MANUAL DE SEGURIDAD DE LA INFORMACIÓN

GESTIÓN INTEGRAL DE LA INFORMACIÓN

GII-GEI-MA-03
VERSIÓN 2
ABRIL DE 2022

HOSPITAL UNIVERSITARIO DE SANTANDER
EMPRESA SOCIAL DEL ESTADO

TABLA DE CONTENIDO

1. OBJETIVO 4
2. ALCANCE 4
3. APLICABLE A 4
4. RESPONSABLE 4
5. DEFINICIONES 4
6. CONDICIONES GENERALES 6
7. DESARROLLO 6
7.1. POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN 6
7.2. CLASIFICACIÓN DE LA INFORMACIÓN 7
7.2.1. Clasificación de activos 8
7.3. ROLES Y RESPONSABILIDADES 8
7.3.1. Responsabilidad del Comité de Gestión y Desempeño 8
7.3.2. Responsabilidad del proceso de Gestión de Adquisición de Bienes, Servicios y Obras 9
7.3.3. Responsabilidad de los supervisores de contrato 9
7.3.4. Responsabilidades en la terminación o cambio del empleo 9
7.3.5. Responsabilidades de los usuarios 9
7.3.6. Responsabilidades del proceso de Sistemas de Información 10
7.4. ADMINISTRACIÓN DE LA PLATAFORMA TECNOLÓGICA 10
7.5. CONTROL DE ACCESO 11
7.6. CONECTIVIDAD 11
7.7. CONTINGENCIA 11
7.8. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 11
7.9. MANTENIMIENTO DE EQUIPOS 11
7.10. ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN 12
7.11. SERVICIOS DE SOPORTE DE TIC 12
7.12. CONTROL Y AUDITORÍA DEL ACCESO A LA INFORMACIÓN 12
7.12.1. Integridad de la información, cambios en base de datos 13
7.12.2. Privacidad y protección de información 13
7.13. ADMINISTRACIÓN DE PROYECTOS TIC 13
7.14. CLASIFICACIÓN DE ACTIVOS DEL PROCESO DE SISTEMAS 13
7.15. TOMA DE CONCIENCIA EN LA SEGURIDAD DE LA INFORMACIÓN 13
7.16. CAPACITACIÓN EN PLATAFORMAS DIGITALES 14
7.17. COMUNICACIÓN DIGITAL 14

7.18. POLÍTICAS Y LINEAMIENTOS PARA EL USO DE BIENES INFORMÁTICOS 15
7.18.1. Equipos de Cómputo y de Telecomunicaciones 15
7.18.2. Uso de Servicios Informáticos 16
7.18.3. Uso del Servicio de Internet 16
7.18.4. Uso del Servicio de Correo electrónico 16
7.18.5. Transferencia de información 17
7.18.6. Buen Uso y Transmisión de la Información 17
7.18.7. Uso de Cuentas y Contraseña 17
7.19. CUSTODIA Y SEGURIDAD DE LA HISTORIA CLÍNICA 18
7.20. TÉRMINOS Y CONDICIONES PARA FUNCIONARIOS Y/O COLABORADORES 18
7.21. ASIGNACIÓN DE USUARIO 18
7.22. CANCELACIÓN DEL REGISTRO DE USUARIO 19
7.23. PROCESO DISCIPLINARIO 19
7.24. PROCESO DISCIPLINARIO EJECUTORES 19
7.25. CONTROLES DE ACCESO FÍSICOS 19
7.26. ACUERDOS SOBRE CONFIDENCIALIDAD 19
7.27. PROTECCIÓN CONTRA SOFTWARE MALICIOSO 20
7.28. GESTIÓN CON ALIANZAS ESTRATEGICAS 20
8. DOCUMENTOS DE REFERENCIA 20
9. SOCIALIZACIÓN 21
10. CONTROL DE MODIFICACIONES 21

1. OBJETIVO

Establecer reglas y lineamientos técnicos orientados a estandarizar las herramientas que contribuyan a la seguridad de la información, minimizando el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información.

2. ALCANCE

Este manual inicia con la descripción de la Políticas aprobadas en la E.S.E Hospital Universitario de Santander para la seguridad de la información y finaliza con los lineamientos establecidos para la gestión con alianzas estratégicas.

3. APLICABLE A

Este manual 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

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.
- **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.

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

- **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).

6. CONDICIONES GENERALES

- Para toda persona que labore en el área administrativa y asistencial de la E.S.E HUS se requiere la creación de un usuario de acuerdo a la actividad que desarrolle
- Es responsabilidad de los usuarios identificar y cumplir las políticas de seguridad de la información de la E.S.E. HUS
- El proceso de Sistemas de Información revisa la disponibilidad de recursos antes de asignarlos, teniendo en cuenta la prioridad y recursos existentes.

7. DESARROLLO

7.1. POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

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 determinadas por las siguientes premisas:

- 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, en aras de preservar la información y al mismo tiempo puntualizar acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas, adopta la normatividad vigente mediante la Resolución 358 del 3 de agosto de 2018 modificada por la Resolución 427 del 28 de septiembre del mismo año, aprobó las Políticas Institucionales de la E.S.E HUS socializadas a través del Formato Enunciado Políticas Institucionales (GDI-PLA-FO-10).

Según en lo dispuesto en las Resoluciones anteriormente mencionadas, se aprobaron las siguientes políticas asociadas a la seguridad de la información:

- Política de Gestión del Riesgo
- Política de Gestión Pública de Transparencia y Acceso a la Información Pública
- Política de Seguridad Digital
- Política de Tratamiento y Protección de la Información y Datos Personales

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.

7.2. CLASIFICACIÓN DE LA INFORMACIÓN

La E.S.E Hospital Universitario de Santander, clasificará la información de acuerdo con los criterios establecidos en la Guía de Instrumento de Gestión de Información Pública, expedida por la Presidencia de la República.

