MANUAL DE SEGURIDAD DE LA INFORMACIÓN

2020

CONTENIDO

1. INTRODUCCIÓN

El Hospital Universitario Hernando Moncaleano Perdomo de Neiva, 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, consecuencias legales y directrices 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 y la Guía 2 “Elaboración de la Política General de Seguridad y Privacidad de la Información” emitida por el MINTIC.

Las políticas descritas en este manual se constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información del Hospital Universitario Hernando Moncaleano Perdomo de Neiva 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 Hospital Universitario Hernando Moncaleano Perdomo de Neiva 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 al Hospital Universitario Hernando Moncaleano Perdomo de Neiva las políticas y directrices 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 del Hospital Universitario Hernando Moncaleano Perdomo de Neiva.
- Mantener altos niveles de confidencialidad, integridad y disponibilidad de los activos de información críticos del Hospital Universitario Hernando Moncaleano Perdomo de Neiva.
- 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 Hospital Universitario Hernando Moncaleano Perdomo de Neiva.
- 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 directrices 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 y activos de información dentro o fuera de las instalaciones del Hospital Universitario Hernando Moncaleano Perdomo de Neiva, 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
- **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, DGH, INDIGO, etc.
- **Personal**: Todo el personal del Hospital Universitario Hernando Moncaleano Perdomo de Neiva, subcontratado, los usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información.
- **Seguridad de la información**: Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
- **Servicios**: Son tanto los servicios internos, aquellos que una parte de la

organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.

- **Tecnología**: Son todos los equipos utilizados para gestionar la información y las comunicaciones.
- **Instalaciones**: Son todos los lugares en los que se alojan los sistemas de información.
- **Equipamiento Auxiliar**: Todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ej: 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

El Hospital Universitario Hernando Moncaleano Perdomo de Neiva, 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 activos de información más significativos 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 en pro de generar y mantener la confianza de sus usuarios, funcionarios, contratistas y terceros que se benefician directa e indirectamente con los servicios prestados por la institución.

Consciente de las necesidades actuales y apoyados en la innovación tecnológica como mecanismo para mejorar la seguridad de la información, el Hospital Universitario Hernando Moncaleano Perdomo de Neiva 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, recursos de procesamiento de la

información y cualquier otro activo de información del Hospital Universitario Hernando Moncaleano Perdomo de Neiva, 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 del Hospital Universitario Hernando Moncaleano Perdomo de Neiva 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.

Ante la evidencia del incumplimiento de la Política de seguridad y privacidad de la información, de las contenidas en el Manual de seguridad de la información o cualquier otra violación de la seguridad por parte de algún funcionario, contratista o tercero, se iniciará en contra de estos las respectivas investigaciones disciplinarias y multas a que haya lugar, de acuerdo con los procedimientos internos de la institución y normatividad referente a la seguridad de la información, privacidad y confidencialidad.

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) por el Comité de Seguridad de la Información y cuando se requiera alguna información o aclaración sobre la política respectiva, será solicitada al Oficial de seguridad de la información.

3.1.2 Política de Clasificación y etiquetado 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, garantizando una eficaz gestión de su seguridad con criterios de confidencialidad, disponibilidad e integridad.
Referencia normativa
Ley 594 de 2000 “Ley general de archivo”

Ley 1712 de 2014 “Ley de transparencia y del derecho de acceso a la información pública nacional”.
Decreto 103 de 2015 “Por el cual se reglamenta parcialmente la Ley 1712 de 2015.
Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1377 de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
ISO 30301 “Sistemas de Gestión Documental”.
NTC-GP 1000 o ISO 9001de 2008 Sistemas de Gestión de Calidad.
NTC ISO/IEC 27000 “Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – control A8.2.1 “Clasificación de la Información”.
NTC ISO 31000 Gestión del Riesgo
Decreto 2609 de 2012, “Instrumentos archivísticos para la gestión documental”.

Declaración

a) El Hospital definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de esta la cataloguen y determinen los controles requeridos para su protección.
b) La clasificación de la información estará alineada a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política respectiva, será solicitada al Oficial de seguridad de la información.
d) La presente política será revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a líderes y colaboradores de planta, contratistas y todos aquellos que manejen activos de información institucional o que estén involucrados con su administración, quienes tienen la responsabilidad de cumplir cabalmente dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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 y anexos, información contable, información jurídica, entre otras propias de los procesos).
- El líder del proceso/área/propietario de la información o a quien delegue, será el responsable de clasificar la información que tiene bajo su responsabilidad teniendo en cuenta la criticidad, sensibilidad, reserve de la misma y a los riesgos, amenazas e impactos en caso de materialización de éstos.
- Toda la información del hospital debe ser identificada, clasificada y etiquetada de acuerdo con el procedimiento establecido por el hospital y a la referencia normativa relacionada anteriormente.

