ESE ANA SILVIA MALDONADO JIMENEZ

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

COLOMBIA - HUILA
2025

Elaborado por:	Revisado por:	Aprobado por:
Nombre: LILIANA MARCELA CASTRO JIMENEZ	Nombre: LILIANA MARCELA CASTRO JIMENEZ	Nombre: EDUARDO MAHECHA REYES
Cargo: TESORERA	Cargo: TESORERA	Cargo: GERENTE

CONTENIDO

1. INTRODUCCIÓN

El E.S.E. Ana Silvia Maldonado Jiménez de Colombia, siguiendo las directrices de Gobierno Digital, establece como prioridad la gestión de la seguridad de la información; razón por la cual establece un marco mediante el cual se asegura que la información es protegida de una manera adecuada como complemento indispensable para el logro de resultados y la consecución de objetivos estratégicos institucionales.

Este manual describe las políticas, normas, sanciones y reglas en cuanto a la gestión de la seguridad de la información como documento para consulta de todos los interesados (usuarios, funcionarios, contratistas, terceros, etc.) y está basado en la norma NTC-ISO-IEC 27001:2013.

Las políticas descritas en este manual se constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información del E.S.E. Ana Silvia Maldonado Jiménez de Colombia y se tomaran como base para la toma de decisiones en cuanto a controles, procedimientos y estándares definidos en el manejo de la información.

De esta manera, la Seguridad de la Información es una prioridad para el E.S.E. Ana Silvia Maldonado Jiménez de Colombia y por tanto es responsabilidad de todas las partes interesadas cumplir con el presente manual y velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de las políticas contenidas en dicho documento.

2. PRESENTACIÓN

2.1 Objetivos

2.1.1 Objetivo general

Presentar a todas las partes interesadas asociadas a la E.S.E. Ana Silvia Maldonado Jiménez las políticas y lineamentos de seguridad de la información definidos por la dirección del hospital, en beneficio de salvaguardar su información con respecto a su confidencialidad, integridad y disponibilidad. Lo anterior, cumpliendo con el deber constitucional de proteger y custodiar la información de la entidad y de los pacientes para la prestación de servicios de salud y garantizar la continuidad de la entidad.

2.1.2 Objetivos específicos

- Promover una cultura orientada a la seguridad de la información al interior de la E.S.E. Ana Silvia Maldonado Jiménez de Colombia.
- Mantener altos niveles de confidencialidad, integridad y disponibilidad de los activos de información críticos del E.S.E. Ana Silvia Maldonado Jiménez de Colombia.
- Concientizar y sensibilizar a todos los funcionarios, colaboradores, proveedores, contratistas y personas de interés general, acerca del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.
- Atender de manera eficiente y eficaz los incidentes de seguridad de la información que se presenten en el E.S.E. Ana Silvia Maldonado Jiménez de Colombia.
- Controlar, mitigar y/o prevenir impactos ocasionados por posibles materializaciones de riesgos de seguridad de la información, mediante la definición e implementación de medidas de control.
- Dar cumplimiento a la legislación vigente asociada a la seguridad de la información.
- Asegurar el proceso de respuesta a los hallazgos de revisiones y/o auditorias, a través de identificación y ejecución de planes de acción.

2.2 Alcance

Las políticas y lineamiento incluidas en el presente manual serán de aplicabilidad y cumplimiento por todos los funcionarios, contratistas, sindicalizados y en general a toda persona que tenga algún tipo de relación con el hospital y cuenten con acceso a los sistemas de información dentro o fuera de las instalaciones del E.S.E. Ana Silvia Maldonado Jiménez de Colombia, en cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información.

2.3 Definiciones

Acción correctiva: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva: Medida de tipo proactivo orientada a prevenir potencialmente no conformidades asociadas a la implementación y operación del SGSI - Sistema de Gestión de Seguridad de la Información

Aceptación del riesgo: Decisión de aceptar el riesgo

Activo de información: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para organización.

Datos: Todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen. Por ejemplo: Archivos de diferentes formatos.

Aplicaciones: Todo el software que se utiliza para la gestión de la información. Por ejemplo, SIIGHO.

Personal: Todo el personal del E.S.E. Ana Silvia Maldonado Jiménez de Colombia, subcontratado, los usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información.

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 informació

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. Ejemplo: Aire Acondicionado, destructora de papel, etc.

3. CONTENIDO

3.1 Capítulo I – Políticas de seguridad de la Información

3.1.1 Política de seguridad de la información

La E.S.E. Ana Silvia Maldonado Jiménez de Colombia, considera la información como un activo fundamental para la gestión administrativa y para la prestación de servicios de salud; por lo cual asigna un compromiso expreso de la protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad de la información.

Consciente de las necesidades actuales, la E.S.E. Ana Silvia Maldonado Jiménez de Colombia implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se exponen la información, ayudar a la reducción de costos operativos y financieros, establecer una cultura de seguridad y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información del E.S.E. Ana Silvia Maldonado Jiménez de Colombia, deberán adoptar los lineamientos contenidos en el presente documento y en los demás relacionados, con el fin de mantener la confidencialidad, la integridad y disponibilidad de la información.

La política global de seguridad de la información de la E.S.E. Ana Silvia Maldonado Jiménez de Colombia se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información del hospital. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013.

Esta política deberá ser revisada de manera periódica (por lo menos una vez al año, cuando se adicione un nuevo servicio TIC o se identifiquen cambios en el contexto interno o externo en la institución). Los responsables de realizar la revisión de la presente política será el comité de seguridad de la información o el responsable definido para tal labor.

3.1.2 Política de Clasificación de la Información

Objetivo

Gestionar las acciones necesarias para que la información reciba el nivel de protección apropiado de acuerdo con el tipo de clasificación establecido por el Hospital.

Directrices

- Se deberán definir cuáles son los niveles de clasificación de la información (Pública, uso interno, confidencial o restringida) para la información que se maneja en la institución.

- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales escritos en cualquier medio, ya sea magnético, papel u otro que genere el Hospital (Ej: historias clínicas, exámenes de laboratorio, patologías, imágenes diagnósticas, entre otras).

- El propietario de la información o a quien delegue, será el responsable de clasificar la información que tiene bajo su responsabilidad teniendo en cuenta los riesgos, amenazas e impactos en caso de materialización de éstos.

3.1.3 Política de Seguridad para los usuarios de activos de

información Objetivo

Verificar que los funcionarios, contratistas y demás colaboradores de la E.S.E. Ana Silvia Maldonado Jiménez de Colombia, entiendan sus responsabilidades y funciones, con el fin de reducir el riesgo de hurto, fraude o uso inadecuado de la información y de las instalaciones.

Directrices:

- Se debe asegurar que los funcionarios, contratistas y demás colaboradores del E.S.E. Ana Silvia Maldonado Jiménez de Colombia, entiendan sus responsabilidades en relación con las políticas de seguridad de la información y cumplan las mismas actuando de manera consistente frente a estas, con el fin de reducir el riesgo de hurto, fraude o uso inadecuado de la información o de los equipos empleados para el tratamiento de la información.

- Los recursos tecnológicos y de software asignados a los funcionarios del Hospital son responsabilidad de cada uno.

- Los usuarios son los responsables de la información que administren en sus equipos

personales; deberán abstenerse de almacenar en ellos información no institucional.

- Los usuarios solo tendrán acceso a los datos y recursos autorizados por el Hospital y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.

- Es responsabilidad de cada usuario proteger la información que esté contenida en documentos, formatos, listados, etc.; los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entradas de estos procesos.

- Los dispositivos electrónicos de propiedad del hospital (computadoras, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.

- Cualquier evento o posible incidente que afecte la seguridad de la información, deberá ser reportado inmediatamente al Área de Sistemas encargada de la Tecnologías de la Información y las Comunicaciones del Hospital.

- Los jefes de las diferentes áreas del Hospital en conjunto con el Comité de Seguridad de la información propiciarán actividades para concientizar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial.

3.1.4 Políticas específicas para funcionarios y contratistas del Área de TIC.

Objetivos

Garantizar que funcionarios y contratistas del área TIC aseguren una adecuada protección de la información de la cual son responsables de su administración.

Directrices

- El personal del Área de Sistemas encargada de la Tecnologías de la Información y las Comunicaciones no debe dar a conocer sus claves de usuario a personal ajeno a su área.

- Los usuarios y claves de los administradores de sistemas y del personal del área Área de Sistemas encargada de la Tecnologías de la Información y las Comunicaciones son de uso personal e intransferible.

- El personal del Área de Sistemas encargada de la Tecnologías de la Información y las Comunicaciones debe emplear obligatoriamente claves o contraseñas con un alto

nivel de complejidad.

- Los medios de instalación y seriales del software adquirido por la E.S.E. Ana Silvia Maldonado Jiménez de Colombia deben mantenerse custodiados para evitar el acceso a personal no autorizado.

