. Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, y terceros**.
2. La Empresa Social del Estado Hospital Universitario de Santander, **protegerá la información** generada, procesada o resguardada por los procesos de la institución, 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 outsourcing.
3. La Empresa Social del Estado Hospital Universitario de Santander **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.
4. La Empresa Social del Estado Hospital Universitario de Santander **protegerá su información** de las amenazas originadas por parte **del personal**.
5. La Empresa Social del Estado Hospital Universitario de Santander **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.
6. La Empresa Social del Estado Hospital Universitario de Santander, **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. La Empresa Social del Estado Hospital Universitario de Santander **implementará control de acceso** a la información, sistemas y recursos de red.
8. La Empresa Social del Estado Hospital Universitario de Santander trabajara para que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. La Empresa Social del Estado Hospital Universitario de Santander buscara 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.

10. La Empresa Social del Estado Hospital Universitario de Santander **mantendrá la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

11. La Empresa Social del Estado Hospital Universitario de Santander trabajara en el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

12. El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.