HOSPITAL UNIVERSITARIO DE SANTANDER
EMPRESA SOCIAL DEL ESTADO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MACROPROCESO DE GESTIÓN INTEGRAL DE LA INFORMACIÓN

ENERODE 2021

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO

Elaborar el Plan de Seguridad y Privacidad de la Información orientado a proteger la confidencialidad, integridad y disponibilidad de los activos de información de la E.S.E. Hospital Universitario de Santander.

2. ALCANCE

Este documento refleja los principales lineamientos establecidos por el MINTIC, para garantizar la seguridad y privacidad de la información y es aplicable a todos los procesos de la E.S.E. Hospital Universitario de Santander definidos en el mapa de procesos, por otra parte, los lineamientos y actividades que resulten del presente plan deben ser divulgados, conocidos y cumplidos por todos los colaboradores de la institución que tengan acceso, almacenen, procesen o trasmitan información de la entidad.

3. APLICABLE A

Este plan aplica a todos los procesos Estratégicos, Misionales, de Apoyo y de Evaluación de la E.S.E Hospital Universitario de Santander.

4. RESPONSABLE

Subgerente Administrativa y Financiera
Profesional Especializada Unidad Funcional de Apoyo Tecnológico y la Información
Profesional Universitario Unidad Funcional de Apoyo Tecnológico y la Información

5. 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.[1]

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.

[1] Archivo general de la nación – Manual políticas de seguridad de la información – marzo 10 de 2014

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

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.

Dato Personal: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley.

Dato Público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.

Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato Semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

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

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.

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.

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

MSPI: Modelo de Seguridad y Privacidad de la Información.

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.

6. CONDICIONES GENERALES

- Toda persona que ingrese a laborar en el área administrativa o asistencial de la E.S.E HUS deberá solicitar la creación de usuario al sistema de información a través del formato solicitud usuario a red y acceso aplicativos (GII-SIS-FO-17).

- Es responsabilidad de los usuarios identificar y cumplir las políticas de seguridad de la información de la E.S.E. HUS.

- Los colaboradores de la E.S.E. HUS deberán realizar el proceso de inducción y reinducción de la entidad.

7. DESARROLLO

La E.S.E Hospital Universitario de Santander estructura el Plan de Seguridad y Privacidad de la Información en concordancia con los marcos legales y conceptuales del Estado relacionadas con la Seguridad y Privacidad de la Información, lo cual permitirá cumplir con el objetivo definido en este Plan, para esto se definen las siguientes fases:

Fase I Diagnostico

Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Fase II Planificación (Planear)

Hace referencia a establecer el Modelo de Seguridad y Privacidad de la Información, en esta fase se debe establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de la entidad.

Fase III Implementación (Hacer)

Hace referencia a implementar u operar el MSPI, en esta fase se debe implementar y operar la política, los controles y procedimientos del MSPI.

Fase IV Evaluación de Desempeño (Verificar)

Hace referencia a hacer seguimiento y revisión del MSPI, en esta fase se debe evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.

Fase V Mejora Continua (Actuar)

Hace referencia a mantener y mejorar el MSPI, en esta fase de debe emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

La Ese Hospital Universitario de Santander inició a trabajar el Modelo de Seguridad y privacidad de la información en el año 2020 ejecutando cronograma de trabajo para revisión e implementación de la guías del MSPI establecidas por el MINTIC. Para este año 2021 se continúa con lo correspondiente para este año.

Meta	Guías	Fecha posible	Fase
Gestionar controles de seguridad	Guía No 8 - Controles de Seguridad	Febrero -Abril	III
Indicadores De Gestión	Guía No 9 - Indicadores de Gestión SI	Abril - Junio	
Plan de Comunicaciones	Guía No 14 - Plan de comunicación, sensibilización y capacitación	Febrero - Diciembre	
Plan de Transición de IPv4 a IPv6	Guía No 19 - Aseguramiento de protocolo IPv4_IPv6	Julio - Diciembre	III
Plan de diagnóstico de IPv4 a IPv6	Guía No 20 - Transición Ipv4 a Ipv6	Julio - Diciembre	
Integración del MSPI con el Sistema de Gestión documental	Guía No 6 - Gestión Documental	Julio - Diciembre	
Plan de Ejecución de Auditorias	Guía No 15 – Guía de Auditoría	Julio - Septiembre	IV
Plan de revisión y seguimiento, a la implementación del MSPI	Guía No 16 – Evaluación del desempeño	Octubre	
Plan de mejora continua	Guía No 17 – Mejora Continua	Noviembre - Diciembre	V

8. DOCUMENTOS DE REFERENCIA

- Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se 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.

- Decreto 2578 de 2012: Por medio del cual se 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.

- Decreto 2609 de 2012: Por medio del 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.

- Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Decreto 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Norma ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.

- Modelo de Seguridad y Privacidad de la Información MINTIC.

9. SOCIALIZACIÓN

Una vez aprobado este documento, es responsabilidad del líder del macroproceso y el responsable del procesos garantizar su socialización en los grupos primarios que le aplique, y/o mediante la utilización de cualquiera de las herramientas desarrolladas por la institución para tal fin, dejando la evidencia respectiva, las cuales deben ser enviado como soporte al correo institucional procesoscalidad@hus.gov.co.

10. CONTROL DE MODIFICACIONES

Versión	Fecha	Descripción de la Modificación	Actualizado por	Revisado por	Aprobado por
NA	MM-AA	NA	NA	NA	NA