Los niveles de clasificación de la información definidos en la E.S.E Hospital Universitario de Santander son:

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal;
- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley;
- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley;

7.2.1. Clasificación de activos

La E.S.E. Hospital Universitario de Santander realiza la clasificación de activos de información a través de la metodología propuesta en el procedimiento de elaboración de instrumentos de gestión de información pública (GII-GDO-PR-05), en el cual se establece la metodología para la construcción y actualización de los instrumentos de gestión de Información pública.

De igual forma se cuenta con herramientas como el Formato Registro de Activos de Información (GII-GDO-FO-04) y el Formato Índice de Información Clasificada y Reservada (GII-GDO-FO-15).

Con esto se identificar el propietario del activo, quien debe asegurar que la información y los activos asociados con su proceso estén clasificados de manera apropiada, así como el establecer controles para el acceso a estos.

7.3. ROLES Y RESPONSABILIDADES

7.3.1. Responsabilidad del Comité de Gestión y Desempeño

Esta responsabilidad se encuentra definida en la Resolución 585 del 31 de Octubre de 2017, Por medio de la cual se crea el comité de gestión y desempeño y se dictan nuevas disposiciones, que en su artículo octavo define como función del Comité Institucional de Gestión y Desempeño la de "(…) Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información (…)". En el mismo sentido, la Resolución 356 de 01 de agosto de 2018, Por medio de la cual se modifican los artículos segundo, tercero, séptimo, octavo y décimo segundo del Comité de Gestión y Desempeño y se dictan nuevas disposiciones, dispone en su artículo cuarto:

MODIFICAR el artículo octavo: FUNCIONES del Comité Institucional De Gestión Y Desempeño del Comité de Gestión y Desempeño, de la Resolución 585 del 31 de octubre de 2017, el cual quedara así:

Definir los lineamientos para la implementación efectiva de políticas y estándares asociados, como la política de actualización del sitio Web (donde deberán estar involucradas las diversas áreas, direcciones y/o programas de la entidad), política de uso aceptable de los servicios de Red y de Internet, política de servicio por medios electrónicos, política de privacidad y condiciones de uso y política de seguridad del sitio Web, entre otros.

- El Comité de Gestión y Desempeño es el encargado de aprobar y actualizar las políticas y procedimientos relativos a seguridad de información.
- Es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres relativos a la seguridad de la información.
- Durante sus reuniones, el Comité efectuará la evaluación y revisión de la situación de la E.S.E. HUS en cuanto a seguridad de información, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad y la continuidad del negocio.

- De realizar seguimiento a los incidentes de seguridad de información, identificar, revisar y actualizar anualmente amenazas y planes de continuidad del negocio, detectar y revisar errores en el análisis de riesgos y hacer continuo seguimiento al proceso de seguridad de información.
- Tiene la responsabilidad de informar a la oficina asesora de Control Interno y/o supervisores de contratos según corresponda, el incumplimiento de las Directrices impartidas en el presente manual a fin de aplicar las acciones que correspondan.

7.3.2. Responsabilidad del proceso de Gestión de Adquisición de Bienes, Servicios y Obras

- Debe garantizar la inclusión de la cláusula de confidencialidad en los contratos estatales que suscriba la E.S.E. HUS, en aras de garantizar el correcto uso de los activos de información y el buen manejo de la información.
- Así mismo, incluir dentro de los contratos y/o convenios el correcto tráfico de la información, contemplando la entrega y devolución de la misma, suministrada al colaborador y la producida por este durante la ejecución del correspondiente convenio o contrato.
- Incluir y mantener vigente en el manual de supervisión e interventoría de contratos (Acuerdo de junta Nro. 031 de 2014) los mecanismos tendientes a preservar por parte de los supervisores la seguridad de la información a la que se refiere este manual.

7.3.3. Responsabilidad de los supervisores de contrato

El o los supervisores de cada contrato y/o convenio, deben asegurar la entrega y salvaguarda de la información de los colaboradores del proceso, mediante las herramientas que se definan en el manual de supervisión e interventoría de contratos (Acuerdo de junta Nro. 031 de 2014) para garantizar la seguridad de la información.

7.3.4. Responsabilidades en la terminación o cambio del empleo

Los subgerentes y jefes de oficinas asesoras deberán informar al proceso de Sistemas de Información, las novedades de los colaboradores correspondientes a sus procesos, inmediatamente sucede el ingreso, el retiro o la modificación para que sean cancelados y/o modificados los permisos en los diferentes sistemas de información con los que cuenta la E.S.E HUS.

7.3.5. Responsabilidades de los usuarios

Los usuarios son responsables de cumplir con todas las políticas institucionales de la E.S.E HUS relativas a la seguridad información o relacionadas con la seguridad de la información, al buen uso de los bienes informáticos, con los siguientes apartados:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos, así como la ley de transparencia y del derecho de acceso a la información.
- No divulgar información confidencial de la E.S.E HUS a personas no autorizadas.
- Los colaboradores no deben suministrar información de la entidad a ningún ente externo sin las autorizaciones respectivas.
- Todo colaborador que utilice los Recursos Informáticos tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o critica.
- No permitir y no facilitar el uso de los sistemas informáticos de la E.S.E HUS a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (correo, teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo de la E.S.E HUS.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- Las palabras claves o contraseñas de acceso a los recursos informáticos, que asignen los usuarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgadas a ninguna persona.
- Las contraseñas y claves de acceso son de uso personal e intransferible, por tanto, no pueden ser compartidas ni utilizadas por terceros.