3.1.3 Política de Seguridad para los usuarios de activos de información

Objetivo

Verificar que los funcionarios, contratistas y demás colaboradores del Hospital Universitario Hernando Moncaleano Perdomo de Neiva, entiendan sus responsabilidades y funciones, con el fin de reducir el riesgo de hurto, pérdida de integridad, fraude, uso inadecuado de la información y de las instalaciones

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – control A7 “Seguridad de los recursos humanos”.

Declaración

a) El hospital reconoce la importancia del factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará un proceso de formación orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos con el fin de darle un tratamiento responsable a los activos de información a su cargo.
b) Las directrices de la política de seguridad para los usuarios de activos de información están alineadas a la normatividad enunciada anteriormente

(Referencia normativa).

c) Toda información o aclaración sobre la política de seguridad para los usuarios de activos de información, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores (planta, contratistas, entre otros) que de forma directa o indirecta tengan responsabilidad sobre los activos de información y gestión de las TIC bajo sus procesos o aquellos que estén involucrados con su administración y, serán responsables de cumplir sin excepción alguna las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- Asegurar que los funcionarios de planta, contratistas y demás colaboradores del Hospital Universitario Hernando Moncaleano Perdomo de Neiva, entiendan sus responsabilidades en relación con las políticas de seguridad de la información y cumplan estrictamente las mismas, 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 los equipos asignados y 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 cualquier documento generado, procesado o almacenado por el hospital; los cuales son el resultado de los procesos informáticos generados en cada área.

- La información generada y recibida del hospital (verbal, física o electrónica), debe ser usada por los usuarios o contratistas únicamente para los propósitos de la misionalidad de la institución, por las funciones propias de su cargo; la cual debe ser procesada, entregada o transmitida íntegra y exclusivamente a las personas o entes de control (previa autorización del jefe inmediato) que la requieran, a través de los medios definidos, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.
- Los equipos tecnológicos 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 a la mesa de ayuda (Service Desk) del Área de TIC del Hospital por quien haya detectado el suceso y/o el líder responsable del área afectada a través de los siguientes canales:

    - Plataforma tecnológica de solicitudes a la mesa de ayuda.
    - Correo electrónico institucional.
    - Llamado a través de líneas telefónicas.

- Se deben reportar eventos o incidentes de seguridad relacionados con los medios de procesamiento de información, medios de almacenamiento de información, plataforma tecnológica, sistemas de información, medios físicos de almacenamiento y personas.
- Todo evento o incidente de seguridad de la información se debe reportar en la presencia de los siguientes casos:

    - Daño, pérdida, fuga y/o robo de información.
    - Robo de credencias.
    - Modificación no autorizada de la información.
    - Comportamiento anormal del computador y/o sistema de información.
    - Suplantación de identidad.

- Accesos no autorizados.
- Pérdida o alteración de registros de base de datos.
- Pérdida de un activo de información.
- Presencia de códigos maliciosos “malware, Ransomware”.
- Denegación del servicio.
- Ciberataques.

- De ser necesario, reportar los incidentes de seguridad a las autoridades competentes a través de los datos de contacto descritos en el numeral 3.2.5 del presente manual.
- Dar cumplimiento al procedimiento de Gestión de eventos e incidentes de seguridad de la información, aprobado por el 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – control A9 “Control de acceso”.

Declaración

a) El hospital a través del área TIC tiene la gran responsabilidad de brindar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información por medio de una gestión efectiva y eficiente del área TIC orientada a la correcta administración de accesos de los sistemas, bases de datos y gestión TIC.
b) Las directrices de la política para funcionarios y contratistas del área TIC están alineadas a la normatividad enunciada anteriormente (Referencia

normativa).

c) Toda información o aclaración sobre la política para funcionarios y contratistas del área TIC, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida al personal del área TIC como responsables de la administración de los sistemas de información (accesos, gestión), quienes deberán cumplir a cabalidad las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- El personal del área TIC no debe dar a conocer las claves de usuario de la administración de los sistemas informáticos y demás a personal ajeno a su área.
- Los usuarios y claves de los administradores de sistemas y del personal del área TIC son de uso personal e intransferible.
- El personal del área TIC debe emplear obligatoriamente claves o contraseñas con un alto nivel de complejidad.
- Los medios de instalación y seriales del software adquirido por el Hospital Universitario Hernando Moncaleano Perdomo 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 aplicar las mejores prácticas para la eliminación segura de la información contenida en ellos (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 TIC no otorgará privilegios especiales a usuarios sobre

las estaciones de trabajo sin la autorización correspondiente del Oficial de seguridad de la información.

