Contenido

Introducción

El Hospital San Juan Bautista E.S.E, reconoce y determina la Información como un activo de gran valor e importancia que permite el desarrollo y ejecución de los procesos misionales, administrativos y financieros, permitiendo que los objetivos descritos en el plan de gestión y de desarrollo de la alta gerencia sean ejecutados de acuerdo a los lineamientos establecidos, garantizando los principios de Seguridad – Integridad y Portabilidad de la información.

El presente manual permite establecer las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, y su adopción por parte de los grupos de interés determinados en la política general de tratamiento de la información (usuarios directos,indirectos,terceros relacionados y entidades externas) y funcionarios, contratistas, personal en comisión administrativa o misional, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la E.S.E.

Objetivo

Establecer las políticas de seguridad y privacidad de la información para el Hospital San Juan Bautista E.S.E. a través de elementos y regulaciones en el uso adecuado de la información física y digital, bajo el liderazgo de la alta gerencia y área de gestión informática de sistemas.

Alcance

La política de seguridad y privacidad de la información será aplicada a todos los procesos misionales, administrativos y financieros de la E.S.E. y será de cumplimiento obligatorio por parte de los grupos de interés determinados en la política general de tratamiento de la información y funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la E.S.E.

Las excepciones al cumplimiento de las políticas de seguridad de la información, serán autorizadas única y exclusivamente por la alta gerencia, el área de gestión informática y/o el comité de seguridad de la información de la E.S.E, cuando sea considerado un obstáculo o genere un impacto negativo en el funcionamiento de los procesos institucionales.

Definiciones

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Aceptación del Riesgo: Después de revisar las consecuencias que puede acarrear el riesgo, se toma la decisión de afrontarlo.

Activo: Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y administrativos y financieros de la E.S.E. Se pueden clasificar de la siguiente manera:

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

- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información. Ejemplo: Hosvital HIS.

- **Personal:** Es todo el personal del E.S.E, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del E.S.E.

- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.

- **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones.

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

- **Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos.

- **Administración de riesgos:** Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

- **Administración de incidentes de seguridad:** Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

  Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

  - Detectar cualquier alteración en los servicios TI.
  - Registrar y clasificar estas alteraciones.
  - Asignar el personal encargado de restaurar el servicio.
  - APT: (Advance Persistent Threat) Amenaza Avanzada Persistente Especie de ciberataque que es responsable del lanzamiento de ataques de precisión y tienen como objetivo comprometer una máquina en donde haya algún tipo de información valiosa.

- **Alcance:** Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

- **Alerta:** Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

- **Almacenamiento en la Nube:** Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan esos archivos.

- **Amenaza: Según [ISO/IEC 13335-1:2004):** causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Análisis de riesgos**: A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

- **Auditabilidad:** Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

- **Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
  Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

  Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

  Datos Personales Públicos: 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. (Decreto 1377 de 2013, art 3).

  Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

  Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

  Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquello 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.

  Información Pública Reservada: Es aquella información que estando en 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 del artículo 19 de la ley 1712 de 2014

  Información Pública Clasificada: Es aquella información que estando en 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.

  Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Normatividad

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 1581 de 2012 Por la cual se dictan disposiciones generales para la Protección de Datos Personales

Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

CONPES 3584 de 2016 Política nacional de seguridad digital

Decreto 0886 de 2014 por el cual se reglamenta el Registro Nacional de Bases de Datos, cuya creación se estableció dentro del Régimen General de Protección de Datos Personales (Ley 1581 de 2012).

Ley 1273 de 2009 Ley del delito informático

Ley 1266 de 2008 por el cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en las bases de datos personales, en especial la financiera, crediticia, comercial De servicios, y la proveniente de otros países y se dictan otras disposiciones.