- Para aportar mayor seguridad al sistema, las contraseñas deberán ser cambiadas de forma obligatoria como mínimo cada 90 días.
- Reportar inmediatamente a su jefe inmediato y al proceso de Sistemas de Información cualquier evento que pueda comprometer la seguridad de la E.S.E HUS y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o perdida de datos y otras actividades poco usuales.
- Los colaboradores, contratistas y estudiantes deben cumplir con los lineamientos establecidos en la modalidad de contratación definidos por la E.S.E HUS.
- Es responsabilidad del usuario definir qué información es importante y sensible en su equipo de cómputo, con el objetivo de realizar copias de seguridad como lo solicita el Procedimiento Copias de Seguridad de PCS (GII-SIS-PR-01).
- Es responsabilidad del usuario el correcto registro de la información y que la misma sea fidedigna e íntegra
- al momento de su retiro o cambio de funciones en la E.S.E Hospital Universitario de Santander, deberá hacer entrega a su supervisor del contrato del equipo que se le haya asignado, con toda la información contenida en él y una relación de la misma.
- Los usuarios de la E.S.E Hospital Universitario de Santander, son responsables de la información que usan y deben seguir los lineamientos establecidos por la institución para protegerla, evitar pérdidas, accesos no autorizados y utilización indebida de la misma.
- Todo usuario mantendrá total confidencialidad sobre la información a que tenga acceso y no será utilizada con propósitos distintos a los determinados en razón de su cargo, si se requiere copiar información sensible, se debe contar con una autorización, del personal designado.
- Por ningún motivo los usuarios podrán hacer uso ni copiar Software propiedad de la E.S.E HUS para uso personal, o beneficio propio.

7.3.6. Responsabilidades del proceso de Sistemas de Información

- El proceso de Sistemas de Información es responsable de implementar controles y velar por el cumplimento de las políticas y procedimientos de seguridad de la información en toda la E.S.E. HUS; así como la actualización de normas que definen el buen uso de los bienes informáticos y activos de información, todo esto en coordinación con la alta dirección y el comité de gestión y desempeño.
- Es responsable de gestionar, evaluar, e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro.
- Debe proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad de la información correspondiente al ambiente informático.

7.4. ADMINISTRACIÓN DE LA PLATAFORMA TECNOLÓGICA

- La Gerencia través del proceso de Sistemas de Información provee y actualiza la plataforma de sistemas de información utilizados para los diferentes procesos. Esta plataforma es la única fuente de registro o ingreso de información y a su vez es la herramienta de consulta y extracción de datos para información histórica, estadística y de toma de decisiones.
- Las necesidades de mejora o actualización del sistema de información se deben tramitar a través de la mesa de ayuda y/o los medios oficiales establecidos por la E.S.E HUS
- El proceso de Sistemas de Información se encargará de identificar las necesidades de software y capacitación que requieren los diferentes procesos de la institución.
- El proceso de Gestión de la Tecnología se encargará de identificar las necesidades de hardware y redes de comunicaciones que requieren los diferentes procesos de la E.S.E HUS
- El proceso de Gestión de la Tecnología mantendrá vigente un programa de mantenimiento preventivo de la plataforma tecnológica de la E.S.E HUS con el fin evitar posibles daños o pérdida de información.
- El proceso de Gestión de la Tecnología es responsable de disponer un sistema de control de inventario del hardware y el software instalado en los equipos de la E.S.E HUS. Así como definir la baja y renovación de

equipos de cómputo y Hardware en general.

7.5. CONTROL DE ACCESO

Desde el proceso de gestión de tecnología se dispone del Procedimiento para el Control y Gestión del Data Center (GTE-GTE-PR-04). En el cual se enmarcan las actividades de control y gestión en la administración del datacenter de la E.S.E Hospital Universitario de Santander.

7.6. CONECTIVIDAD

- El proceso de Sistemas de Información es responsable de administrar los servicios de conectividad entre sistemas internos de la entidad y sistemas o redes externas.
- El proceso de Sistemas de Información establecerá controles con el fin de no comprometer la seguridad de la información interna de la E.S.E HUS.

7.7. CONTINGENCIA

- El proceso de Gestión Directiva y el proceso de Sistemas de Información de Información proveerá y garantizará un plan de continuidad del servicio en caso de afrontar cualquier evento que interrumpa la disponibilidad de un servicio TIC
- La E.S.E Hospital Universitario de Santander, realiza el registro de eventos y fallos que ocurran en los sistemas de información a través del Formato Reporte de Daños a los Sistemas de Información (GII-SIS-FO-02).

7.8. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E. Hospital Universitario de Santander a través de la política de gestión integral del riesgo es responsable de definir el nivel de riesgo que es aceptable y crea una estructura de control de riesgo para mantener los riesgos dentro de los limites apropiados, garantizando recursos humanos, financieros y logísticos a fin de favorecer la gestión del riesgo.
De igual manera la institución analizará y tomará decisiones estratégicas con las cuales podrá gestionar efectivamente los riesgos, las cuales contemplan:

- Aceptar el riesgo, pero tomando algunas acciones para disminuir su probabilidad de ocurrencia o su magnitud de impacto.
- Transferir el riesgo a un tercero u organización.
- Eliminar el riesgo por el retiro o cesación del desarrollo o ejecución de la actividad o función causante de éste.
- Implementar controles por deficiencias en el diseño, la implementación o la eficacia operativa que minimice los riesgos identificados.

Dando cumplimiento a lo mencionado el proceso de sistemas de información dispone del instructivo de riesgos digitales (GII-SIS-IN-04) en el cual se estructura las acciones a seguir que permitan identificar, medir, controlar, y monitorear, comunicar y mitigar la materialización de los riesgos de seguridad digital.

7.9. MANTENIMIENTO DE EQUIPOS

La E.S.E Hospital Universitario de Santander dispone de los siguientes procedimientos para el mantenimiento de equipos de cómputo:

- Procedimiento Mantenimiento Preventivo y Predictivo (GTE-GTE-PR-01), en el cual se establece las actividades a realizar que aseguran la correcta ejecución del mantenimiento preventivo y predictivo de equipos biomédicos, industriales y de cómputo de la E.S.E Hospital Universitario de Santander.
- Procedimiento Mantenimiento Correctivo (GTE-GTE-PR-02), en el cual se estandarizan las actividades que permitan atender y solucionar las fallas presentadas en los diferentes equipos biomédicos, industriales y equipos

de cómputo de la E.S.E Hospital Universitario de Santander, de manera que se pueda brindar continuidad y buen funcionamiento de los mismos.