- Para el cambio o retiro de equipos de cómputo por daño u obsolescencia, se deben seguir políticas de saneamiento; es decir, llevar a cabo mejores prácticas para la eliminación de la información de acuerdo con el software disponible en la entidad. (Ej. formateo o borrado seguro de información).

- Los funcionarios encargados de realizar la instalación o distribución de software sólo instalarán productos con licencia y software autorizado.

- El personal del Área de Sistemas encargada de la Tecnologías de la Información y las Comunicaciones está obligado a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.

- El personal del Área de Sistemas encargada de la Tecnologías de la Información y las Comunicaciones no utilizará la información del hospital para fines comerciales o diferentes al ejercicio de sus funciones.

- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar por quien designe el gerente en el área de Sistemas de Información Hospitalaria, de tal forma que asegure su protección y disposición en un futuro.

- El software licenciado y registrado como software adquirido, será únicamente instalado en equipos y servidores de propiedad del hospital, excepto aquellas empresas que mantengan un convenio contractual con la E.S.E. Ana Silvia Maldonado Jiménez de Colombia para la ejecución de las actividades requiera el acceso al software.

- La E.S.E. Ana Silvia Maldonado Jiménez de Colombia, instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados y en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización por parte del ingeniero de Sistemas de Información Hospitalaria puede implicar amenazas legales y de seguridad de la información para la entidad, por lo cual esta práctica no está autorizada. La persona o empresa encargada de redes e infraestructura, deberá llevará el control de las cantidades de licencias disponibles.

- El acceso al software y la documentación de éste solamente podrá ser consultada y usada en el ejercicio de las actividades contractuales.

- Cumplir siempre con el registro en la bitácora de acceso al Data Center de las personas que ingresen y que hayan sido autorizadas previamente por el Jefe Oficina Asesora Sistemas de Información Hospitalaria o por quien éste delegue.

- Por defecto deben ser bloqueados todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por el Comité de Seguridad de la Información o la gerencia.

- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.

- Todos los servidores deben ser configurados con el mínimo de servicios posibles y asociados para el desarrollo de las funciones designadas.

3.1.5 Políticas específicas para Webmaster

Proteger la integridad de la página Web institucional, el software y la información contenida en ellas.

Directrices

- Los responsables de áreas que requieran publicar información institucional en la página Web deben preparar y depurar la información de su área o dependencia y reportar al área de sistemas y comunicaciones para su revisión quien será responsable de verificar ortografía, redacción e imagen corporativa de la información a publicar.

- El responsable de redes e infraestructura realizará las copias de seguridad de la página web y mantendrá el histórico respectivo.

- Se deberá tener especial cuidado en la información que es publicada en la web y debe ser la autorizada por las áreas y con nivel de clasificación pública.

3.1.6 Política de Tercerización u Outsourcing

Objetivo

Mantener la seguridad de la información y los servicios de procesamiento de información

a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por esta.

Directrices

- Se deben establecer criterios de selección que contemplen la historia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

- Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas. El análisis de los riesgos será la base para el establecimiento de los controles y deben ser presentado al Comité de Seguridad de la Información y área TIC antes de firmar el contrato de Outsourcing.

- Con el fin de proteger la información por ambas partes, se debe formalizar un acuerdo de confidencialidad en donde se defina claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir. Si la información intercambiada lo amerita teniendo en cuenta la clasificación de la información de acuerdo con los niveles de seguridad, se debe preparar y legalizar un acuerdo de confidencialidad entre la entidad y el Outsourcing de acuerdo al objetivo y al alcance del contrato; el cual debe quedar firmado por ambas partes. En todos los casos deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información y con los objetivos de la entidad.

3.1.7 Política de disposición de información, medios y equipos

Objetivo

Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y propender por su recuperación oportuna.

Directrices

- Los medios y equipos 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.

3.1.8 Política de respaldo y restauración de información

Objetivo

Asegurar que la información crítica para la entidad se encuentre disponible en situaciones de contingencia y poder asegurar la continuidad del negocio.

Directrices

- La información de cada sistema debe ser respalda regularmente en medios de almacenamiento como discos externos, servidores de almacenamiento o el medio que disponga el hospital.
- Los administradores de los servidores son los responsables de la realización y custodia de las copias de seguridad según el procedimiento establecido.
- Todas las copias de información crítica deben ser almacenadas en un área adecuada con los controles ambientales aplicables y con control de acceso físico.
- Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal, entre otros.
- El plan de contingencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, actualizado y periódicamente probado y revisado.
- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; para lo cual la E.S.E. Ana Silvia Maldonado Jiménez de Colombia dispone de un espacio para el almacenamiento de la información en los servidores.
- Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera del edificio en donde se encuentre el Data Center del Hospital.
- Las restauraciones de copias de respaldo en ambientes de producción deben estar debidamente aprobada por el propietario de la información.
- Periódicamente desde el Área de Sistemas encargada de la Tecnologías de la Información y las Comunicaciones se verificará la correcta ejecución de los procesos de backup ejecutados.

- Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada. Este proceso deberá ser controlado y aprobado por las áreas de Revisoría Fiscal y/o Control Interno.

- Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización de los recursos de almacenamiento que entrega el Hospital a los usuarios.

3.1.9 Política de gestión de activos de información

Objetivo

Establecer la forma en que se logra mantener la protección adecuada de los activos de información.

Directrices

- La E.S.E. Ana Silvia Maldonado Jiménez de Colombia mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el Área de Sistemas encargada de la Tecnologías de la Información y las Comunicaciones - TIC.

- La E.S.E. Ana Silvia Maldonado Jiménez de Colombia, es el propietario (En cabeza de sus líderes de áreas) de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología de la información y comunicaciones (TIC).

3.1.10 Política de uso de los activos

Objetivo

Proteger de forma adecuada los activos de información mediante la asignación de estos a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.

Directrices

- Los activos de información pertenecen al Hospital y el uso de estos deben emplearse exclusivamente con propósitos laborales. Los activos de información de Hardware proveídos por el contratista o de terceras partes, serán administrados y estarán bajo

la supervisión del personal de tecnología de la información y comunicaciones TIC del Hospital y deberán cumplir con políticas de seguridad de la información, tal como control de acceso a redes y aplicativos, entre otros.

- Los usuarios deberán utilizar únicamente software, programas y equipos autorizados por el área de tecnología de la información y comunicaciones TIC del E.S.E. Ana Silvia Maldonado Jiménez de Colombia.

- El Hospital proporcionará al usuario los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad del Hospital, los funcionarios o usuarios solo podrán realizar backup de información pública. Para copiar cualquier tipo de información clasificada como confidencial o restringida debe pedir autorización a su jefe inmediato, de acuerdo con las normas sobre clasificación de la información.

- Periódicamente, el personal de redes e infraestructura efectuará una auditoria a los computadores para revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerado como violación a las Políticas de Seguridad de la Información del Hospital.

- El Hospital no se hará responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.

- Todos los requerimientos de aplicativos, sistemas y equipos informáticos que requieran un nivel de aprobación, deben ser solicitados, analizados y aprobados por el área de Sistemas de Información Hospitalaria.

- Estarán bajo custodia del Sistemas de Información Hospitalaria, los medios magnéticos/electrónicos (CD, DVD u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso; adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet.

- Los Password de administración de los equipos informáticos, sistemas de información o aplicativos estarán bajo la responsabilidad del funcionario que tenga la administración de los servicios del área de Sistemas de Información Hospitalaria TIC.

- En caso de ser necesario y previa autorización del Comité de Seguridad de la Información o del área de Sistemas de Información, los funcionarios del Hospital podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban a través de internet o de cualquier otra red o medio, en los equipos informáticos su cargo.

- Los recursos informáticos no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenidos personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos.

- Los usuarios no podrán efectuar ninguna de las siguientes actividades:

  - Instalar software en cualquier equipo instalado en áreas físicas del Hospital.
  - Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo del Hospital.
  - Modificar, revisar, transformar o adaptar cualquier software propiedad del Hospital.
  - Descompilar o realizar ingeniería inversa en cualquier software de propiedad del Hospital.
  - Copiar o distribuir cualquier software de propiedad del Hospital.

- El usuario deberá informar al jefe inmediato de cualquier violación de las políticas de seguridad o uso indebido del cual tenga conocimiento.

- El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.

- Ningún usuario deberá acceder a la red o a los servicios de TIC, utilizando una cuenta de usuario o clave de otro usuario.

- Cada usuario es responsable de asegurar que el uso de redes externas, tal como internet, no comprometa la seguridad de los recursos informáticos del Hospital. El área de redes e Infraestructura es responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad.

- Todos los archivos provenientes de equipos externos del Hospital deben ser revisados para detención de virus antes de ser utilizados en la red del Hospital.