Política de Tratamiento de la Información

POLITICA DE TRATAMIENTO DE LA INFORMACIÓN HOSPITAL SAN JUAN BAUTISTA E.S.E. CHAPARRAL TOLIMA

El HOSPITAL SAN JUAN BAUTISTA E.S.E. de CHAPARRAL TOLIMA, NIT 890.701.459-4, en cumplimiento de la ley estatutaria 1581 de 2012 y su Decreto reglamentario N° 1377 de 2013, sobre la privacidad y protección de datos personales en Colombia, asegura el manejo adecuado de la información que obtenga, registra, use, transmita y actualice mediante la autorización previa, expresa y voluntaria del titular de la información y actúa como responsable del tratamiento y custodia de los datos personales que por virtud de sus funciones y competencias legales establecidas le han sido suministradas a la entidad, con los cuales tiene, ha tenido o espera tener algún tipo de relación, cualquiera sea su naturaleza (Civil, Comercial y/o Laboral etc.), incluyendo pero sin limitarse, los grupos de interés (usuarios directos, usuarios indirectos, terceros relacionados y entidades externas).

En virtud de los procesos misionales y administrativos del Hospital San Juan Bautista E.S.E. de Chaparral Tolima, enmarcados en los modelos de atención tratamientos médicos, se compromete que la información recolectada, almacenada, usada, transferida o eliminada tendrá los procesos adecuados y documentados con las descripciones de acuerdo a las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso que establezca la ley y normatividad vigente.

Dada en el municipio de Chaparral, a los 9 días del mes de enero de 2018.

DIANA PATRICIA BUENAVENTURA JIMÉNEZ
Gerente
Hospital San Juan Bautista E.S.E.
Chaparral Tolima

Roles y Responsabilidades

Rol	Responsabilidad
Comité de seguridad y privacidad de la información	• Impulsar la implementación del Sistema de Gestión de Seguridad de la Información SGSI en la E.S.E. • Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SGSI de los procesos institucionales de la E.S.E. • Supervisar la integración del Sistema de Gestión de Seguridad de la Información - SGSI con el Sistema Integrado de Gestión de la Información. • Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información para la E.SE. • Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos de la seguridad de la información para la E.S.E, con el fin de tomar y establecer las medidas necesarias. • Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de Información de la entidad. • Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información. • Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación. • Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello. • Evaluar los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información. • Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información. • Las demás funciones inherentes a la naturaleza del Comité.
Responsable de Seguridad de la Información U Oficial de Seguridad de la Información CIO.	• Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias de las políticas de seguridad y privacidad. • Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo. • Capacitar, socializar e implementar acciones que permitan el cumplimiento, seguimiento y control de las políticas de seguridad definidas. • Trabajar de manera integrada con el grupo o áreas asignadas. • Custodiar y velar por la aplicación y mantenimiento de las políticas de seguridad definidas • Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
Personal de interés: • **Funcionarios.** • **Usuarios Internos.** • **Usuarios externos.**	• Apoyar al CIO (Oficial de Seguridad de la Información) al interior de la entidad. • Informar sobre los incidentes de seguridad presentadas en los activos de información o dudas presentadas en procedimientos o políticas definidas.

• **Contratistas.** • **personal que haga uso de los activos de información de la E.S.E.**	• Ayudar al CIO designado, en la gestión de proveedores de tecnología e infraestructura. • Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el CIO. • Las que considere el CIO o el comité de seguridad de la entidad. • Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales. • Tramitar las consultas, solicitudes y reclamos. • Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran. • Respetar las condiciones de seguridad y privacidad de información del titular. • Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

Políticas de Seguridad de la Información.

Política de estructura organizacional de seguridad de la información

El Hospital San Juan Bautista E.S.E en cumplimiento con el Sistema de Gestión de Seguridad de la Información, conforma el esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades de acuerdo a los procesos y procedimientos Misionales, Administrativos y Financieros de la E.S.E., la conformación del Comité de Seguridad de la Información y el administrador de la seguridad de la Información.

A través del área de Gestión Informática de Sistemas se establecerán los roles, funciones y responsabilidades de operación y administración de los sistemas de información por parte de los funcionarios y/o personal de interés, los cuales deberán están documentadas y distribuidas.