- El personal del área TIC 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 TIC 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 Oficial de seguridad de la información, 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 el Hospital Universitario Hernando Moncaleano Perdomo para la ejecución de las actividades que requieran el acceso al software.
- El Hospital Universitario Hernando Moncaleano Perdomo, 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 Oficial de seguridad de la información puede implicar amenazas legales y de seguridad de la información para la entidad, por lo cual esta práctica no está autorizada. El personal encargado de redes e infraestructura dentro del área TIC, deberá llevará el control de las cantidades de licencias disponibles.
- El acceso al software y la documentación de éste solamente podrá ser consultado y usado en el ejercicio de las actividades contractuales.
- Cumplir siempre con el registro en la bitácora de acceso al DataCenter de las personas que ingresen y que hayan sido autorizadas previamente por el Oficial de seguridad de la Información 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 la entidad a través del Comité de Seguridad de la Información.
- 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

Objetivo

Proteger la integridad de la página Web institucional al igual que el software y la información contenida en ellas.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A8 “Gestión de activos”.
Control A9 “Control de acceso”.
Control A13 “Seguridad de las comunicaciones”.

Declaración

a) Controlar la administración, permisos y accesos de la página WEB con el fin de controlar y disminuir las posibles amenazas y vulnerabilidades que pueden afectar la imagen institucional, la disponibilidad de los servicios brindados, la integridad y la confidencialidad de la información que se trasmite a través de la misma.
b) Las directrices de la política para Webmaster están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política para Webmaster, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con las áreas responsables de la administración y control de la misma, a fin de evitar su ocurrencia.
f) La presente política va dirigida al personal del área TIC como responsable de la administración de las página, al área de Mercadeo y Comunicaciones como responsable de la revisión de los contenidos a publicar bajo

lineamientos de publicación estándar y a los líderes de las áreas que requieran la necesidad de realizar publicaciones alusivas a lo laboral en la página, cumpliendo los lineamientos y directrices por las áreas administradoras y cuya responsabilidad de las partes involucradas se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- Los líderes de áreas que requieran publicar información institucional en la página Web deben preparar y depurar la información de su área y reportar a la Oficina de Mercadeo y Comunicaciones como área responsable de verificar ortografía, redacción e imagen corporativa de la información a publicar. Posteriormente esta área (Mercadeo) generará una solicitud a la mesa de ayuda del área TIC para efectuar los cambios correspondientes.
- El responsable de redes e infraestructura del área TIC 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.
- Toda información publicada en la web propia de la misión institucional debe conservar el principio de integridad; razón por la cual no deben realizarse modificaciones ni alteraciones no autorizadas por el responsable de dicha información.

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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A7 “Seguridad de los recursos humanos”.

Declaración

a) Establecer mecanismos de control en las relaciones contractuales con terceros con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los terceros, cumplan con las políticas de seguridad de la información del Hospital, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios, en pro de preservar la confidencialidad, integridad y disponibilidad de la información generada, transmitida, almacenada en el marco de las relaciones contractuales a que haya lugar.
b) Las directrices de la política de tercerización u outsourcing están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de tercerización u outsourcing, será solicitada al Oficial de seguridad de la Información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los contratistas, terceros, agremiaciones que tengan relación contractual con el hospital y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A12 “Seguridad de las operaciones”.

Declaración

a) Propender por la protección, el correcto monitoreo y funcionamiento de los medios y equipos donde se almacena y procesa la información institucional, velando por la disponibilidad y restauración en caso de emergencia.
b) Las directrices de la política de disposición de información, medios y equipos están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de disposición de información, medios y equipos, será solicitada al Oficial de seguridad de la Información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.

e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los funcionarios que hacen parte del área TIC como responsables en la administración de sistemas y medios de almacenamiento y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas que permitan su monitoreo y correcto estado de funcionamiento; para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.
- El servicio de acceso a internet, sistemas de información, medio de almacenamiento, aplicaciones (Software), accesos a la red, navegadores y equipos de cómputo son propiedad del hospital y deben ser usados únicamente para el cumplimiento de la misión del hospital.
- Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita el servicio de puertos USB en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través del Comité de seguridad de la información.

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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A12 “Seguridad de las operaciones”.

Declaración

a) Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.
b) Las directrices de la política de respaldo y restauración de la información están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de respaldo y restauración de la información, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los funcionarios que hacen parte del área TIC como responsables de la administración de los sistemas de información y líderes de área como responsables de verificar y depurar la información de sus áreas contenidas en las unidades de almacenamiento dispuestas por el hospital y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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 el Hospital Universitario Hernando Moncaleano Perdomo de Neiva 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 TIC 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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A8 “Gestión de activos”.

Declaración

a) El hospital como propietario de la información física y así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.
b) Las directrices de la política de gestión de activos de información están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de gestión de activos de información, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la Información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los líderes de área y funcionarios con responsabilidad y relación directa sobre los activos de información a su cargo y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- El Hospital Universitario Hernando Moncaleano Perdomo mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado en el área TIC.
- El inventario de activos se debe actualizar cada vez que ocurra alguno de los siguientes eventos: identificación de un nuevo activo de información, se reclasifique el activo y/o por lo menos una vez al año.
- Los responsables de realizar la actualización de los activos de información serán los líderes del proceso/ área y para ello utilizarán el formato “Inventario de activos de información”.
- El Hospital Universitario Hernando Moncaleano Perdomo de Neiva, 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A6 “Organización de la seguridad de la información”.
Anexo A – control A7.2.2 “Toma de conciencia, educación y formación en la seguridad de la información”.