- La información del Hospital debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se puede garantizar que la información sea segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

3.1.11 Política de uso de estaciones cliente

Objetivo

Asegurar que los usuarios usen correctamente las estaciones de trabajo como parte integral de los activos de información institucional.

Directrices

- La instalación de software en los computadores suministrados por el Hospitales una función exclusiva del área de Sistemas de Información TIC. Se mantendrá una lista actualizada del software autorizado para instalar en los computadores.

- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.

- Los programas instalados en los equipos son de propiedad del Hospital; la copia no autorizada de programas o de su documentación, implica una violación a la política general del Hospital. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las sanciones disciplinarias establecidas por el Hospital o las sanciones que especifique la ley. (Dichas copias no autorizadas deberán ser eliminadas).

- El Hospital se reserva el derecho de proteger su buen nombre y sus inversiones de hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad intelectual. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorias anunciadas y no anunciadas.

- En el disco o unidad C: de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a estos archivos.

- Los usuarios podrán trabajar sus documentos institucionales en borrador en las estaciones cliente asignado y deberá ubicar copias y documentos finales en las carpetas virtuales centralizadas que se establezca para cumplir con las tablas de retención documental del Hospital.

- Los usuarios que cuenten con Office 365 podrán utilizar los servicios de OneDrive para el almacenamiento de archivos institucionales solamente.

- Los equipos que ingresan temporalmente al hospital y que sean de propiedad de terceros, deben ser registrados en las porterías de la entidad para poder realizar su retiro sin autorización; el Hospital no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.

- El área de Sistemas de Información TIC no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo de información) a equipos que no sean del Hospital dentro de sus instalaciones y horario laboral.

3.1.12 Política de uso de Internet

Objetivo

Establecer lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando perdida, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones web.

Directrices

- La navegación en Internet debe realizarse de forma razonable y con propósitos laborares.

- No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas del Hospital o que representen peligro para la entidad como: pornografía, terrorismo, segregación racial, música, redes sociales u otras fuentes.

- El acceso a sitios WEB con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del Comité de Seguridad de la Información ó el área de Sistemas de Información Hospitalaria.

- La descarga de archivos de Internet debe ser con propósitos labores y de forma razonable para no afectar el servicio de Internet.

- Los documentos o software que se descarguen de Internet deben tener las debidas licencias o permisos de uso, respetando siempre la propiedad intelectual del mismo.

3.1.13 Política de uso de mensajería instantánea y redes sociales

3.1.14 Objetivos

Definir las pautas generales para asegurar una adecuada protección de la información en la E.S.E. Ana Silvia Maldonado Jiménez de Colombia, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios.

Directrices

- El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones con el fin de facilitar canales de comunicación con la ciudadanía.

- No se permite el envío de mensajes con contenido que atente la integridad de las personas o instituciones o cualquier contenido que presente riesgo de código malicioso.

- La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador del hospital, que sea creado a nombre personal en redes sociales (Twitter, Facebook, YouTube, blog, etc.) se considera fuera del alcance del SGSI y por lo tanto su confiablidad, integridad y disponibilidad, así como los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya publicado.

3.1.15 Política de uso de discos de red o carpetas virtuales

Objetivo

Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Directrices

- Para que los usuarios tengan acceso a la información en los discos de red, el jefe inmediato deberá enviar una solicitud al área de sistemas TIC del hospital, autorizando el acceso y permisos correspondientes al rol y funciones a desempeñar. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.

- El hospital suministrará una cuota de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información que crea importante y sobre ella se garantizará la disponibilidad en caso

de daños en el equipo asignado.

- La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.

- La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.

- Está prohibido almacenar en las estaciones de trabajo (computadores de escritorio o portátiles, tabletas, celulares inteligentes, etc.), o en los discos de red de propiedad de la entidad, archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso.

- Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización del jefe inmediato.

- Se prohíbe el uso de información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

3.1.16 Política de uso de impresoras y del servicio de Impresión

Objetivo

Asegurar la operación correcta y segura de las impresoras y del servicio de impresión en las diferentes áreas del hospital.

Directrices

- Los documentos que se impriman en las impresoras del Hospital deben ser de carácter institucional.

- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras (y/o cualquier equipo de cómputo). En caso de presentarse alguna falla, esta se debe reportar al área TIC por medio de su mesa de ayuda.

- Agregar o alinear la presente política con la de política de cero papel, si existe.

3.1.17 Política de uso de puntos de red de datos

Objetivo

Asegurar la operación correcta y segura de los puntos de red instalados en la entidad.

Directrices

- Los usuarios deberán emplear los puntos de red para la conexión de equipos informáticos estándar. Los equipos de uso personal, que no sean de propiedad del Hospital, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el área de redes e infraestructura. Se deberá identificar el equipo por medio de la MAC.

- La instalación, activación y gestión de los puntos de red es responsabilidad del área de infraestructura y redes.

3.1.18 Política de seguridad del centro de datos (DataCenter)

Objetivo

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Directrices

- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visite el centro de datos.
- El área de redes e infraestructura debe garantizar que el control de acceso al centro de datos del Hospital cuente con dispositivos de control necesarios (electrónicos de autenticación o sistemas de control biométrico) para asegurar accesos autorizados.

- El área de redes e infraestructura deberá garantizar que todos los equipos delos centros de datos cuenten con un sistema alterno de respaldo de energía.

- La limpieza y aseo del centro de datos estará a cargo del área de redes e infraestructura. En caso contrario, deberá ser supervisado por personal de esta área si el aseo lo llegase a realizar personal ajeno a ésta.

- En las instalaciones del centro de datos o centros de cableado, no se debe fumar,

comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

- El centro de datos debe estar provisto de:
  - Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación.
  - Pisos elaborados con materiales no combustibles.
  - Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración
  - Unidades de potencia ininterrumpida UPS, que proporcione respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
  - Alarma de detención de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán se probados de acuerdo con las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar prevista en los procedimientos de mantenimiento y control.
  - Extintores de incendios o un sistema contra incendios debidamente probado y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
- El cableado de la red debe ser protegido de interferencias a través del uso de canaletas.
- Los cables de potencia deben estar separados de los de comunicaciones (datos), siguiendo las normas técnicas.
- La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizadas por el comité de seguridad de la información o Área de Sistemas de Información Hospitalaria.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista de redes e infraestructura.
- Las puertas de acceso al centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario de la actividad se ubicará dentro del centro de datos.

- Cuando se requiera realizar actividad sobre algún armario (rack), este deberá siempre estar y/o quedar ordenado, cerrado y con llave cuando se finalice la actividad.

- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

- Los equipos del centro de datos que se requieran deben estar monitoreados para poder detectar las fallas que se puedan presentar.

3.1.19 Políticas de seguridad de los equipos de cómputo

Objetivo

Asegurar la protección de la información procesada en los equipos de cómputo.

Directrices

- Dar cumplimiento a las siguientes normas de seguridad:

  - Encender y apagar correctamente el equipo de cómputo.
  - No colocar encima de los equipos de cómputo ningún objeto que pueda caer y dañarlos.
  - Toda CPU que se encuentre en servicio no debe estar en el piso sin ningún tipo de soporte.
  - No consumir alimentos ni bebidas cerca al equipo de cómputo.
  - Limpiar regularmente el equipo de cómputo asignado.

- Conectar a la red de energía regulada únicamente equipos de cómputo y tecnológicos de propiedad del hospital. Equipos ajenos al hospital y autorizados para su uso dentro de la institución se deben conectar a la red no regulada.

- Seguridad del cableado: los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

  - Deben existir planos que describan las conexiones del cableado
  - El acceso a los centros de cableado, deben estar protegidos.

- Mantenimiento de los equipos de cómputo:

  - El Hospital debe mantener contratos de soporte y mantenimiento de los equipos de cómputo.

- Las actividades de mantenimiento tanto preventivo como correctivo debe registrarse para cada equipo de cómputo.
- Las actividades de mantenimiento de los servidores, comunicación, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.
- Los equipos que requieran salir de las instalaciones del Hospital para reparaciones o mantenimientos deben estar debidamente autorizados y se deben garantizar que en dichos elementos no se encuentre información confidencial.
- Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información confidencial contenida en ella. Realizar copia de información.

- El retiro e ingreso de todo activo de información de propiedad de los usuarios del Hospital utilizados para fines personales, se realizará mediante los procedimientos establecidos por la entidad. El Hospital no se hace responsable de los daños ocasionados a los bienes del usuario al haberse conectado a la red eléctrica del Hospital. El retiro e ingreso de todo activo de información de los visitantes (consultores, pasantes, visitantes, pacientes y sus familias), será registrado y controlado en las porterías. El personal de vigilancia registrará las características de la identificación del activo de información en el formato destinado para tal fin.

- El traslado entre dependencias del Hospital de todo activo de información (equipos de cómputo), está a cargo del área Administrativa (Activos Fijos) para el control de Inventarios.