7.10. ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN

La E.S.E Hospital Universitario de Santander, estableció los siguientes procedimientos de copias de seguridad para garantizar la disponibilidad, integralidad de la información:

- **Procedimiento Copias de Seguridad del Servidor de Datos:** este procedimiento define la información a seleccionar para la generación de copias de seguridad y se describe el nivel de importancia de acuerdo a las bases datos y aplicativos existentes en los servidores.
- **Procedimiento de Copias de Seguridad de PCS (GII-SIS-PR-01)**, en el cual se definen los pasos que se deben ejecutar para realizar una copia periódica de la información guardada en los pc de cada uno de los diferentes procesos.

Los respaldos de la información generada en cada terminal y/o equipo de cómputo es responsabilidad de cada usuario, el cual genera copias de seguridad constantes o en el periodo establecido, para evitar la pérdida de la información.

El proceso de Sistemas de Información de Información deberá orientar y capacitar a todos los usuarios internos que lo requieran, en cómo deben realizar copias de respaldo de los archivos en uso e identificar a cuáles debe hacerle periódicamente copia de acuerdo a los sistemas de información que se manejan.

7.11. SERVICIOS DE SOPORTE DE TIC

La E.S.E HUS a través del proceso de Sistemas de Información brindará una mesa de ayuda que permita el registro, trazabilidad y suministro de estadística de las actividades de soporte prestadas a los diferentes procesos.

7.12. CONTROL Y AUDITORÍA DEL ACCESO A LA INFORMACIÓN

Con el fin de garantizar la seguridad de la información, la E.S.E. HUS a través del proceso de Sistemas de Información define diferentes niveles de acceso y manipulación autorizada de la información, implementando un procedimiento de administración de roles, permisos y claves de usuarios, determinando:

- El acceso a los sistemas de información está restringido por el rol de usuario definido con base a los perfiles y funciones del cargo aprobado por el subgerente o profesional de planta a través del Formato Solicitud Usuario a Red y Acceso Aplicativos (GII-SIS-FO-17) dichos perfiles son asignados por el administrador del sistema.
- Cuando un colaborador ingresa a la Institución se asignará una cuenta de usuario de ingreso a la red de la institución y en los sistemas permitidos de acuerdo con el rol que determinan su cargo y funciones. Si se requiere algún permiso adicional el jefe inmediato debe solicitar al proceso de Sistemas de Información la actualización de los permisos de ese usuario en particular.
- El proceso de sistema implementará las herramientas que considere convenientes para proteger la privacidad de las contraseñas impidiendo el acceso a los servidores que las custodian, adicionalmente, registrará el autor y el momento en que se realicen ingresos y cambios de información en el sistema.
- Para garantizar el control de los activos de información físicos como equipos de cómputo, equipos de red y demás recursos tecnológicos, el proceso de almacén realizará el ingreso e identificación del inventario de los equipos anteriores.
- El proceso de recolección de evidencia ante un incidente de seguridad que implique acciones legales debe estar sujeta al marco legal vigente aplicable mencionado en este manual, y debe contar con altos niveles de integridad, calidad y veracidad.
- El proceso de Sistemas de Información puede monitorear y hacer seguimiento a la información y registros de auditoría de los servicios TIC, como: correo institucional, Bases de Datos de la E.S.E HUS, servidores de

archivos y otras aplicaciones y/o sistemas sobre la cual el proceso de Sistemas de Información tiene su administración.

- Todos los sistemas automáticos que operen y administren información sensible, valiosa o crítica para la Entidad, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoría.
- El macroproceso de Gestión Integral de la Información en apoyo con el macroproceso de Gestión Jurídica definirá el formato de autorización de uso de datos personales para sus proveedores, clientes, pacientes, colaboradores, etc. Será responsabilidad de los procesos de la E.S.E. HUS su aplicación.

7.12.1. Integridad de la información, cambios en base de datos

Si después del análisis del caso de una solicitud de soporte se determina que se debe realizar un ajuste a algún registro de la base de datos, se debe notificar por correo electrónico y/o físico la aprobación de esta modificación por parte del propietario de esta información. En ningún caso se modificará información legalmente protegida de alteración, como estados financieros aprobados, historia clínica electrónica, etc. Todo cambio en la base de datos debe estar debidamente documentado para su trazabilidad.

7.12.2. Privacidad y protección de información

La Empresa Social del Estado Hospital Universitario de Santander, a través del comité de Gestión y Desempeño, diagnostica, analiza y desarrolla la puesta en marcha y seguimiento al Manual de Seguridad de la Información, así como la **Política de Tratamiento y Protección de Datos Personales** en cumplimiento de la ley 1581 de 2012 y su decreto reglamentario 1377 de 2013.

La Política de Tratamiento y Protección de Datos Personales, regula la recolección, almacenamiento, administración, tratamiento y protección de la información y datos personales que se reciban de las personas, ésta deberá ser comunicada a todas las personas involucradas en el proceso de información de datos personales.

Los usuarios de la E.S.E Hospital Universitario de Santander, mantendrán total confidencialidad sobre la información a la que tengan acceso y no la utilizarán con propósitos distintos a los determinados en razón de su cargo, si se requiere copiar información sensible, se debe contar con autorización correspondiente.

7.13. ADMINISTRACIÓN DE PROYECTOS TIC

Todo proyecto de desarrollo propio o contratado con terceros, antes de ser ejecutado debe tener un cronograma de ejecución, estudio de factibilidad técnica y financiera, recursos requeridos, el cual será objeto de seguimiento y control continuo. Además, debe contar con un alcance y la aprobación de la Subgerencia y la Gerencia de la ESE HUS, se designarán un líder de proyecto y un supervisor.

7.14. CLASIFICACIÓN DE ACTIVOS DEL PROCESO DE SISTEMAS

Desde el proceso de sistemas de información se dispone del formato Clasificación de activos del proceso de sistemas (GII-SIS-FO-07), en el cual se clasifican los activos del proceso de sistemas de información de la siguiente manera:
Sistemas operativos, red de datos, equipos de cómputo, Sistemas de información.