Política de seguridad para los recursos humanos

La E.S.E implementa acciones que permitan que los funcionarios y personal de interés, entiendan las responsabilidades como usuarios y roles asignados, con el fin de reducir el riesgo de fraude, filtraciones, o uso inadecuado de la información y las instalaciones

Los aspirantes, contratistas y proveedores deberán dar su consentimiento y aprobación para el tratamiento de los datos personales de acuerdo a la ley 1032 de 2006, por la cual se dictan disposiciones generales del Habeas Data y es regulado el manejo de la información contenidas e las bases de datos, estas serán reflejados en las cláusulas de los contratos.

Se debe realizar capacitación y socialización a los funcionarios durante la inducción sobre las políticas de seguridad de la información, establecidas en la E.S.E.

El funcionario o contratista debe entregar los activos de información, cuando se realice la terminación de su contrato por cualquiera de las partes o en mutuo acuerdo, mediante acta de entrega o documento que lo reemplace y debe ser verificado por el supervisor del contrato o jefe directo del servicio.

Política de gestión de activos de Información

La E.S.E es la propietaria de los activos de la información y los administradores de estos activos son los funcionarios, contratistas y demás personal que hace uso directo de ellos a los cuales se denominaran "Usuarios", que se encuentren debidamente autorizados y sean responsables por la información de los procesos que se encuentren a su cargo, de los sistemas de información, aplicaciones informáticas, plataformas de acceso, hardware e infraestura de tecnologías de la información y las comunicaciones.

La E.S.E debe tener actualizado el catalogo de activos de la información, de acuerdo a la guía MINTIC de catálogos de servicios, la cual será adoptada por la institución, dejándolo bajo la responsabilidad de cada propietario de la información y centralizado por el área de gestión informática de sistemas.

La E.S.E. debe realizar el tratamiento de la información de acuerdo a lo establecido en el manual de gestión documental.

Política de uso de las estaciones de trabajo clientes

La instalación de software en las estaciones de trabajo de la E.S.E. es una función exclusiva de área de gestión informática de sistemas y su proceso de instalación e indicaciones se encuentra establecidos en el Manual Instalación Estación de Trabajo.

Los usuarios que hagan uso de equipos institucionales en calidad de préstamo, NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso.

Los usuarios no deben almacenar en las unidades de disco duro información de tipo multimedia (Imágenes, texto, videos y audio) o cualquier tipo de información que no sea de carácter institucional.

En la unidad de almacenamiento o partición Disco Local C:\, se localizarán los archivos y directorios propios del sistema operativo y de los sistemas de información que son de uso institucional, los usuarios no deberán realizar modificaciones a dichos archivos y directorios, al igual que las configuraciones de redes y demás.

Los equipos que ingresan temporalmente a la E.S.E y que son propiedad de terceros, deberán ser registrados en el control de acceso a la institución, al igual que su retiro, la E.S.E. no se responsabiliza en caso de perdida o daño relacionado con dicho equipo.

Los equipos de uso personal y que nos son de propiedad de la E.S.E. solo tendrán acceso a servicios limitados y deben ser autorizados por el jefe directo o de dependencia y su configuración se realizara exclusivamente por el área de gestión informática de sistemas.

Política de uso de Internet y publicaciones en sitio web interno y externo.

La E.S.E permite la navegación a servicios de internet mediante unos lineamientos basados en acceso y trafico seguro, permitiendo de esta manera el uso adecuado del servicio.

El acceso a plataformas de streaming, ocio, redes sociales y similares se encuentran restringidas a través de un datacenter externo administrado por el proveedor de servicio, al igual que la apertura de puertos y control de tráfico entrante y saliente, para el caso de habilitación de puertos o acceso a alguna plataforma que se encuentre bloqueado o no permita la navegación total se debe elevar la solicitud al área de gestión informática de sistemas, quien tendrá 24 horas para permitir el acceso a dicha plataforma, siempre y cuando esta plataforma o sitio web sea importante para el debido proceso del cumplimiento de los objetivos de la E.S.E.

Para la realización de las publicaciones en los sitios institucionales, el jefe de dependencia deberá elevar la solicitud al área de gestión informática de sistemas, en el cual deberá dar un descripción u objeto de la publicación, determinando el tiempo de la publicación, tipo de sitio institucional.