3.1.20 Política de escritorio, pantalla limpia y de equipos desatendidos

Objetivo

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de información durante y fuera del horario de trabajo normal de los usuarios.

Directrices

- El personal del Hospital o contratistas debe conservar su escritorio libre de información confidencial, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- El personal del Hospital debe bloquear la pantalla de su computador con el protector de pantalla en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba ausentarse del puesto de trabajo.

- Al imprimir documentos de carácter confidencial, estos deben ser retirados dela impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

- Almacenar bajo llave y cuando corresponda, los documentos en físico y/o medios informáticos en gabinetes u otro tipo de mobiliario seguro, cuando no estén siendo utilizados, especialmente fuera del horario de trabajo.

- No se deben utilizar fotocopiadoras, escáners, equipos de fax, cámaras digitales y en general equipos tecnológicos que no se encuentren configuradosa la red del hospital.

3.1.21 Política de uso de correo electrónico

Objetivo
Establecer una serie de directrices para el uso responsable del correo electrónico institucional.

Directrices

- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de correo institucional; toda información o contenido que sea transmitido por las cuentas de correo de este sitio, son responsabilidad únicamente del dueño de la cuenta.

- La cuenta de correo es personal e intransferible, siendo su responsabilidad salvaguardar la clave de acceso, cambiándola en forma periódica, ni prestar la clave en ninguna circunstancia, pues su uso recae bajo su responsabilidad. Así mismo, el usuario se compromete a notificar personalmente al administrador de correo electrónico de manera inmediata la pérdida de su contraseña o acceso no autorizado por parte de terceros a su cuenta.

- Se requiere que la primera vez que el usuario ingrese a su cuenta de correo cambie su clave. Por motivos de seguridad, es recomendable cambiar la clave, como mínimo, cada tres meses. El correo electrónico es una herramienta de trabajo para uso exclusivamente de la Institución, no es una herramienta de difusión masiva e indiscriminada de información.

- Los miembros del Hospital deben ser cuidadosos cuando decidan abrir los archivos adjuntos en mensajes de remitentes desconocidos o sospechosos, para evitar descarga de algún virus informático o programa sospechoso.

- Será responsabilidad del administrador de las cuentas de office 365 tener copias de respaldo (Backups) de los mensajes de las carpetas de correo electrónico.

- Es responsabilidad del propietario de la cuenta mantener el buzón por debajo de su capacidad para evitar que se sature (eliminando regularmente mensajes antiguos, etc.). Si el buzón llega a saturarse no podrán recibirse mensajes nuevos mientras permanezca saturado. No se deben distribuir listas de direcciones de Correos de la Institución sin expresa autorización del Jefe Oficina Asesora Sistemas de Información Hospitalaria.

- El usuario es responsable de difundir su cuenta de correo, por lo tanto, la publicación de esta en sitios web, listas de correo, inscripciones a sitios de interés, provocara probablemente, el ataque continuo de correo basura (Spam) con publicidad en internet, por lo tanto, no se puede divulgar la cuenta de correo en estos medios.

Condiciones de uso

- Podrán tener correo electrónico Institucional todas aquellas personas de las diferentes áreas administrativas y asistenciales que se considere tenga necesidad de este servicio y tengan un vínculo laboral con la E.S.E. Ana Silvia Maldonado Jiménez de Colombia, las cuales serán asignadas con previa autorización del área de Sistemas de Información Hospitalaria.

- Los usuarios podrán tener correo institucional siempre y cuando cumplan con los términos de condiciones y las normas internas de la Institución; como también deberá tener claro que es para uso exclusivo del Hospital mas no para uso de tipo personal o comercial.

- Los usuarios serán completamente responsables del uso y manejo de las actividades realizadas con la cuenta de correo asociada a nuestra Institución, así como de la información enviada a través de este servicio.

- Se deberá usar lenguaje apropiado para los mensajes y manejar conductas de cortesía al momento del uso.

- Están completamente prohibidas las siguientes actividades:

  - Utilizar el correo electrónico para cualquier propósito personal de índole comercial o financiero.
  - No se debe participar en la propagación de “cartas en cadenas”, ni en esquemas piramidales de índole político, religioso o temas similares.

- Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados.
- Distribuir mensajes ofensivos, con palabras inapropiadas o que vulneren la integridad o buen nombre de la institución o de las personas.
- Leer correos ajenos, generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
- Violar los derechos de cualquier persona o Institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.
- Usar el correo con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil o maliciosa.
- Enviar por correo electrónico material que contenga virus de software, o cualquier otro código de computadora, archivos o programas diseñados para, destruir o limitar el funcionamiento de algún software o disco duro de computadora o equipo de telecomunicaciones.
- Usar el Servicio con fines fraudulentos o inapropiados.
- Causar daño a menores de edad.

- El usuario se responsabiliza de mantener la confidencialidad de su contraseña y cuenta y de todas las actividades que se efectúen bajo éstas, con el fin de que en toda información o contenido se mantenga su seguridad.

- Cada usuario se compromete a informar inmediatamente a la administración del correo institucional de cualquier acceso no autorizado de su contraseña o cuenta o de cualquier otro fallo de seguridad y se compromete asegurarse de que su cuenta sea cerrada al final de cada sesión.

- El usuario se obliga a cumplir las normas sobre protección de la información yde los datos que consagre la Constitución y la ley.

Caducidad de las cuentas de correo

El uso inapropiado, el abuso en el servicio de correo electrónico o no uso del mismo pueden ocasionar la desactivación temporal o permanente de las cuentas. La desactivación de una cuenta de correo electrónico supone la pérdida automática de la capacidad de enviar y recibir mensajes. Si existe evidencia de que el usuario está haciendo mal uso del servicio, no está respetando los lineamientos establecidos en esta política o está incurriendo en actividades ilícitas mediante el servicio de correo, el Hospital se reserva el derecho de tomar acciones disciplinarias, incluyendo las medidas pertinentes, de acuerdo con la normativa de la institución y a la legislación vigente. Como norma general, las cuentas de correo electrónico se mantendrán activas mientras la relación laboral de la persona con el Hospital esté vigente.

Buzón de correo

Todas las cuentas de correo tienen asignado un espacio de 50 Gb para almacenarlos mensajes recibidos (buzón). Si se sobrepasa la capacidad máxima el usuario no podrá recibir ni enviar correos.

El usuario deberá asegurarse de que su cuenta sea cerrada al final de cada sesión con el fin de evitar perdida de la información o suplantación.

3.1.22 Políticas de asignación de nombres de usuario para las cuentas de correo institucional

El nombre de usuario asignado será el primer nombre más un punto más el primer apellido. Por ejemplo, para Diana María Valencia Montoya sería diana.valencia@eseasmj.gov.co. En el caso de que el nombre de usuario ya estuviera asignado o resultara inapropiado, se irán agregando las iniciales del segundo nombre hasta cumplir con el criterio. Por ejemplo, para Carlos Darío Valencia Tangarife sería carlosd.valencia@eseasmj.gov.co . Si por algún motivo la persona no cuenta con segundo nombre, y el usuario ya se encontrará asignado, se irán agregando las iniciales del segundo apellido hasta cumplir con el criterio.

Por ejemplo, León Valencia Montoya sería leon.valenciam@eseasmj.gov.co. En cualquier otro caso el Hospital se reserva el derecho de asignarle otro lo más parecido posible a los criterios aquí expuestos.

Recomendaciones para la asignación de contraseña

- Para la asignación de la contraseña, los usuarios deben utilizar al menos 8 caracteres para crear la contraseña. Se recomienda o se exigirá utilizar en una misma contraseña dígitos, letras y caracteres especiales.
- Es recomendable que las letras se alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula.
- Elegir una contraseña que pueda recordarse fácilmente y que pueda escribirse rápidamente.

Acciones que deben evitarse en la gestión de contraseñas seguras

- Evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, si se utilizan varias cuentas de correo, se debe recurrir a contraseñas distintas para cada una de las cuentas.

- No utilizar información personal en la contraseña: nombre del usuario o de familiares, ni apellidos, ni fecha de nacimiento, y por supuesto, en ninguna ocasión utilizar datos como el número de cedula o número de teléfono.

- Evitar utilizar secuencias básicas de teclado (por ejemplo: “qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”), ni repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).

- Evitar utilizar solamente números, letras mayúsculas o minúsculas en lacontraseña.

- No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de esta. Tampoco se deben guardar en documentos de texto dentro del propio computador o dispositivos móviles.

- No enviar nunca la contraseña por correo electrónico o en mensajes de texto; tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.

- No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.

- Tener especial cuidado al ingresar las contraseñas en computadores que se desconozca su nivel de seguridad y puedan estar monitorizados, o en computadores de uso público (Ej.: bibliotecas, cibercafés, telecentros, etc.).

3.1.23 Política de control de acceso a sistemas y aplicativos

Objetivo

Definir las pautas generales para asegurar un acceso controlado lógico, a la información de la plataforma informática del Hospital, así como el uso de medios de computación móvil.