Declaración

a) Proporcionar las directrices necesarias que orienten a los usuarios al uso responsable de los activos de información a su cargo, en pro de cumplir con los propósitos y objetivos del negocio.
b) Las directrices de la política de uso de los activos están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de uso de los activos, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores del hospital (de planta, contratistas, agremiaciones, etc) que tengan relación directa o

indirecta con el manejo, procesamiento, almacenamiento de información y uso de los activos en la ejecución de las relaciones contractuales con el hospital y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- Los activos de información pertenecen al Hospital y el uso de estos deben emplearse exclusivamente con propósitos laborales. Los activos de información (hardware) proveídos por el contratista o de terceras partes, serán administrados y estarán bajo la supervisión del personal 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 TIC del Hospital.
- 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 área TIC efectuará una auditoria a los computadores para revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas 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 Comité de seguridad de la Información.
- Estarán bajo custodia de la Oficina del Oficial de seguridad de la información los medios magnéticos (CD, DVD u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso; al igual 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 TIC.
- En caso de ser necesario y previa autorización del Comité de Seguridad de la 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 a 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 no 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 del hospital.
    - Bajar o descargar software de internet u otro servicio en línea en cualquier equipo del Hospital.
    - Modificar, revisar 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A6 “Organización de la seguridad de la información”.
Anexo A – control A7.2.2 “Toma de conciencia, educación y formación en la seguridad de la información”.

Declaración

a) El propósito del hospital es establecer reglas que permitan orientar que la seguridad sea parte integral de los activos de información a través de la correcta y responsable utilización de las estaciones de trabajo.
b) Las directrices de la política de uso de estaciones cliente están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de uso de estaciones cliente, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la Información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.

f) La presente política va dirigida a todos los colaboradores del hospital (de planta, contratistas, agremiaciones, etc) que tengan relación directa o indirecta con el manejo, procesamiento, almacenamiento de información y uso de los activos en la ejecución de las relaciones contractuales con el hospital y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- La instalación de software en los computadores suministrados por el Hospital es una función exclusiva del área 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 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A7.2.2 “Toma de conciencia, educación y formación en la seguridad de la información”.
Anexo A – Control A8 “Gestión de activos”.

Declaración

a) El hospital consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias y de igual forma a través del área TIC realizar monitoreos sobre el uso del servicio.
b) Las directrices de la política de uso de internet están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de uso de internet, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando

haya lugar.

e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.

f) La presente política va dirigida a todos los colaboradores del hospital (de planta, contratistas, agremiaciones, etc) que producto de su rol y actividades laborales a ejecutar requieran de acceso al servicio de internet proporcionado por el hospital y aquellos involucrados con la administración y control de acceso a estos servicios en red y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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.
- 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.
- 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

Objetivos

Definir las pautas generales para asegurar una adecuada protección de la información del Hospital Universitario Hernando Moncaleano Perdomo, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A7.2.2 “Toma de conciencia, educación y formación en la seguridad de la información”.
Anexo A – Control A8 “Gestión de activos”.

Declaración

a) Concientizar a los colaboradores del hospital de las buenas prácticas a seguir sobre las normas y el uso del servicio de mensajería instantánea para aquellos roles autorizados; así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.
b) Las directrices de la política de uso de mensajería instantánea y redes sociales están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de uso de mensajería instantánea y redes sociales, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando hay lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a los colaboradores del hospital que por la naturaleza de sus funciones requieran hacer uso de los servicios de mensajería instantánea y redes sociales y aquellos involucrados con la administración y control de acceso a estos servicios en red y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- El uso de servicios de mensajería instantánea y 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 institución o cualquier contenido con riesgo de código malicioso.
- La información que se publique por cualquier medio de Internet de algún colaborador o contratista del hospital, que sea creado a nombre personal en redes sociales (Twitter, Facebook, YouTube, 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.
- Toda información publicada a través de los servicios de mensajería instantánea y redes sociales propia de la misión institucional debe conservar el principio de integridad; razón por la cual no deben realizarse modificaciones ni alteraciones no autorizadas por el responsable de dicha información.

3.1.14 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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A9 “Control de acceso”.
Anexo A – Control A13 “Seguridad de las comunicaciones”.