7.15. TOMA DE CONCIENCIA EN LA SEGURIDAD DE LA INFORMACIÓN

La E.S.E Hospital Universitario de Santander, establece estrategias direccionadas a la toma de conciencia en la seguridad de la información mediante jornadas de inducción, Jornadas de reinducción, coordinadas a través de la unidad funcional de talento humano y/o docencia servicio.

7.16. CAPACITACIÓN EN PLATAFORMAS DIGITALES

Desde el estándar de gerencia de la información se cuenta con un Plan de Capacitaciones en Plataformas Digitales (GII-GEI-PL-01) el cual busca fortalecer las competencias de los usuarios de la ESE la ESE Hospital Universitario de Santander en las diferentes PLATAFORMAS DIGITALES disponibles en la institución logrando un mejor uso de las mismas, así como la solución oportuna en los problemas que se derivan de la falta de conocimientos en el uso de las plataformas.

El Plan de capacitaciones en las diferentes PLATAFORMAS DIGITALES de la E.S.E HUS es una herramienta de construcción permanente, en donde se realiza un diagnóstico de necesidades de capacitación teniendo en cuenta directrices tanto internas como externas o requerimientos específicos que pueden llevar a identificar nuevos temas, así como las formas de ejecutar las capacitaciones

El plan de capacitaciones en plataformas digitales se identifican los siguientes objetivos a ejecutar.

- Identificar las necesidades de formación y capacitación en los módulos de las diferentes PLATAFORMAS DIGITALES de la E.S.E HUS.
- Programar las acciones de Capacitación en las PLATAFORMAS DIGITALES, para la respectiva vigencia articulada a la detección de necesidades.
- Contribuir al mejoramiento institucional, fortaleciendo las competencias de los servidores de la E.S.E Hospital Universitario de Santander en plataforma de tecnologías de la información, apoyando la solución pronta a la problemática que se deriva por el error humano, en la manipulación del software.
- Aportar a la transformación digital, utilizando herramientas digitales para el desarrollo de plan de capacitación.

7.17. COMUNICACIÓN DIGITAL

La E.S.E HUS dispone de un Plan de Comunicaciones Institucionales (GDI-COM-PL-01) y un Manual de Imagen Corporativa y Visual (GDI-COM-MA-01), en los cuales se establece de forma detallada los parámetros y las directrices para el manejo de la Imagen Institucional y las comunicaciones de la Institución, estos documentos deben ser aplicables en todas las actividades de comunicación que se lleven a cabo en la E.S.E HUS.

El proceso de Sistemas de Información es responsable de mantener disponibles los medios de comunicación digital, que son:

- **Correo Electrónico y plataforma de comunicaciones GOOGLE**: El correo interno institucional es el medio de comunicación electrónico oficial en la ESE HUS, la distribución de mensajes de correo electrónico masivos es una herramienta que se debe canalizar por la oficina de prensa.
  Las normas y restricciones como orientación en su utilización reposan en la Resolución 000122 de 2015 en la cual establece la Política de Uso de la Plataforma de Comunicaciones Interna de la Empresa Social del Estado Hospital Universitario de Santander.
- **Página Web**: Es el canal masivo de comunicación externa en donde se encuentra información de interés que la E.S.E HUS y sus procesos desean transmitir y compartir a la comunidad en general. La interfaz gráfica de la Página Web se regirá por los parámetros y directrices consignados en el Manual de Imagen Institucional.
- **Mensajería Instantánea**: Herramientas de comunicación instantánea que permite comunicación entre dos o más personas. (SPARK) Esta herramienta solo es habilitada para el proceso de facturación.
- **Telefonía en VoIP**: Comunicación telefónica digital administrada por el proceso de Sistemas de Información.

El proceso de Sistemas de Información proporcionará asesoría y asistencia técnica oportuna en materia de instalación, configuración y uso de los servicios de comunicación digital.

7.18. POLÍTICAS Y LINEAMIENTOS PARA EL USO DE BIENES INFORMÁTICOS

7.18.1. Equipos de Cómputo y de Telecomunicaciones

- El uso de los equipos de cómputo será destinado única y exclusivamente para apoyar las funciones que son propias de la E.S.E HUS y en beneficio de la misma.
- El equipo de cómputo no se debe utilizar fumando o consumiendo alimentos o bebidas.
- El equipo de cómputo debe estar conectado a la red eléctrica implementada por la E.S.E HUS.
- Si no se utiliza el equipo de cómputo durante un periodo prolongado (horas de comidas, noches, etc.) éste debe estar apagado.
- Si el usuario se ausenta de su puesto de trabajo por un tiempo superior a cinco (5) minutos, el equipo de cómputo debe mantenerse protegido con una contraseña.
- El equipo de cómputo debe encenderse en el siguiente orden: monitor, unidad de control de proceso (CPU), equipo periférico e impresora; y debe apagarse en el orden inverso.
- El Usuario será responsable del equipo de cómputo y de tener instalados solo los programas autorizados por la E.S.E HUS.
- No está permitido realizar cambios a nivel de Hardware ni de Software sin previa autorización del proceso de Sistemas de Información.
- El proceso de Sistemas de Información tiene la responsabilidad y autoridad para monitorear y hacer seguimiento al software instalado en toda máquina.
- El software gratuito que se requiera por la Organización en el desarrollo de sus actividades empresariales o se adquiera por el personal de la E.S.E HUS de manera autónoma, deberá ser validado y autorizado por el proceso de Sistemas de Información antes de su uso.
- En caso de requerir permisos en una carpeta específica del Servidor de Archivos se deberá solicitarlo a través de los canales formales establecidos con previa autorización del responsable de la información allí contenida.
- El cambio y/o movilidad de los equipos de cómputo debe ser notificado al proceso de Sistemas de Información y al responsable del control de Inventarios de la E.S.E HUS mediante oficio por parte líder del proceso al que este asignado el equipo.
- Está prohibido realizar cambios a la configuración tanto de hardware como del software entregado o no por la E.S.E HUS, pues tal actividad puede generar una brecha de seguridad en el mismo y en la estructura de la seguridad informática, siendo responsabilidad del usuario los daños resultantes de este obrar negligente e imprudente.
- Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, cambios de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del proceso de Sistemas de Información.
- Ningún usuario podrá abrir físicamente los equipos de cómputo asignados para actualizar y/o realizar cambios no autorizados y que son competencia de sistemas.
- El uso de medios extraíbles para almacenamiento de información como disquetes, CD-ROM, memoria USB se deberá efectuar de manera racional y únicamente como herramienta de trabajo. Está totalmente prohibido el uso de estas herramientas para almacenar información con fines distintos al cumplimiento de las funciones.
- Todo archivo contenido en dispositivos externos (USB, Discos Duros) y adjuntos a correos electrónicos, deben ser escaneados por el antivirus institucional antes de su utilización. Por tal motivo es obligatorio el uso del correo institucional para toda comunicación laboral. Se debe informar al servicio de Soporte de Sistemas, en el caso que el antivirus no esté activado o actualizado en el equipo asignado.
- Todo equipo (desktop, laptop, notebook, tablet, etc.) que no sea propiedad de la E.S.E HUS e ingrese a cualquiera de las instalaciones debe seguir las siguientes indicaciones:1) Si el equipo se requiere para labores propias de la E.S.E HUS, debe ser registrado previamente en la portería. El equipo debe contar con Antivirus instalado y actualizado. Todo Software instalado en el equipo debe estar licenciado y deben ser presentados todos los soportes legales.