Directrices:

- El Hospital proporcionará a los funcionarios y contratistas todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados; por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tablets, agendas electrónicas, celulares inteligentes, access point, entre otros que no estén

autorizados por la Oficina Asesora Sistemas de Información Hospitalaria.

- Todo equipo de cómputo ajeno al hospital debe cumplir con los siguientes criterios para la conexión a la red interna de la institución:

  - Sistema operativo licenciado que permita unirse al dominio del hospital.
  - Sistema operativo en su versión Windows 10 Professional.
  - Sistema operativo actualizado, con todos los parches de seguridad.
  - Antivirus actualizado.
  - Escaneo total con el antivirus con un día de anticipación al ingreso de dominio del hospital.
  - Licencias de todo el software que este instalado en el equipo.
  - Todo equipo que no cumpla con alguno de estos criterios, por seguridad de la información no podrá ser instalado a la red, recursos y sistemas internos del hospital.

- El hospital suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados; las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se le dé a las claves asignadas.

- El área de TIC será el responsable de generar el usuario y la contraseña de primer acceso para el ingreso a los aplicativos institucionales del personal autorizado por el área de talento humano.

- El área TIC será el responsable de mantener los registros de cada uno de los usuarios a los cuales se les han concedido permisos de acceso o eliminación de estos.

- El propietario de los activos de información o a quien delegue debe autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

- El propietario de los activos de información o a quien delegue debe monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

- Cada usuario es responsable de los mecanismos de control de acceso que le han sido proporcionados; esto es usuario y contraseña de primer acceso, porl o que se deberá mantener de forma confidencial.

- Cada usuario que tenga acceso a sistemas y aplicativos debe contar con un único usuario para el aplicativo asignado.

- Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

- No se podrá realizar ninguna actividad de tipo remoto sobre los equipos, servidores principales sin la debida aprobación del Jefe Oficina Asesora Sistemas de Información Hospitalaria.

- La conexión remota a la red área local del Hospital debe ser hecha a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada.

- Solo usuarios del área TIC, están autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones.

- Las contraseñas de acceso deberán cumplir con un mínimo de 8 caracteres y la combinación se hará con números, letras mayúsculas y minúsculas, y caracteres especiales.

- Los usuarios con acceso a los diferentes sistemas de información deberán cambiar su contraseña de acceso con una frecuencia mínima de 3 meses.

- Los usuarios deben cumplir las siguientes normas para la creación de contraseñas:

  - Mantener los datos de acceso en secreto.
  - Contraseñas fáciles de recordar y difíciles de adivinar.
  - Que las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente.
  - Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

3.1.24 Política para dispositivos móviles

Objetivo

Proveer las condiciones de seguridad para el manejo de los dispositivos móviles (memorias USB, Discos duros externos, teléfonos inteligentes y tabletas, entre otros) institucionales y personales autorizados que hagan uso de activos de información en los servicios del hospital.

Directrices:

- El área TIC debe implementar las medidas de protección física y lógica sobre los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por el hospital.
- El uso de dispositivos de almacenamiento externo (D.D externos, DVD, CD, memorias USB, agendas electrónicas, celulares, entre otros) pueden generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar algunos de los dispositivos de almacenamiento externo enunciados anteriormente, se debe obtener aprobación formal e individual del Jefe Oficina Asesora Sistemas de Información Hospitalaria.
- El área de Sistemas de Información TIC debe establecer las configuraciones de seguridad de acceso para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por el hospital, previamente autorizados.
- El área de Sistemas de Información TIC deberá configurar el control de bloqueo automático de sesión de usuarios por inactividad.
- El área de Sistemas de Información TIC debe activar la opción de cifrado de discos en aquellos dispositivos móviles institucionales que almacenan información sensible y/o crítica.
- El área de Sistemas de Información TIC debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- El área de Sistemas de Información TIC debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales del hospital; dichas copias deben acogerse a la política de respaldo y restauración de la Información.
- El área de Sistemas de Información TIC debe instalar un software de antivirus tanto en los dispositivos móviles institucionales como en los personales que hagan uso de los servicios provistos por el hospital.
- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias paraevitar pérdida o robo de estos.

- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

- Los usuarios deben evitar la instalación de software no autorizado y/o desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados mientras se encuentren en lugares diferentes al hospital.

- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de bibliotecas o cafés internet, entre otros.

- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

3.1.25 Política de transferencia de información

Objetivo

Presentar los lineamientos orientados para la protección de la información tanto del Hospital como de los pacientes en aquellas situaciones en las cuales sea necesario o se requiera realizar su transferencia a terceros, asegurando que la información sensible y crítica del Hospital y de los pacientes sea transferida a su destino a través de los medios disponibles y autorizados, de manera adecuada para prevenir su posible interceptación, acceso y/o uso no autorizado.

Directrices generales:

- El propietario de los activos de información o a quien él delegue debe velar porque la información del hospital o de sus usuarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información.

- El propietario de los activos de información o a quien él delegue debe asegurar que los datos requeridos de los usuarios sólo puedan ser entregados a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.

- El propietario de los activos de información o a quien él delegue, debe verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

- El propietario de los activos de información o a quien él delegue debe autorizar los requerimientos de solicitud/envío de información del hospital por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

- El propietario de los activos de información o a quien él delegue debe asegurar que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a la presente política.

- Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando carpetas, archivos compartidos, discos virtuales, medios removibles, entre otros que no estén controlados ni auditados por el área de Sistemas de Información TIC.

- El área de correspondencia debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por el hospital y que estos permitan ejecutar rastreo de las entregas.
- El área de Sistemas de Información TIC debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

- No está permitido el intercambio de información sensible del hospital ni de sus usuarios o pacientes por vía telefónica o fax.

<u>Contacto vía telefónica</u>

- Realizar la transferencia de información únicamente a través de líneas telefónicas internas.
- Al realizar contacto telefónico, marcar el número registrado en la base de dato por parte del paciente o familiar.
- Siempre se deberá preguntar por el nombre completo del paciente para asegurar que se está comunicado con la persona indicada y a través del uso de validación de información.
- No se deberán dejar mensajes con información sensible con personas diferentes al paciente, en equipos de respuesta automática o mensajes de voz, siempre y

cuando el mensaje sea demasiado urgente y sin datos sensibles.

- Asegúrese de dejar el mensaje en la máquina de respuesta correcta y de uso permanente por el paciente.

Contacto vía correo electrónico

- Únicamente información NO sensible podrá ser enviada a cuentas de correo electrónico de pacientes.
- Los usuarios (asistenciales – administrativos) bajo ninguna circunstancia deben utilizar el correo electrónico personal como medio para enviar o recibir información propia del hospital, de sus usuarios o pacientes (salvo aquellos autorizados).
- Información sensible solamente podrá ser entregada o compartida a los pacientes a través de medio conversación telefónica o de manera personal y no a través de correo electrónico.

Comunicación electrónica de información a terceros

- Bajo ninguna circunstancia información o datos personales de usuarios o pacientes podrán ser enviados sin los controles de encriptación necesarios.
- El intercambio de información sensible a través de redes públicas o links con entidades del sector o terceros autorizados, deberá ser protegida mediante el uso de mecanismos criptográficos que garanticen su confidencialidad y autenticidad.

Transporte de información digital en medio físico

- La información sensible de pacientes o del Hospital que requiera ser entregada físicamente, deberá ser protegida mediante el uso de mecanismos criptográficos que garanticen su confidencialidad y autenticidad en cualquier dispositivo de almacenamiento que se establezca para su transporte (discos duros, USB, entre otros, que estén autorizados por la Oficina Asesora Sistemas de Información Hospitalaria).

3.1.26 Política para revisión de los derechos de acceso a usuarios

Objetivo:

Verificar y validar que el acceso lógico asignado a los sistemas de información y aplicaciones, se encuentran debidamente aprobados y acceden a la información y/o recursos apropiados de acuerdo con sus roles y responsabilidades del funcionario dentro de la institución.

Directrices:

- Para administrar los accesos a los Sistemas de información se definirán perfiles de acceso asignables a grupos de usuarios que, por su responsabilidad en la organización presenten necesidades de acceso.

- Los líderes de procesos o área deben revisar en forma periódica los perfiles de usuarios del personal a su cargo y solicitar al área TIC la actualización de éstos cada vez que ocurra un cambio en la definición de funciones.

- Se mantendrá registro de los intentos de acceso fallidos a sistemas considerados críticos, el cual será revisado periódicamente por el responsable de los sistemas de información.

- Constituirá falta grave el intento de obtener accesos no autorizados a los aplicativos institucionales.

- De forma periódica se suspenderán las cuentas de usuarios que no fueron accedidas durante un lapso determinado de tiempo; para ello, se deberá asegurar la copia de respaldo con información de registro de actividades de usuarios en los diferentes sistemas de información o aplicaciones.