Declaración

a) El área TIC como responsable de las redes de datos y los recursos de red del hospital, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.
b) Las directrices de la política de uso de discos de red o carpetas virtuales están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de uso de discos de red o carpetas virtuales, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando

haya lugar.

e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.

f) La presente política va dirigida a todos los colaboradores del hospital que por la naturaleza de sus funciones les hayan generado permisos para accesos a carpetas de red internas para el almacenamiento y transferencia de información y aquellos involucrados con la administración y control de acceso a estos servicios en red y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- Para que los usuarios tengan acceso a la información en los discos de red, el jefe inmediato deberá enviar una solicitud a la mesa de ayuda del área 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.
- 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 de propiedad del hospital (computadores de escritorio o portátiles, tablets, 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 (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.

3.1.15 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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A7.2.2 “Toma de conciencia, educación y formación en la seguridad de la información”.
Anexo A – Control A8 “Gestión de activos”.

Declaración

a) Establecer normas claras para el uso de periféricos (impresoras) pertenecientes al hospital en concordancia a las actividades laborales y al cumplimiento de los lineamientos ambientales a fin de minimizar o mantener controlado el impacto ambiental que estas actividades generan.
b) Las directrices de la política de uso de impresoras y servicio de impresión están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de uso de uso de impresoras y servicio de impresión, será solicitada al Oficial de seguridad de la Información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores del hospital que hagan uso de los recursos tecnológicos como impresoras, escáner de propiedad del hospital y cuya responsabilidad se verá reflejada en el

cumplimiento a cabalidad de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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.

3.1.16 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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A12 “Seguridad de las operaciones”.

Declaración

a) Resguardar la seguridad de la red de datos del hospital de intrusiones maliciosas, infecciones de virus y tener un control adecuado de la misma.
b) Las directrices de la política de uso de puntos de red de datos están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de uso de puntos de red de datos, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.

e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida al área TIC como responsable de controlar y monitorear los accesos a la red de datos del hospital y a los colaboradores autorizados para hacer buen uso de la red de datos a los que fueron autorizados y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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.

3.1.17 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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A12 “Seguridad de las operaciones”.

Declaración

a) Establecer normas para un buen uso del DataCenter con el propósito de mantener la seguridad, integridad y apariencia del mismo.
b) Las directrices de la política de seguridad del centro de datos (DataCenter)

están alineadas a la normatividad enunciada anteriormente (Referencia normativa).

c) Toda información o aclaración sobre la política de seguridad del centro de datos (DataCenter), será solicitada al Oficial de seguridad de la Información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida al área TIC como responsable directo de administrar y controlar los accesos y gestiones que se realicen dentro del DataCenter y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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 TIC debe garantizar que el 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 TIC deberá garantizar que todos los equipos de los 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 TIC. 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 oficial de seguridad de la información.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista del área TIC.
- 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.

3.1.18 Políticas de seguridad de los equipos de cómputo

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

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A7.2.2 “Toma de conciencia, educación y formación en seguridad de la información”.
Anexo A – Control A8 “Gestión de activos”.
Declaración

a) Generar los controles necesarios para evitar la pérdida, robo, daño o exposición al peligro de los recursos de la plataforma tecnológica del hospital que se encuentren dentro o fuera de sus instalaciones.
b) Las directrices de la política de seguridad de los equipos de cómputo están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de seguridad de los equipos de cómputo, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores que hagan uso de los activos y recursos tecnológicos del hospital en función de sus actividades laborales y aquellos involucrados con la administración y protección de los mismos y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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), 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.

3.1.19 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A7.2.2 “Toma de conciencia, educación y formación en seguridad de la información”.
Anexo A – Control A8 “Gestión de activos”.
Anexo A – Control A11.2.9 “Política de escritorio, pantalla limpia y equipos desatendidos”

Declaración

a) Establecer buenas prácticas para el orden y la limpieza en el puesto de trabajo, acompañadas de las políticas de seguridad de la Información y seguridad física enmarcada en el esfuerzo eficaz y la aceptación de responsabilidades en el manejo de activos de la entidad que estén a cargo del colaborador, logrando un ambiente seguro y propicio al cambio.
b) Las directrices de la política de escritorio, pantalla limpia y equipo desatendidos están alineadas a la normatividad enunciada anteriormente

(Referencia normativa).

c) Toda información o aclaración sobre la política de escritorio, pantalla limpia y de equipo desatendido, será solicitada al Oficial de seguridad de la Información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores que hagan uso de los activos y recursos tecnológicos del hospital en función de sus actividades laborales y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- El personal del Hospital o contratistas debe conservar su escritorio libre de información confidencial de la entidad, que pueda ser alcanzada, copiada o utilizada 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 de la 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 configurados a la red del hospital.

3.1.20 Política de uso de correo electrónico

Objetivo

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

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A7.2.2 “Toma de conciencia, educación y formación en seguridad de la información”.
Anexo A – Control A8 “Gestión de activos”.