- Los equipos de cómputo de la ESE HUS deben permanecer en áreas donde se aseguren condiciones ambientales adecuadas, en factores como iluminación, ventilación, temperatura, polvo, humedad, interferencias electromagnéticas y localización.
- Queda estrictamente prohibido descargar y almacenar en el hardware entregado por la E.S.E HUS información personal o no, como fotografías, videos, música, juegos, obras multimedia, bases de datos, entre otras, ajenas al desempeño de las funciones contratadas en el marco de relaciones laborales o de prestación de servicios.

7.18.2. Uso de Servicios Informáticos

La E.S.E. Hospital Universitario de Santander, es propietaria tanto de la información física como de la información generada, procesada, almacenada en cada uno de los procesos, el personal de planta y los usuarios tercerizados que usen estos activos de información o tengan acceso a ellos deberán tomar conciencia de los requisitos de seguridad de la información, cumpliendo con los lineamientos establecidos en este documento.

La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, aplicaciones, teléfonos y faxes, entre otros) propiedad de la E.S.E. Hospital Universitario de Santander, son activos de la Institución y se proporcionan al personal, contratista y/o tercero autorizado, para cumplir con las funciones o actividades asignadas.

7.18.3. Uso del Servicio de Internet

- 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, o que atente contra las leyes vigentes o políticas establecidas en este documento.
- No está permitido el acceso y el uso de servicios de mensajería instantánea que tenga como objetivo crear comunidades para intercambiar información o para fines diferentes a las actividades propias de la E.S.E Hospital Universitario de Santander.
- No está permitido las descargas, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que atenten contra la propiedad intelectual de sus actores, o que contengan archivos ejecutables y/o herramientas que atenten contra la disponibilidad, integridad, y/o confidencialidad de la infraestructura tecnológica de la E.S.E Hospital Universitario de Santander.
- Cada uno de los usuarios de la E.S.E Hospital Universitario de Santander, es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o malintencionadas que atenten contra la integridad de un tercero, la legislación vigente y los lineamientos de seguridad de información.
- El uso de internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la E.S.E Hospital Universitario de Santander.

7.18.4. Uso del Servicio de Correo electrónico

La Empresa Social del Estado Hospital Universitario de Santander, dando la aplicación de la ley 527 de 1999, en la cual se define y reglamenta el acceso y uso de los mensajes de datos, del correo electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones, define y reglamenta el uso y acceso a los mensajes de datos determinando su naturaleza requisitos y forma de comunicación en las Entidades Estatales, mediante la **Resolución 000122 de 2015 en la cual establece la Política de Uso de la Plataforma de Comunicaciones Interna de la Empresa Social del Estado Hospital Universitario de Santander.**

El proceso de Sistemas de Información como responsable de las funciones relativas a la administración de recursos informáticos, asigna al personal vinculado de la entidad una cuenta de correo electrónico con el nombre del servicio del cual depende; si ya existe esta cuenta y se requiere tener otro buzón, se crea con el nombre de la actividad que va a desarrollar, ejemplo: autorizaciones, notificaciones de contratos...etc.

El proceso de sistemas de información es el encargado de administrar, monitorear y hacer seguimiento del uso que el personal vinculado a la Entidad le da al sistema de correo electrónico institucional.

El monitoreo realizado se limitará a verificar la existencia o no de virus y de material inapropiado en los mensajes de datos recibidos y enviados por los usuarios del sistema.

7.18.5. Transferencia de información

La E.S.E Hospital Universitario de Santander dispone del procedimiento para el flujo y transmisión de la información (GII-GEI-PR-04), define los mecanismos para el flujo y la transmisión de información entre los procesos institucionales y grupos de interés de la institución, asegurando la oportunidad, confiabilidad, seguridad, facilidad de acceso y validez de dicha información.