3.1.27 Política para disposición final de medios cuando no se requieran

Objetivo:

Establecer las directrices y actividades necesarias para el manejo, almacenamiento y disposición final de los medios de almacenamiento de información usados por la institución.

Directrices:

- La disposición final de documentos se hará de acuerdo con el programa de gestión documental, procesos y procedimientos internos para el archivo, conservación y disposición final de documentos.
- La disposición final de los documentos se realizará en las mejores condiciones, procurando siempre fomentar la transparencia, el acceso y el cumplimiento de los lineamientos que al respecto puedan ser aplicados.
- Todo documento en físico que se requieran dar de baja se debe coordinar con la Oficina de Seguridad y Salud en el Trabajo para la destrucción y disposición final de los mismos, dando cumplimiento a las siguientes actividades:

    - Separar el papel que se encuentre en buen estado para disponer de forma final.
    - Realizar destrucción manual del papel que va a ser dispuesto de forma final.
    - Comercializar (venta de material reciclable) con empresas que tengan licencia ambiental para disposición y tratamiento de residuos sólidos.

- El hospital garantizará la consulta, utilización y conservación de la documentación de la entidad para satisfacer necesidades de información de los usuarios.
- Los equipos de cómputo que ya no se requieran por su obsolescencia o daño, serán revisados por personal del área de sistemas de información TIC, quienes emitirán el reporte técnico respectivo para la disposición final por parte del hospital.
- Toda disposición final de medios electrónicos que ya no se usen (equipos de cómputo y/o periféricos) se debe ejecutar de acuerdo con lo establecido en el procedimiento interno del hospital para baja de equipos y a la normatividad vigente emitida por el gobierno colombiano para la disposición de aparatos electrónicos.

Algunas de las estrategias para disposición final son las siguientes:

- Subastar mediante un intermediario, aquellos equipos en funcionamiento y que para el hospital sean considerados obsoletos.
- Comercializar todo equipo dañado con empresas que tengan licencia ambiental para disposición y tratamiento de equipos electrónicos.

- Aquellos medios de información que ya no se requieran por obsolescencia (PC portátil y de escritorio), deben cumplir con las condiciones de borrado y/o formateo seguro antes de su disposición final (instructivo para borrado y/o formateo seguro).

3.1.28 Política de devolución de activos

Objetivo

Asegurar que los activos de información de propiedad del hospital sean devueltos de forma íntegra por funcionarios, contratistas y demás personas quienes hayan tenido responsabilidad de propiedad sobre los mismos.

Directrices

- Los funcionarios, contratistas y todos aquellos que se vinculen directa o indirectamente con el hospital, tienen como responsabilidad final realizar la devolución de los activos de información de la institución a su cargo y responsabilidad (software, documentos corporativos, equipamiento, dispositivos de computación móvil, entre otros) al jefe de área respectiva; que a lo largo de su vida laboral se le asignó una vez que se dé por concluida toda relación o vínculo laboral.

- En los casos donde el funcionario, contratista y demás tengan bajo su administración información importante generada o accedida durante su desempeño en las funciones del cargo; dicha información deberá ser entregada al hospital a través de cada jefe de área para su almacenamiento y/o respaldo; la devolución de la información y demás activos será tenida en cuenta para el concepto de paz y salvo para con el hospital.

- Si un funcionario, contratista y demás con autorización de la Área de Sistemas de Información Hospitalaria utiliza su equipo de cómputo personal, éste es responsable de transferir toda la información de propiedad del hospital al área de interés; dicha información deberá ser eliminada de manera confiable de su equipo como resultado de la finalización de su relación laboral.

- Al momento que un funcionario termine su vínculo laboral con el hospital o sea reasignado de área, éste debe hacer entrega formal de los activos de información que estaban a su cargo al jefe inmediato.

- Al momento que un funcionario termine su vínculo o relación laboral, las áreas responsables de gestionar los permisos de acceso físico y/o lógico a través de medios electrónicos o similares, deberán inactivar de manera oportuna dichos permisos.

- Toda devolución de activos tangibles de información se debe realizar mediante el área de activos fijos a través del formato de traslado generado por esta área.

- El área de recursos humanos y aquellas que gestionen contratistas o similares, deben ser las fuentes de información de los retiros de funcionarios, contratistas y demás externos.

3.1.28. Política de seguridad para relación con proveedores

Objetivo

Establecer pautas para identificar y mantener relaciones claras y fortalecidas con los proveedores de la E.S.E. Ana Silvia Maldonado Jiménez, orientadas a recibir servicios y/o productos con calidad, oportunos y/o continuos teniendo en cuenta los acuerdos establecidos con ellos, garantizando de esta forma la aplicación de medidas de seguridad adecuadas que aseguren el cumplimiento de los objetivos institucionales.

Directrices

La política de relación con proveedores, indica aquellas buenas prácticas que la E.S.E. Ana Silvia Maldonado Jiménez deberá tener en cuenta para establecer una relación clara y bien establecida con respecto al apoyo y soporte que debe tener en cuanto a la protección de seguridad de la información.

Por esta razón y para la protección de seguridad de la información, la relación con proveedores se define teniendo en cuenta las siguientes directrices:

- Calidad; seleccionar proveedores que ofrezcan productos y/o servicios que cumplan con estándares de calidad determinados por las mejores prácticas del sector y en lo posible que demuestre buenas prácticas de gestión mediante la presentación de certificaciones que evidencien su gestión de calidad, seguridad de la información u otro afín.
- Proveedor competente; determinar que el personal contratista sea calificado y competente para brindar los servicios que ofrecen dentro de sus propuestas.
- Idoneidad del proveedor; instaurar relaciones con proveedores legalmente constituidos, íntegros, formales y éticos en su accionar, sin ningún tipo de inhabilidad.
- Competitividad**;** que ofrezcan productos y/o servicios en las condiciones más competitivas del mercado a los intereses de la E.S.E. Ana Silvia Maldonado Jiménez.
- Capacidad técnica y logística**;** que el proveedor cuente con la capacidad técnica, administrativa, logística y financiera para entregar los bienes y servicios en las condiciones negociadas.
- Respaldo; que la atención del proveedor sea directa y con mayor flexibilidad para adaptarse a las necesidades de la E.S.E. Ana Silvia Maldonado Jiménez.
- Referencias; calificación en el sector o mercado como organización prestadora de servicios o proveedora de bienes o productos.
- Validación; todo acuerdo establecido formalmente entre el E.S.E. Ana Silvia Maldonado Jiménez y el proveedor, deberá estar soportado por medio de un contrato y/u orden de compra donde se valide el objeto del contrato
- Seguimiento; todo servicio contratado por parte de la E.S.E. Ana Silvia Maldonado Jiménez deberá estar bajo permanente monitoreo de su desempeño, calidad y oportunidad.
- Acceso a información; todo acceso a información a ser asignado a un tercero deberá estar previamente autorizado por el propietario del activo de información del área respectiva.

3.1.29. Política para la gestión de proyectos

Objetivo:
Definir las reglas de seguridad para el resguardo de los activos de información sensibles para la gestión de los proyectos que se lleven a cabo dentro de la institución.

Directrices:

- Dentro de los objetivos del proyecto se deben incluir objetivos de seguridad de la información en concordancia con los activos de información a tratar.

- Identificar los activos de información sensibles que estarán involucrados en el diseño y desarrollo del proyecto.

- Incluir en la gestión del proyecto una evaluación de los riesgos para la protección de los activos de información y de esta forma identificar los controles necesarios.

- Definir los responsables en cada una de las etapas del proyecto a fin de que bajo su responsabilidad se implementen los controles relacionados al uso y/o tratamiento de los activos de información.

- La seguridad de la información debe ser parte de todas las etapas del proyecto, independiente de la metodología utilizada.

3.1.30. Política para desarrollo externo de software

Objetivo:

Velar porque el desarrollo externo de software cumpla con los requerimientos de seguridad esperados, con buenas prácticas para desarrollo seguro, así como con metodologías para la realización de pruebas de aceptación y seguridad. Además, asegurar que todo software desarrollado externamente cuente con el nivel de soporte requerido por el hospital.

Directrices:

- El propietario de los sistemas de información o a quien delegue es responsable de realizar las pruebas para asegurar que los sistemas de información cumplan con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- El área de sistemas de información TIC debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del hospital.

- El área de sistemas de información TIC debe asegurar que los sistemas de información desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificarlas condiciones de uso del software y los derechos de propiedad intelectual.

- El área de sistemas de información TIC, a través de sus funcionarios, debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los

parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

- Validar que los desarrolladores de los sistemas de información empleen buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

- El área de sistemas de información TIC debe contar con un contrato de soporte vigente o asegurar la prestación de soporte por parte del proveedor de software (SLA). Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo del hospital; dicho soporte debe contemplar tiempos de respuesta aceptables.