Declaración

a) Definir pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de correo electrónico por parte de los colaboradores autorizados.
b) Las directrices de la política de uso de correo electrónico están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de uso de correo electrónico, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores a quienes se les haya asignado una cuenta de correo electrónico institucional para uso laboral y aquellos involucrados con la administración y control de acceso a estos servicios en red y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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.
- Toda información propia de la misión institucional transmitida a través de los correos electrónicos institucionales debe conservar el principio de integridad; razón por la cual no deben realizarse modificaciones ni alteraciones no autorizadas por el responsable de dicha información.
- 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 debe 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 Oficial de seguridad de la información.
- 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 el Hospital Universitario Hernando Moncaleano Perdomo, las cuales serán asignadas con previa autorización del Oficial de seguridad de la información.
- 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 y ofensivos
  - 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 u 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 y de 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 almacenar los 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.

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

Objetivo
Establecer una serie de directrices para la asignación correcta de cuentas de correo institucional y evitar confusiones con usuarios homólogos.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A8 “Gestión de activos”.
Control A9 “Control de acceso”.

Declaración

a) Ofrecer una guía y requerimientos mínimos que se deben satisfacer para la asignación de cuentas y posterior uso adecuado del correo electrónico.
b) Las directrices de la política de asignación de nombres de usuario para las cuentas de correo institucional están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de asignación de nombres de usuario para las cuentas de correo institucional, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores a quienes se les haya asignado una cuenta de correo electrónico institucional para uso laboral y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización

del Manual de seguridad de la información.

Recomendación general

El nombre de usuario asignado será el primer nombre más un punto más el primer apellido. Por ejemplo, para León Darío Valencia Montoya sería leon.valencia@huhmp.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 León Darío Valencia Tangarife sería leond.valencia@huhmp.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@huhmp.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. Se recomienda o se exigirá utilizar en una misma contraseña números, letras (mayúsculas – minúsculas) 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 la contraseña.
- 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.).

3.1.22 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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A9 “Control de acceso”.

Declaración

a) El área TIC del hospital como responsable de la administración de los sistemas de información, debe propender por el adecuado control y monitoreo de los accesos que se hagan a los diferentes sistemas los usuarios con los roles asignados y evitar intrusiones no autorizadas.
b) Las directrices de la política de control de accesos a sistemas y aplicativos están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de control de accesos a sistemas y aplicativos, será solicitada al Oficial de seguridad de la información.

d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores a quienes se les haya asignado permisos de accesos a los sistemas de información en uso de sus actividades y al área TIC como área involucrada en la administración de dichos permisos y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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 el Oficial de seguridad de la información.
- 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 del 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.
- 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 procedimientos establecidos, perfiles y necesidades de uso.
- 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, por lo 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 la contraseña de otros usuarios.
- No se podrá realizar ninguna actividad de tipo remoto sobre los equipos, servidores principales sin la debida aprobación del Oficial de seguridad de la información.
- 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.

3.1.23 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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A8.3.1 “Gestión de medios removibles”.
Control A6.2.1 “Política para dispositivos móviles”

Declaración

a) Los dispositivos móviles en el hospital son imprescindibles para el desarrollo del trabajo, sin embargo, los mismos representan un riesgo asociado frente a la pérdida y el uso no autorizado, por lo cual se definen una serie de directrices orientadas a regular el manejo de los mismos y evitar los riesgos.
b) Las directrices de la política para dispositivos móviles están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política para dispositivos móviles, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área

respectiva, a fin de evitar su ocurrencia.

f) La presente política va dirigida a todos los colaboradores (de planta, contratistas, etc) a quienes se les haya autorizado los permisos para el uso de dispositivos móviles (propios y del hospital) dentro de la institución y al área TIC como responsable de la administración de dichos permisos y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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 (Discos duros 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 Oficial de seguridad de la información.
- El área 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 TIC deberá configurar el control de bloqueo automático de sesión de usuarios por inactividad.
- El área TIC debe activar la opción de cifrado de discos en aquellos dispositivos móviles institucionales que almacenan información sensible.
- El área 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 en caso de pérdida o hurto.
- El área 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 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 para evitar 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.

3.1.24 Política de transferencia de información

Objetivo

Presentar los lineamientos orientados para la protección de la información sensible tanto del Hospital como de los usuarios en aquellas situaciones en las cuales sea necesario o se requiera realizar su transferencia a terceros, asegurando que ésta 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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A8 “Gestión de activos”.
Control A8.3.3 “Transferencia de medios físicos”.

Declaración

a) Propender por la protección de la información en el momento de ser transferida o intercambiada con terceros por medio de controles necesarios que eviten la interceptación, accesos y usos no autorizados.
b) Las directrices de la política de transferencia de información están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de transferencia de información, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores, contratistas, y terceros que hagan transferencia de información producto de las relaciones contractuales, de prestación de servicios de salud, comerciales, judiciales, entre otras y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- 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, ni medios removibles que no estén controlados ni auditados por el área TIC.
- El área de correspondencia debe certificar que todo envió de información física a terceros (documentos en físico 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 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, familiar o usuario en común.
- Siempre se deberá preguntar por el nombre completo del paciente o usuario para asegurar que se está comunicado con la persona indicada y a través

del uso de validación de información.