La solicitud de habilitación de puertos o sitios web y publicaciones en sitios web institucionales, se debe realizar mediante el formato Transmisión de Datos e Información.

Política de clasificación de la información.

El Hospital San Juan Bautista E.S.E. como responsable del tratamiento y custodio de la información, define la clasificación de la información de acuerdo al inventario de activos elaborado y asignado a cada responsable de la información y proceso.

De acuerdo a lo anterior podemos tener diferentes formatos y medios:

- Los documentos de carácter electrónico.
- Bases de datos.
- Documentos en formato papel.
- Correos electrónicos.
- Medios de almacenamiento.
- Información verbal.

Los usuarios y responsables deben identificar los riesgos a los que se encuentran expuesta la información en sus áreas, teniendo en cuenta que la información puede ser copiada, divulgada, eliminada, modificada física y digitalmente por personal interno o externo, de acuerdo al marco normativo legal expuesto en este manual y al vigente.

Los usuarios y grupos de interés deben tener pleno conocimiento sobre el tipo de información que fue clasificada, garantizando la confidencialidad, seguridad e integridad de la misma.

La divulgación o copia de la información catalogada como **Información Pública de Reserva o Información Publica Clasificada** según su **CONFIDENCIALIDAD** enmarcada en el artículo 19 de la ley 1712 de 2014, debe ser de estricto control en cualquiera de sus formatos, en especial en el físico, al momento de reutilizar el papel generado en la institución.

Política de manejo disposición de información, gestión de medios y equipos.

Las estaciones de trabajo y medios donde se almacena, procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo deben ser usados únicamente para el cumplimiento de la misión y procesos administrativos o financieros de la Entidad.

La administración de la información almacenada en las estaciones de trabajo y medios, es responsabilidad directa del usuario, en caso de la realización de una copia de seguridad, el área de gestión informática de sistemas prestara el apoyo necesario para la realización del proceso de acuerdo a los recursos disponibles en el momento.

Las estaciones de trabajo o medios que requieran ser trasladados a otra área, deben cumplir con el proceso establecido de traslados de activos institucionales o con la autorización del personal a cargo de los activos y del jefe de dependencia, una vez se encuentre autorizado el área de gestión informática de sistemas realizara un diagnóstico de las instalaciones, determinara recurso físico y el tiempo necesario, generara las copias de seguridad y borrado de la información de las estaciones de trabajo involucradas en el traslado.

El acceso a redes inalámbricas por parte del personal de interés de la E.S.E. debe contar con la autorización del área de gestión informática de sistemas, quien realizara las configuraciones pertinentes sobre los equipos en mención.

El uso de los puntos de red es exclusivo de las estaciones de trabajo y medios institucionales, se prohíbe el cambio, desconexión o conexión de los puntos de red, el área de gestión informática de sistemas es el único que puede realizar dichos cambios.

Política de control de acceso

Dentro de la política que se generan para el control de acceso la E.S.E encontramos las siguientes:

Ingreso a los sistemas de información Misionales, Administrativos y Financieros: para el ingreso a los sistemas de información el jefe de dependencia o jefe inmediato deberá elevar la solicitud mediante el correo electrónico, indicando los datos personales del nuevo funcionario, perfil que se otorgará y tipo de aplicación que requiere el acceso, el cual se dará respuesta por el mismo medio, aplica también para el cambio de rol o perfil.

Las conexiones remotas a la red LAN de la institución se realizará a través de la VPN institucional, el cual deberá ser autorizado por el jefe inmediato o de dependencia, el área de gestión informática de sistemas es el único que realizara la instalación y configuración del agente VPN institucional.

Todo aplicativo informático o software debe ser aprobado por el área de gestión informática de sistemas en concordancia con la política de adquisición de bienes de la E.S.E. de acuerdo con lo definido en el manual de compras.

Para el uso de plataformas online o web que sean suministrado por usuarios externos, proveedores o instituciones que tienen un vínculo contractual con la E.S.E, el apoyo técnico de configuración y adecuación será suministrado por el área de gestión informática de sistemas, pero la administración de los usuarios asignados serán estrictamente responsabilidad del área que haga uso de ellas.