- Validar que los desarrolladores construyan los aplicativos de tal manera que se efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable.

- Verificar que en los desarrollos efectuados se asegure la validación de la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

- Validar que en los desarrollos ejecutados existan los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

- Validar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

3.1.31. Política para seguridad de equipos y activos fuera de las instalaciones

Objetivo:
Proteger los activos y equipos de la organización que se encuentren fuera de las instalaciones.

Directrices:

- La asignación de equipos de cómputo debe ser realizada por el jefe de área y esta

debe quedar documentada detallando el equipo asignado y usuario a quien se responsabiliza.

- El uso de equipos de cómputo y activos de información fuera de las instalaciones del hospital, debe ser autorizado por el jefe del área respectiva.

- Todo equipo de cómputo que sea retirado del hospital por aprobación del jefe de área para funciones del cargo, debe ser registrado en las bitácoras llevadas por la empresa de vigilancia al momento de ser retirado e ingresado de las instalaciones.

- Todo equipo que sea retirado del hospital no debe ser desatendido en áreas de acceso público y deben seguirse las directrices de la política de escritorio, pantalla limpia y equipos desatendidos.

- Cuando el usuario viaje con un equipo de cómputo portátil de propiedad del hospital, éste debe ser transportado como equipaje de mano y de forma disimulada.

- Se deben observar siempre las instrucciones del fabricante para proteger los equipos contra exposiciones a campos electromagnéticos, fuertes entradas de polvo, humedad, entre otros.

3.1.32. Política para seguridad de oficinas, recintos e instalaciones

Objetivo:
Proveer mecanismos de control y seguridad física en aquellas áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren equipos y demás infraestructura de soporte a los sistemas de información que se consideren áreas seguras y de acceso restringido.

Directrices:

- Mantener de manera discreta el centro de datos, las oficinas TIC y demás áreas donde se almacene información sensible, sin señales externas o internas de tal manera que las actividades de procesamiento de información se mantengan reservadas.

- No dejar solos en las oficinas o áreas seguras a personal ajeno al área (visitantes, proveedores, entre otros).

- Las puertas y ventanas de oficinas y recintos se deben mantener cerradas cuando se termine la jornada laboral (en áreas que aplique) o cuando no haya vigilancia y se debe contar con protección externa para las ventanas ubicadas en niveles bajos.

- Restringir el acceso público a las guías telefónicas y listados de teléfonos internos.

- Almacenar los equipos redundantes y la información de resguardo (Backup)en un sitio seguro y distante del lugar de procesamiento de información.

- Las visitas autorizadas para ingresar a áreas seguras donde se maneja información sensible, debe quedar registrado en bitácoras de control y durante la permanencia en éstas debe haber acompañamiento siempre por personal debidamente autorizado y que haga parte del área.

- El acceso a áreas seguras donde se procesa o almacena información sensible debe ser controlado y restringido solo a personas autorizadas.

- Todo lugar de trabajo en que exista algún riesgo de incendio, ya sea por la estructura del edificio o por la naturaleza del trabajo que se realiza, debe contar con extintores de incendio, de acuerdo al tipo de material combustible o inflamable.

- En áreas donde existan, se almacenen, trasvasijen o procesen sustancias inflamables o de fácil combustión, deberá establecerse una estricta prohibición de fumar.

- Almacenar los materiales peligrosos o combustibles en lugares seguros y bajo condiciones de seguridad.
- No se deben ingerir alimentos y/o bebidas en cercanías a los equipos y/o dispositivos de cómputo.

- Los funcionarios y terceros deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren dentro de las instalaciones.

- Mantener vigilancia continua dentro de las instalaciones del hospital.

3.1.33. Política de tratamiento y protección de datos personales

Introducción

En virtud de la Ley 1581 de 2012 (Art. 17 Lt. k y Art. 18 Lt. f) y del Decreto 1377 de2013 (Art. 13.) mediante los cuales se dictan disposiciones para la protección de datos personales y en el desarrollo del derecho constitucional que tienen todas las personas a

conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos, la E.S.E. Ana Silvia Maldonado Jiménez en calidad de responsable del tratamiento de los datos personales de sus grupos de interés conformado por los usuarios y sus familias, colaboradores, contratistas, estudiantes, entidades responsables de pago y las entidades de inspección, vigilancia y control, información que se ha obtenido en el desarrollo de su actividad misional de prestar servicios de salud, por lo cual se compromete con el cumplimiento de la normativa mencionada y la protección de los derechos de las personas e informa a su grupo de interés que adopta las siguientes políticas sobre recolección, tratamiento y uso de datos personales.

Responsable del tratamiento de datos

La E.S.E. Ana Silvia Maldonado Jiménez, identificada con NIT. 813011706-8, con domicilio en la ciudad de Colombia, Carrera 3 NO 7 - 12, Correo Electrónico: gerencia@esecolombia.gov.co teléfono 8319547- 8319710, es la responsable del tratamiento de los datos obtenidos de sus diferentes grupos de interés.

Directrices

La E.S.E. Ana Silvia Maldonado Jiménez, en virtud de su objeto social, ha obtenido y conservado desde su creación, datos personales de sus grupos de interés, los cuales en adelante llamáremos titulares, los cuales son recolectados, almacenados, organizados, usados, transmitidos, actualizados, rectificados y en general administrados, de acuerdo con la respectiva relación y/o vinculación (civil, laboral, comercial o educativa) aplicando las siguientes directrices:

- La E.S.E. Ana Silvia Maldonado Jiménez, está comprometida en dar un correcto uso y tratamiento de los datos personales y datos personales sensibles de sus titulares, evitando el acceso no autorizado a terceros que permita conocer, vulnerar, modificar, divulgar y/o destruir la información, para lo cual cuenta con políticas de seguridad de la información que incluyen medidas de control de obligatorio cumplimiento.
- La E.S.E. Ana Silvia Maldonado Jiménez, solicita a los titulares de la información los datos necesarios para administrar el riesgo en salud y dar cumplimiento a las funciones asignadas por la normativa vigente que regula el Sistema General de Seguridad Social en Salud. La información sensible requerida será de libre y voluntaria entrega por parte del respectivo Titular.
- Salvo las excepciones previstas en la ley, el tratamiento de los datos personales sólo podrá realizarse con el consentimiento previo, expreso e informado de sus titulares, manifestado por escrito, de forma oral o mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización.

- La E.S.E. Ana Silvia Maldonado Jiménez, solicitará a las entidades responsables de pago, colaboradores, estudiantes y contratistas, los datos personales necesarios para establecer la respectiva relación y/o vinculación (civil, laboral, comercial o educativa). La información sensible requerida será de libre y voluntaria entrega por parte del respectivo Titular, quien deberá otorgar su consentimiento y

autorización para su respectivo tratamiento.

- La E.S.E. Ana Silvia Maldonado Jiménez, velará por el respeto y cumplimiento de los derechos fundamentales de los niños, niñas y adolescentes, observando los requisitos especiales establecidos para el tratamiento de sus datos personales y datos personales sensibles.
- El tratamiento de los datos personales proporcionados por los usuarios y sus familias de la E.S.E. Ana Silvia Maldonado Jiménez, tendrá la siguiente finalidad:

  - Para la prestación de los servicios asistenciales de sus usuarios y familias.
  - Actualización de datos entregados por el Titular.
  - Caracterización y seguimiento a la población, para la gestión del riesgo en salud, utilizando la información derivada de los servicios asistenciales.
  - Entrega de reportes de Salud Pública de obligatorio cumplimiento.
  - Dar respuesta a requerimientos a entidades de control.
  - Evaluación de indicadores de oportunidad y calidad de los servicios.
  - Evaluación de la calidad de los productos y servicios de salud ofrecidos por la institución.
  - Ejercer acciones legales y en la defensa de las mismas.
  - Suministro de información a las autoridades competentes en caso de ser requerida.
  - En general para cualquier otra finalidad que se derive de la naturaleza jurídica de la E.S.E. Ana Silvia Maldonado Jiménez.

- El tratamiento de los datos personales proporcionados por los colaboradores de la E.S.E. Ana Silvia Maldonado Jiménez, tendrá la siguiente finalidad:

  - Realización del proceso de selección de personal de acuerdo con su aptitud para un cargo o tarea.
  - Establecer una relación contractual.
  - Ofrecerle oportunidades de capacitación.
  - Evaluaciones de desempeño, satisfacción laboral, crecimiento personal, bienestar, seguridad y salud en el trabajo.
  - Cumplir el proceso de afiliación al Sistema General de Seguridad Social Integral (Entidades Promotoras de Salud, Administradoras de riesgos laborales, Fondos de pensiones y cesantías, Caja de Compensación)
  - Efectuar el proceso de Remuneración.
  - Ejercer acciones legales y en la defensa de las mismas.
  - Cumplir con exigencias judiciales.
  - Dar a conocer avances de la institución en aspectos investigativos, académicos y clínicos
  - Suministro de información a las autoridades competentes en caso de ser requerida.
  - En general para cualquier otra finalidad que se derive de la vinculación contractual.