- No se deben dejar mensajes con información sensible con personas diferentes al paciente o usuario, en equipos de respuesta automática o mensajes de voz, a no ser que el mensaje sea urgente y sin datos sensibles.

Contacto vía correo electrónico

- Únicamente información NO sensible podrá ser enviada a cuentas de correo electrónico de pacientes o usuarios.
- 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, usuarios 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 el Oficial de seguridad de la información).

3.1.25 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A9 “Control de acceso”.

Declaración

a) Proveer una serie de directrices para establecer el control de los accesos sobre los sistemas de información, aplicaciones y servicios en red, basados en los requerimientos de seguridad y operacionales del hospital.
b) Las directrices de la política para revisión de los derechos de acceso a usuarios están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política para revisión de los derechos de acceso a usuarios, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores y contratistas con permisos de acceso a aplicativos, sistemas de información y servicios en red y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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.

3.1.26 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A8.3.2 “Disposición final de medios”.

Declaración

a) Proveer directrices claras sobre las medidas a tomar al momento de dar de baja los medios de información de forma segura y evitar la recuperación de la información contenida en ellos.
b) Las directrices de la política para disposición final de medios cuando no se requieran están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política para disposición final de medios cuando no se requieran, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando

haya lugar.

e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.

f) La presente política va dirigida a las áreas de activos fijos, gestión documental, seguridad y salud en el trabajo, área TIC como responsables de realizar los análisis y tomar la decisión de disponer de forma final los medios de información que ya no se requieran dentro del hospital y cuya responsabilidad se verá reflejada en el cumplimiento a cabalidad de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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, dando cumplimiento a las siguientes actividades:

    - Separar el papel a disponer y que se encuentre en buen estado.
    - Realizar destrucción manual del papel a disponer.
    - 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.
- Los equipos de cómputo que ya no se requieran por su obsolescencia o daño, serán revisados por personal del área 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).

3.1.27 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A7 “Seguridad de los recursos humanos”.

Declaración

a) Realizar la recepción de los activos devueltos por los diferentes procesos o áreas y determinar el estado, integridad y disposición final de los mismos.
b) Las directrices de la política de devolución de activos están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de devolución de activos, será solicitada al Oficial de seguridad de la información.

d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los funcionarios y contratistas que, por motivo de terminación de la relación laboral o contractual, reubicación laboral y que hasta dicha terminación o cambio hayan tenido información y activos a su cargo, deben ser devueltos de forma íntegra y aquellas áreas responsables de la gestión de retiro de usuarios (Talento humano), gestión de permisos a sistemas (área TIC), gestión de devolución de equipos (activos fijos), dando cumplimiento a cabalidad de las directrices siguientes.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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 del Oficial de seguridad de la información 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 del Hospital Universitario Hernando Moncaleano Perdomo, 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A13.2.4 “Acuerdos de confidencialidad o de no divulgación”
Control A15 “Relaciones con los proveedores”.

Declaración
a) Establecer mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.
b) Las directrices de la política de seguridad para relación con proveedores

están alineadas a la normatividad enunciada anteriormente (Referencia normativa).

c) Toda información o aclaración sobre la política de seguridad para relación con proveedores, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los proveedores de servicios e insumos que tengan relación contractual con el hospital, dando cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

La política de relación con proveedores, indica aquellas buenas prácticas que el Hospital Universitario Hernando Moncaleano Perdomo 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 del Hospital Universitario Hernando Moncaleano Perdomo.
- 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 del Hospital Universitario Hernando Moncaleano Perdomo.
- 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 Hospital Universitario Hernando Moncaleano Perdomo 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 del Hospital Universitario Hernando Moncaleano Perdomo 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.

NTC ISO/IEC 27001 – Anexo A – Control A6.1.5 “Seguridad de la información para la gestión de proyectos”.

Declaración

a) Definir los lineamientos que se deben tener en cuenta en materia de seguridad de la información para la gestión de nuevos proyectos en el hospital con el fin de tener en cuenta los riesgos inmersos en cada uno de ellos y generar la planeación respectiva.
b) Las directrices de la política para la gestión de proyectos están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política para la gestión de proyectos, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la Información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los procesos del hospital en donde se definan y propongan proyectos de inversión para mejora de la institución y aquellos que lo lideran deben dar cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A12 “Seguridad de las operaciones”.
Control A14 “Adquisición, desarrollo y mantenimiento de sistemas”.