Las cuentas de correo electrónico institucional, requiere autorización escrita o E-mail por el jefe de dependencia para su creación y estará sujeta al nombre del área o unidad funcional, no a nombre propio del usuario, con el fin de permitir acceso a la información a personal propio del área en caso de un evento no planeado, la información contenida en cada cuenta es propiedad de la E.S.E.

- La administración de la información, bandejas de almacenamiento y copias de seguridad o similares de las cuentas electrónicas son responsabilidad directa del personal de interés a quienes se les asignan, el área de gestión informática de sistemas prestara el apoyo necesario para la realización de algún proceso en la cuenta electrónica se lleve a cabo de acuerdo a los recursos disponibles en el momento.

- Bajo ninguna circunstancia se debe fomentar las cadenas o correo SPAM tanto al interior como al exterior de la Institución. Estas cadenas atentan contra la seguridad y el buen rendimiento de la red, por lo tanto, quedan totalmente prohibidas.

El usuario y contraseña asignado para el ingreso a los sistemas de información institucionales, es único e intransferible, por lo tanto, el préstamo o suplantación de él, es responsabilidad directa del funcionario, contratista o personal de interés al que le fue asignado.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose al área de gestión informática de sistemas, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser solicitada por el jefe de dependencia a través de un correo electrónico.

Es responsabilidad del usuario terminar o realizar cierre de las sesiones activas que tiene en uso en los sistemas de información una vez finalice el registro de la información.

El bloqueo de sesión del usuario asignado a la estación de trabajo se ejecutará 10 minutos después de inactividad, cerrando automáticamente la conexión de red y obligando el cierre forzado de los sistemas de información institucionales.

El personal del área de gestión informática de sistemas debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.

El ingreso al área de servidores y datacenter principal del personal de interés de la E.SE. será de estricto control y vigilancia liderado por el área de gestión informática de sistemas o los jefes de área en donde se encuentren estos recursos.

El personal de interés como funcionarios y contratistas deberán hacer uso del correo electrónico asignado por la E.S.E. como responsable del tratamiento de la información del área que representa, la transmisión de la información institucional como activo de esencial, debe ser uso exclusivo de la E.S.E. por ende es de estricta obligatoriedad el uso de la cuenta electrónica institucional, y la E.S.E está en completa autonomía de acceder a ella en caso de requerirse.

Política de adquisición, desarrollo y mantenimiento de sistemas de información

Para el caso de desarrollos de interfaces, web services o similares, se deberá realizar y confirmar su funcionalidad a través de un ambiente de pruebas preestablecido.

El área de gestión informática de sistemas junto con el área beneficiada o relacionada en la adquisición o desarrollo de un sistema de información, deberán realizar las pruebas necesarias en el ambiente de pruebas y posteriormente dar su diagnóstico o aval de inicio en ambiente de producción.

La E.S.E. adquirirá el software requerido necesario para la ejecución de los procesos de las áreas involucradas en coordinación con el área de gestión informática de sistemas, quien establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas en la arquitectura de hardware, software, de red y de comunicaciones.

El área de gestión informática de sistemas será la única dependencia autorizada para realizar copia de seguridad del software original.

La instalación de software o aplicativos en los activos informáticos se realizará a través del área de gestión informática de sistemas.

El área de gestión informática de sistemas tiene implementado el manual de instalación de estación de trabajo, dentro del cual esta estipulado el paso a paso y el software o aplicativos utilizados en la institución de acuerdo a los procesos asistenciales y/o administrativos.

El software adquirido por la E.S.E. no podrá ser copiado, divulgado o suministrado a terceros.

En caso de requerirse la instalación de alguna aplicación o software específico por parte del usuario en el cual la licencia es de uso comercial o viola en algún momento los derechos de autor, se debe realizar nueva solicitud de servicio para la instalación mediante el formato **PA-GSI-ARI-R1 (V1) Mantenimiento de Equipos Informáticos,** en cuyo caso se debe buscar una solución de TI de tipo software libre, por el contrario, estas solicitudes deben ser llevados a comité MIPG para su análisis y proceder.