De igual manera se cuenta con el formato de Solicitud de información (GII-GEIFP- 08), para realizar solicitudes de información entre procesos y sistemas de información el cual debe contar con la autorización del subgerente del servicio y/o jefe del área para realizar dicha entrega

7.18.6. Buen Uso y Transmisión de la Información

- Cualquier tipo de documentación necesaria diferente a los que el sistema de información provee, tales como cartas, reportes, memorandos y otros que el usuario realice y que sean parte del funcionamiento normal de la E.S.E HUS, se consideran propiedad intelectual y patrimonial de la E.S.E. HUS, por tanto, no debe ser extraída, modificada y/o borrada para beneficio personal y/o de terceros.
- Los usuarios no deberán acceder a la información corporativa de la E.S.E HUS por otro mecanismo diferente a las aplicaciones desarrolladas y aprobadas conjuntamente por el proceso de Sistemas de Información.
- Todos los medios impresos, diskettes, CD-ROM, memorias USB, o cualquier otro medio extraíble diferente a los equipos de cómputo autorizados, en que se almacene información, deben ser protegidos de usuarios y/o terceros no autorizados para acceder dicha información.
- Todos los medios impresos, diskettes, CD-ROM, memorias USB, o cualquier otro medio extraíble que por cualquier motivo se deseche debe ser destruido para evitar el acceso de usuarios y/o terceros no autorizados para acceder a dicha información.
- Proveedores o terceras personas solamente deben tener acceso a la información durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.
- Es deber de todos los usuarios no divulgar ni revelar información confidencial de la E.S.E. HUS de su conocimiento por ningún medio telefónico, mensajería instantánea, correo electrónico personal, reuniones informales o lugares públicos. La información confidencial en medios impresos no debe estar al alcance de personal no autorizado. No se deben dejar estos documentos en fotocopiadoras, impresoras o faxes, ni en lugares de fácil acceso (sin llave o a la vista).
- Toda información (documentos, correo electrónico, actas, etc.) que se utilice como evidencia en caso de un incidente de seguridad, y que involucre consecuencias o acciones legales; debe ser recolectada, conservada y presentada, protegiendo también su integridad.
- La información relevante y personal de los pacientes y de los colaboradores de la ESE HUS debe ser resguardada adecuadamente, con el fin de evitar accesos no autorizados o por terceros para fines no institucionales o que violen requerimientos legales vigentes.

7.18.7. Uso de Cuentas y Contraseña

Los usuarios son responsables de las claves de acceso al equipo de cómputo y a los diferentes sistemas de información, y a su vez del cambio de las mismas periódicamente. Cualquier uso indebido que se haga de la respectiva contraseña por negligencia de los funcionarios, acarreará las sanciones disciplinarias y judiciales establecidas. Por lo mencionado anteriormente, los usuarios son responsables de no revelar sus contraseñas de acceso a terceros con el fin de evitar inserción, modificación y/o eliminación en nuestros sistemas de información.

Las contraseñas críticas (servidores, bases de datos, administración de aplicaciones y demás equipos de red) deben

manejar un mayor nivel de seguridad y complejidad. Igualmente se debe establecer un nivel de autorización para su correcta utilización; no deben ser del conocimiento de más de 3 personas. Se debe documentar los fines de utilización de estas claves, modificaciones y registrar los responsables por las mismas.

El proceso de Sistemas de Información asigna las contraseñas para acceder a los sistemas de información, se asignan de manera individual recomendando que se cumplan con los siguientes criterios:

- Permitir que los usuarios seleccionen y cambien sus propias contraseñas.
- Sugerir que escojan una contraseña segura y que esta se cambia de forma regular.
- Recomendar a los usuarios a cambiar su contraseña cuando ingresan por primera vez.
- La longitud mínima de caracteres permisibles en una contraseña se establece en 5 caracteres, los cuales tendrán una combinación alfanumérica.
- Cada usuario deberá mantener de forma confidencial y queda prohibido divulgar o prestar su contraseña.
- El usuario debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancias de ellas, a menos que esta sea guardada en un lugar seguro.
- El usuario será responsable por el acceso a todos los recursos informáticos que sean realizados con su usuario y contraseña.

7.19. CUSTODIA Y SEGURIDAD DE LA HISTORIA CLÍNICA

- Las solicitudes de copia de la historia clínica serán atendidas por el proceso de Estadística de la E.S.E Hospital Universitario de Santander. Este servicio se presta en días y horas laborales, de acuerdo al Procedimiento de Entrega y Préstamo de Historias Clínicas a Clientes Internos y Externos (GII-EST-PR-02).
- Para la consulta de la historia clínica electrónica se establecen privilegios de acceso al personal de planta, personal contratista y/o terceros de acuerdo con el desarrollo de sus funciones y competencias. Estos privilegios serán establecidos por cada subgerente o profesional de planta de los procesos a las que correspondan el personal.
- Solo es permitida la entrega de resúmenes o copia de la historia clínica a través del proceso de estadística. Está totalmente prohibido imprimir folios de Historia Clínica para ser entregados al usuario y/o terceros

7.20. TÉRMINOS Y CONDICIONES PARA FUNCIONARIOS Y/O COLABORADORES

- Todo el personal, contratista y/o tercero definido por la E.S.E. Hospital Universitario de Santander, deberá regirse al presente manual.
- Los empleados y contratistas de la E.S.E Hospital Universitario de Santander, que tengan acceso a información deberán firmar un acuerdo de confidencialidad y no divulgación antes de tener acceso al procesamiento de la información.
- El proceso de talento humano hará firmar al personal de planta nuevo de la E.S.E Hospital Universitario de Santander el acuerdo de confidencialidad, a su vez los supervisores solicitan la firma del acuerdo de confidencialidad del personal de la E.S.E HUS contratistas.