- El tratamiento de los datos personales proporcionados por las entidades responsables de pago y contratistas de la E.S.E. Ana Silvia Maldonado Jiménez, sean personas naturales o jurídicas, tendrá la siguiente finalidad:

  - Realizar la vinculación contractual.
  - Efectuar el reconocimiento económico por la prestación del servicio.
  - Suministro de información a las autoridades competentes en caso deser requerida.
  - Ejercer acciones legales y en la defensa de las mismas.
  - Cumplir con exigencias judiciales.

- El tratamiento de los datos personales de estudiantes que realizan prácticas en la E.S.E. Ana Silvia Maldonado Jiménez, tendrá la siguiente finalidad:

  - Presentar informes a las instituciones educativas
  - Hacer invitación a eventos clínicos y académicos.
  - Evaluar los conocimientos adquiridos durante su formación.
  - Dar a conocer avances de la institución en aspectos investigativos, académicos y clínicos.
  - Ejercer acciones legales y en la defensa de las mismas.
  - Suministro de información a las autoridades competentes en caso de ser requerida.
  - En general para cualquier otra finalidad que se derive de la vinculación contractual.

Deberes de la E.S.E. Ana Silvia Maldonado Jiménez

- Garantizar al usuario el pleno y efectivo derecho constitucional de habeas data.
- Mantener la información en condiciones de seguridad y privacidad.
- Hacer uso de la información para los fines misionales y previstos en la ley.
- Tramitar de manera oportuna los reclamos que tengan los usuarios frente a la información consignada en la base de datos.
- No vender, circular o intercambiar la base de datos de sus usuarios, sin causa legal o contractual que lo justifique.
- Se debe conservar prueba del cumplimiento de la información suministrada al Titular, y cuando éste lo solicite, entregarle copia de esta.
- Al momento de solicitar al Titular la autorización la E.S.E. Ana Silvia Maldonado Jiménez deberá informar de manera clara y expresa lo siguiente:

  - El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
  - El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas se realicen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

- Los derechos que le asisten como Titular.
- La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

- El uso de los datos personales de los niños, niñas y adolescentes deberá cumplir con el requisito de responder y respetar los derechos prevalentes de este grupo poblacional, y sus derechos fundamentales.
- El representante legal del niño, niña o adolescente otorgará la autorización para el tratamiento de los datos personales del menor.

Derechos de los Titulares

El Titular de los datos personales y datos personales sensibles tendrá los siguientes derechos:

- Conocer, actualizar y rectificar los datos que aparezcan en la misma. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Conocer por qué y para qué la E.S.E. Ana Silvia Maldonado Jiménez, recolecta información en base de datos.
- Revocar en cualquier momento la autorización dada para contener información personal en las bases de datos de la E.S.E. Ana Silvia Maldonado Jiménez.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento considere que no se respetan los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a esta ley y a la constitución.
- Poner queja ante la Superintendencia de Industria y Comercio, cuando considere que le ha sido violado por parte de la E.S.E. Ana Silvia Maldonado Jiménez, su derecho al Habeas Data.
- Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento

Casos que no requieren autorización para el tratamiento de datos

La autorización del Titular no será necesaria cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos,

estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

Entrega de información

La información que reúna las condiciones establecidas en el Art. 13 de la Ley 1581de 2012, podrá suministrarse a las siguientes personas:

- A los Titulares, sus causahabientes o sus representantes legales.
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- A los terceros autorizados por el Titular o por la ley.

Área responsable de la atención de peticiones, consultas y reclamos.

El área responsable de la atención de peticiones, quejas, reclamos, sugerencias y felicitaciones será la oficina de Atención al Usuario (SIAU) de la E.S.E. Ana Silvia Maldonado Jiménez, mediante la aplicación de su proceso: Gestión y tratamiento de PQRSF.

3.2 Capítulo II – Organización de la Seguridad de la Información

3.2.1 Compromiso de la dirección

La Junta Directiva de la E.S.E. Ana Silvia Maldonado Jiménez de Colombia aprueba el presente Manual de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información del hospital.

La Junta Directiva y la Gerencia del E.S.E. Ana Silvia Maldonado Jiménez demuestran su compromiso a través de la:

- Revisión y aprobación de las políticas de seguridad de la información contenidas en este documento.
- Promoción de una cultura de seguridad de la información.
- Divulgación del presente manual a todas las partes interesadas.
- Disposición de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- Verificación del cumplimiento de las políticas aquí mencionadas.
- Creación y seguimiento al Comité de Seguridad de la Información, con la participación de un representante de la alta gerencia.

3.2.2 Coordinación de la seguridad de la información

En la E.S.E. Ana Silvia Maldonado Jiménez de Colombia ha designado como representante de la alta dirección al Líder de Sistemas de Información Hospitalaria y responsable del

Comité de Seguridad de la Información.

Dentro del Comité de Seguridad de la Información se definirán los responsables, roles y las funciones de los representantes de las otras áreas de la organización y quienes harán parte de dicho comité. Estas responsabilidades deben quedar inmersas en los contratos de trabajo, manual de funciones o el documento pertinente (para terceras partes).

3.2.3 Proceso de autorización para servicios de procesamiento de información

Al ingresar nuevos servicios, estos deben ser aprobados por la Oficina Asesora Sistemas de Información Hospitalaria y coordinados con el área que se encargará de la prestación del soporte y deben seguir el siguiente orden.

- Presentar la propuesta de la modificación o adición de un nuevo servicio TIC al Líder de Sistemas de Información.
- Documento o acta de aprobación de la propuesta por parte del Jefe Oficina Asesora Sistemas de Información Hospitalaria.

La propuesta debe contener como mínimo:

- Descripción del problema a solucionar.
- Estudio de opciones con puntos a favor y en contra.
- Cotizaciones o presupuesto requerido
- Riesgos asociados antes, durante y después de la implementación.
- Diseño del plan de contingencia y temas relativos a la seguridad de la información

3.2.4 Acuerdos de confidencialidad

El departamento de Jurídica del E.S.E. Ana Silvia Maldonado Jiménez de Colombia y el area del sistema de Información Hospitalaria, diseñaran los acuerdos de confidencialidad de acuerdo con los roles de todos los interesados (funcionarios de planta, contratistas, Outsourcing, prestación de servicios, convenios docencia-servicios, etc.).

El área TIC NO podrá conceder permisos a ningún sistema de información sin que exista el debido acuerdo de confidencialidad y de no-divulgación firmado.

Los acuerdos de confidencialidad serán revisados como mínimo de forma anual por el departamento de Jurídica E.S.E. Ana Silvia Maldonado Jiménez de Colombia y el Jefe Oficina Asesora Sistemas de Información Hospitalaria.

3.2.5 Autoridades y datos de contacto

Entidad	Descripción	URL - Teléfono

Centro Cibernético Policial	Centro especializado de atención de delitos Cibernéticos de la policía Nacional de Colombia.	Tel: 57(1) 4266302 https://caivirtual.policia.gov.co/Tel: 57(1) 5159700
Fiscalía General de la Republica	Delitos Informáticos, dependencia adscrita al CTI de la Fiscalía General de la Nación	www.fiscalia.gov.co/colombia/tag/delitos-informaticos/
Dirección de Investigación Criminal "SIJIN"	Grupo general de delitos informáticos	caivirtual@delitosinformaticos.gov.co Tel: 57(1)4266301 / 57(1)4266302 Delitos informáticos en el dpto. Huila Número de celular 3112157043

3. EVALUACIÓN

Para evidenciar el nivel de comprensión y adherencia del Manual de Seguridad de la Información dentro de funcionarios, colaboradores, proveedores, contratistas y personas de interés general de la E.S.E. Ana Silvia Maldonado Jiménez de Colombia, se utilizará el instrumento: auditoria de adherencia en seguridad de la información.

Los que se pretende una vez realizado el proceso de sensibilización o capacitación, es medir el conocimiento y percepción de las políticas de seguridad de la información por medio de la lista de chequeo de la auditoria medir la adherencia y cumplimiento de las políticas por parte de funcionarios, colaboradores, proveedores, contratistas y personas de interés en general del hospital.

4. CONTROL DE RESPONSABILIDADES

Elaboró	Revisó	Aprobó
NOMBRE: LILIANA MARCELA CASTRO JIMENEZ	**NOMBRE:** LILIANA MARCELA CASTRO JIMENEZ	**NOMBRE:** EDUARDO MAHECHA REYES
CARGO: Tesorera	**CARGO:** Tesorera	**CARGO:** Gerente
FECHA: Agosto 2025	**FECHA:** Agosto 2025	**FECHA:** Agosto 2025