La E.S.E. adquirirá el hardware requerido necesario para la ejecución de los procesos de las áreas involucradas en coordinación con el área de gestión informática de sistemas, quien establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas en la arquitectura de hardware, software, de red y de comunicaciones.

La E.S.E. adquirirá estaciones de trabajo, servidores, nodos de comunicación y/o componentes de arquitectura de Red, de comunicaciones y de hardware, requerido y necesario para la ejecución de los procesos de las áreas involucradas o del sistema de información, en coordinación con el área de gestión informática de sistemas, quien establecerá claramente los requerimientos funcionales, operacionales y especificaciones requeridas.

El líder de proceso del área de gestión informática de sistemas asistirá y establecerá claramente las especificaciones técnicas de arquitectura de red, de comunicaciones y de estaciones de trabajo de acuerdo a la norma y estándares internacionales de cableado estructurado, en el momento que la E.S.E. planee o realice algún tipo de cambio en la estructura edilicia, con el fin de garantizar el correcto funcionamiento del sistema de información y evitar traumatismos posteriores en los procesos misionales, administrativos y financieros.

Política de respaldo y restauración de información

El área de gestión informática de sistemas realiza respaldo del sistema operativo y aplicaciones instaladas en las estaciones de trabajo clientes, mediante las particiones creadas de protección del sistema (Restauración del sistema), determinando un 10% de almacenamiento en disco de acuerdo a la partición generada del disco local C:/, este respaldo se realiza solo para las configuraciones del software de aplicación y de sistema, no aplica a la información almacenada en las unidades de disco de la estación de trabajo cliente.

El área de gestión informática de sistemas, al momento de instalar y configurar una nueva estación de trabajo o al realizar el mantenimiento preventivo, configura las particiones de almacenamiento de información de los usuarios, particularmente en una partición diferente del disco local C:/. Generando de esta forma una posibilidad de recuperación de la información y restauración del sistema de operativo y demás aplicaciones mucho más rápidas en caso de algún incidente con la estación de trabajo.

El área de gestión informática de sistemas prestara el apoyo necesario para la realización del proceso de respaldo o copia de seguridad de acuerdo a los recursos disponibles en el momento, la administración de la información (crear, almacenar, eliminar, transportar, consultar, modificar o actualizar, **respaldar** y cualquier tipo de proceso o actividad que se ejerza en la información) de la estación de trabajo cliente, es responsabilidad directa del usuario que la utiliza.

El respaldo de las bases de datos centralizadas en los servidores de los diferentes servicios de tecnología de la información se realiza de forma completa y de acuerdo a los siguientes periodos:

- **Sistema de Información Hosvital HIS:** Las copias de seguridad de las bases de datos que comprenden el sistema de información Asistencial y Financiero de la institución, se realizan a través de una tarea programa en el administrador de la base de datos diariamente la cual inicia desde las 00:00 horas del día, es decir se realiza una copia de seguridad cada 24 horas y el tipo de copia de seguridad es Backup completo, el tiempo de finalización de la copia depende del tamaño de la base de datos, a hoy se encuentra en 03 horas y se realiza paralelamente a las conexiones que se encuentren activas en el momento.

  El archivo .bak generado de la copia de seguridad es almacenado directamente a un disco duro externo con capacidad de 4Tb, los cuales 3.63 Tb son realmente el disponible para el almacenamiento, es decir aproximadamente es capaz de almacenar 18 copias diarias junto con el informe de resultado de las copias, lo cual obliga a la liberación manual de espacio del disco, es decir para garantizar el espacio de almacenamiento en el disco externo reposaran las copias de seguridad completa de los últimos 10 días .

- **Sistema de Información Canvas:** Las copias de seguridad que corresponden al sistema de información de imagenología, se realiza mensualmente a través de una imagen de disco completo del Workstation en donde se encuentran almacenada la BD y los archivos tipo DICOM, el peso

promedio de la BD e Imágenes de la copia de seguridad es de 1 Tb con tendencia a incrementar diariamente, la realización corresponde al proveedor de servicio.