7.21. ASIGNACIÓN DE USUARIO

- La E.S.E Hospital Universitario de Santander, estableció el **Procedimiento Creación o Acceso e Inactivación de Usuario a la Red y Sistemas de Información (GII-SIS-PR-02),** mediante el cual se define los criterios para crear el ingreso, retiro o inactivación de los usuarios, con acceso y seguridad a la red de datos y sistemas de información y se conceden permisos de acceso a los sistemas de información de acuerdo al perfil solicitado.
- El proceso de Sistemas de Información estableció el **Formato Solicitud Usuario a Red y Acceso Aplicativos** (**GII-SIS-FO-17)**, mediante el cual se crean los usuarios para el acceso a la red y a los sistemas de información de la E.S.E Hospital Universitario de Santander y se conceden permisos a estos mismos.
- El proceso de Sistemas de Información crea las cuentas con el perfil requerido en la solicitud de creación de usuarios, tramitada y aprobada por el jefe de planta de la E.S.E. HUS o el subgerente correspondiente al

proceso

7.22. CANCELACIÓN DEL REGISTRO DE USUARIO

- Cuando el personal vinculado a la institución termina su vinculación, se cuenta con un Formato Paz y Salvo (GTH-RTH-FO-08), el cual es firmado por los principales procesos de la institución en el cual se indica que la persona no tiene pendientes con la institución.
- Cada Macroproceso deberá informar al proceso de Sistemas de Información, cuando se presente un cambio o se retire personal a su cargo, para que el usuario sea deshabilitado de los sistemas de información de la E.S.E Hospital Universitario de Santander.
- Desde el proceso de sistemas de información se dispone del Formato Entrega de Activos de Información (GII-GEI-FO-07), para la entrega de activos de información por parte de los colaboradores y terceros vinculados con la institución.
- De igual manera desde la parte contractual se genera una cláusula en los contratos firmados con las empresas que prestan servicios a la institución donde se estable el cuidado y manejo de la información, incluyendo la entrega de la información una vez finalice el contrato.

7.23. PROCESO DISCIPLINARIO

- La E.S.E Hospital Universitario de Santander, toma acciones pertinentes para el funcionario vinculado con el incidente, mediante un proceso disciplinario formal de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la organización dicho incidente de acuerdo a los procedimientos establecidos por la oficina de Control Interno Disciplinario.
- La oficina de Control Interno Disciplinario definió el Manual de Inducción en Materia Disciplinaria (GJU-DJE-MA-03) y el Procedimiento de Control Interno Disciplinario (GJU-DJE-PR-03).
- El proceso disciplinario no se deberá iniciar sin antes verificar que ha ocurrido una violación a la seguridad de la información.
- El proceso disciplinario también se deberá usar como elemento disuasivo para prevenir que los empleados violen las políticas y procedimientos de seguridad de la información.

7.24. PROCESO DISCIPLINARIO EJECUTORES

- Para los ejecutores de los procesos tercerizados se reportará el incidente a la empresa contratista para realizar el respectivo trámite.

7.25. CONTROLES DE ACCESO FÍSICOS

- La E.S.E. Hospital Universitario de Santander cuenta con áreas en donde se almacena y procesa información, las cuales cuentan con controles de acceso apropiados para asegurar que solo se permite el ingreso a personal autorizado.
- El acceso a las áreas de procesamiento y/o almacenamiento de información se da a los usuarios autorizados solamente mediante la implementación de controles de acceso apropiados y mediante mecanismos de autenticación como el carnet o tarjetas de acceso.
- La llave de seguridad que da acceso a los medios de almacenamiento como el Data Center se encuentra resguardada bajo estricta seguridad por el proceso de Sistemas de Información.

7.26. ACUERDOS SOBRE CONFIDENCIALIDAD

- Todo el personal, contratistas y/o terceros que presten sus servicios a la E.S.E Hospital Universitario de Santander, deben aceptar los acuerdos de confidencialidad definidos por la institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.
- Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la

cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

7.27. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

- La E.S.E Hospital Universitario de Santander, vela porque todos los recursos informáticos estén protegidos mediante herramientas y software de seguridad como Antivirus que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional.
- Los servidores al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activa la protección en tiempo real.
- Para los equipos de cómputo que son entregados como medios de producción por parte del contratista, deberán realizar la instalación de software de solución antivirus, para proteger sus equipos ante cualquier software malicioso.

7.28. GESTIÓN CON ALIANZAS ESTRATEGICAS

Todas las empresas contratistas que por actividades internas tengan un contrato con la E.S.E Hospital Universitario de Santander, deberán acogerse a los siguientes lineamientos:

- Toda empresa contratista deberá cumplir con los lineamientos de seguridad de la información establecidos en la E.S.E Hospital Universitario de Santander.
- Toda empresa contratista debe garantizar la contingencia de cada uno de los equipos de cómputo y de oficina en caso de mantenimiento, daño, o pérdida cumpliendo con las especificaciones mínimas solicitadas.
- El contratista debe realizar un mantenimiento preventivo cada 6 meses a la totalidad de equipos informáticos y mantenimiento correctivo cada vez que se requiera.
- El contratista se compromete y es el responsable que todo el software instalado en cada uno de los computadores que hagan parte de los medios de producción debe ser legal y debidamente licenciado
- El contratista se hace responsable por la legitimidad de marca o patentes relacionadas con los componentes lógicos de los equipos y sistemas ofrecidos.
- El contratista se hace responsable por las reclamaciones que pueda presentarse por concepto de violación a las patentes, licencias o manifiesto de importación, de la calidad de materiales, etc. Y serán por su cuenta todos los gastos que puedan ocasionarse por tal concepto.
- El contratista participa en las sesiones que sean necesarias para la capacitación en las herramientas software que disponga Ese Hospital Universitario de Santander.
- El contratista debe evidenciar que cada uno de sus ejecutores conoce y aplica las políticas de seguridad de la información de la E.S.E. Hospital Universitario de Santander.
- La E.S.E Hospital Universitario de Santander será el único dueño de los derechos de autor de los desarrollos que se realicen internamente, las empresas contratistas deberán respetar su confidencialidad.

8. DOCUMENTOS DE REFERENCIA

- Ley Estatutaria 1581 de 2012: y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan 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 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.
- 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. "Ley 1341 DE 2009: Por medio de la cual se definen 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.
- Norma ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.

9. SOCIALIZACIÓN

Una vez aprobado este procedimiento, es responsabilidad del líder del macroproceso y el responsable del proceso 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, la cual debe ser enviada 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**
2	Abril de 2022	Actualización de acuerdo a los lineamientos institucionales y normatividad vigente.	Sergio Alexander Galvis Profesional Universitario UFATI	Nelly Méndez Mesa Profesional Especializado UFATI	Juan Carlos Supelano Subgerente Administrativo y Financiero