- **Sistema de Información IWANA:** Las copias de seguridad del sistema de información de gestión documental, se realizarán semanalmente, generando un respaldo de los documentos adjuntos, el sitio web y la base de datos, a un disco externo en el cual se mantendrá la última copia realizada por el volumen de información.

- **Carpetas y unidades de Red:** las copias de seguridad de las carpetas y de las unidades de red conectadas a cada estación de trabajo se realizarán por cada cambio que se realizan en ellas y se establecerán en un disco externo.

- **Servicios de Intranet:** Las copias de seguridad de los servicios web internos como el sitio web Mi Hospital, Nextcloud y el Mensajero Instantáneo Spark, se realizarán Mensualmente en unidades externas, debido a que las publicaciones y recurso compartidos en ellas son copias de la información original que contiene los usuarios y las estaciones de trabajo.

Mensualmente se genera un informe de copias de seguridad en donde se exponen el estado, el proceso y el historial de riesgo que se tuvo en el proceso.

Política de registro y eventos de los servicios de tecnología de la Información.

El área informática de sistemas de información garantiza el registro y seguimiento de los eventos ocasionados en los servicios de tecnología de la información como lo son: Servidores de datos, Dominio, Sistema de Información Financiero, Imágenes y de comunicaciones que se encuentran a cargo del área, a través de logs que se generan automáticamente en cada suceso o evento de cada servicio.

La manipulación directa o indirecta de cada registro de actividades y sucesos esta estrictamente prohibida hacia el personal del área de gestión informática de sistemas quienes son los únicos autorizados para la administración.

Los registros de eventos y logs generados en cada uno de los servicios son utilizados solo para realizar análisis de estados e incidentes ocasionados durante la utilización de los servicios de TI, y para la generación de los informes requeridos de disponibilidad de servicios de TI.

Trimestralmente se genera un informe de disponibilidad de servicios de TI y Comunicaciones, basados en los logs transaccionales y registro de eventos de los sistemas de Información.

Política de Incidentes y Vulnerabilidad de seguridad de la Información

El comité de seguridad y privacidad de la información estable los responsables y procedimientos de gestión para el tratamiento de incidentes de seguridad de la información, determinando quienes investigaran y solucionaran el incidente de acuerdo a las acciones presentadas y generando lecciones aprendidas para que no se repitan nuevamente y sirvan de análisis para el mejoramiento de la seguridad de la información.

El comité de seguridad y privacidad de la información designara al área informática de sistemas para dar respuesta a los eventos e incidentes de seguridad de la información que de una u otra forma se generen a través de los canales de tecnología de la información, quien elaborara un informe sobre el incidente y mecanismos de seguridad que eviten nuevamente el incidente.

El personal de interés deberá reportar al líder de proceso o jefe de dependencia, los incidentes de seguridad de la información generados, quien a su vez los escalará al área de gestión informática de sistemas que determinará el riesgo. Elaborara el informe y lo presentara al comité de seguridad y privacidad de la información para su análisis y acciones correspondientes.

El comité de seguridad y privacidad de la información estudiara los incidentes presentados al interior de la E.S.E y determinara las acciones correctivas de acuerdo al análisis realizado y la normatividad vigente disciplinaria.

El área de gestión informática de sistemas implementa la metodología de gestión del riesgo para el tratamiento y los planes de tratamiento periódicamente para minimizar las vulnerabilidades presentadas en los sistemas de información de la E.S.E.

Política de cumplimiento

Las políticas y normas definidas en el presente manual son de estricto cumplimiento y obligatoriedad por el personal de interés (funcionarios, contratistas, usuarios externos) y personal relacionado con el uso y administración de la información y las tecnologías de la información existentes en la E.S.E.

El presente manual pretende establecer el buen uso de las tecnologías de la información y su aplicabilidad permitirá prevenir y mitigar el riesgo al cual se encuentran los activos de información institucionales durante la ejecución de los procesos misionales, administrativos y financieros.

Número	Fecha Aprobación	Ítem Alterado	Motivo	Realizado por
01	25/10/2019	No Aplica	No Aplica	Técnico Administrativo Sistemas