Declaración

a) Realizar un adecuado análisis de los requerimientos legales y de mejora de las aplicaciones del hospital y de esta forma asegurar que el desarrollo implementado cumpla las necesidades de la institución
b) Las directrices de la política para desarrollo externo de software están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política para desarrollo externo de software, será solicitada al Oficial de seguridad de la Información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.

f) La presente política va dirigida a los proveedores externos de software y al área TIC como responsables de realizar seguimiento y pruebas a las mejoras y ajustes a los desarrollos y deben dar cumplimiento a cabalidad de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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 TIC debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del hospital.
- El área TIC debe asegurar que los sistemas de información desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- El área 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.
- 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 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.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A11.2.6 “Seguridad de equipos y activos fuera de las instalaciones”.

Declaración

a) Definir los lineamientos que se deben tener en cuenta en materia de seguridad de la información para dar protección adecuada a los activos de información que requieran salir de la institución.
b) Las directrices de la política para seguridad de equipos y activos fuera de las instalaciones están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política para seguridad de equipos y activos fuera de las instalaciones, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de

la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.

e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.

f) La presente política va dirigida a todos los colaboradores que por autorización de los líderes de áreas y de acuerdo con sus funciones laborales requieran sacar de las instalaciones algún equipo, dando cumplimiento a cabalidad de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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, 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; así como aquellas destinadas a la carga y descarga de equipos, materiales e insumos.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – A11 “Seguridad física y del entorno”
Control A11.1.3 “Seguridad de oficinas, recintos e instalaciones”.
Resolución 0741 del 14 de marzo de 1997, expedida por el Ministerio de Salud), la cual imparte instrucciones sobre seguridad personal de usuarios para instituciones Prestadores de Servicios de Salud.
Decreto 356 de febrero 11 de 1994 Estatuto de Vigilancia y Seguridad Privada
Ley 61 de 1993, en su decreto 2535 del mismo año, estableció las pautas para el control de armas, municiones y explosivos en todo el territorio nacional.

Declaración

a) Proteger físicamente los recursos y la información generada en las diversas áreas a través del control de accesos a las instalaciones y áreas físicas no autorizadas a través del acompañamiento al personal ajeno a la institución con el fin de prevenir daños y robos a los activos de información propios de la entidad.
b) Las directrices de la política para seguridad de oficinas, recintos e instalaciones están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política para seguridad de oficinas, recintos e instalaciones, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.

e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores, proveedores y partes interesadas que tengan acceso a las instalaciones y a los recursos de información del hospital y su compromiso se verá reflejado con el cumplimiento de las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

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 a la institución (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, deben 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.
- Las áreas destinadas a la carga, descarga y entrega de materiales e insumos deben ser controladas y en lo posible separadas de las áreas seguras para evitar el acceso no autorizado a estas últimas.
- Realizar acompañamiento al proveedor en las actividades de carga y descarga de materiales e insumos a fin de prevenir accesos a áreas no autorizadas.
- Todo vehículo que ingrese a las zonas destinadas para carga o descarga de equipos, materiales e insumos y que ingrese para tal fin, será objeto de revisión por parte del personal de vigilancia contratado.
- 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 de 2013 (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 ESE Hospital Universitario Hernando Moncaleano Perdomo 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 ESE ESE Hospital Universitario Hernando Moncaleano Perdomo, identificada con NIT. 891180268-0, con domicilio en la ciudad de Neiva, Calle 9 No. 15-25, Correo Electrónico: hospital.universitario@huhmp.gov.co, teléfono 8715907, Línea gratuita 018000957878, es la responsable del tratamiento de los datos obtenidos de sus diferentes grupos de interés.

Referencia normativa

Ley 1581 de 2012 (Art. 17 Lt. k y Art. 18 Lt. f)
Decreto 1377 de 2013 (Art. 13.
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A18.1.4 “Privacidad y protección de información de datos personales”.

Declaración

a) Establecer los lineamientos para la administración y tratamiento de datos personales de las partes interesadas en el hospital.
b) Las directrices de la política de tratamiento y protección de datos personales están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política de tratamiento y protección de datos personales, será solicitada al Oficial de seguridad de la información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política está orientada a todo el hospital (procesos, líderes, usuarios, pacientes, proveedores, contratistas, estudiantes) en el marco de la protección de los datos personales y el compromiso de las partes

interesadas se verá reflejado con el cumplimiento de las directrices contenidas en dicha política.

g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

La ESE ESE Hospital Universitario Hernando Moncaleano Perdomo, 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 ESE Hospital Universitario Hernando Moncaleano Perdomo, 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 ESE Hospital Universitario Hernando Moncaleano Perdomo, 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 ESE Hospital Universitario Hernando Moncaleano Perdomo, 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 ESE Hospital Universitario Hernando Moncaleano Perdomo, 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 ESE Hospital Universitario Hernando Moncaleano Perdomo 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 ESE Hospital Universitario Hernando Moncaleano Perdomo.

- El tratamiento de los datos personales proporcionados por los colaboradores de la ESE Hospital Universitario Hernando Moncaleano Perdomo 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 ESE Hospital Universitario Hernando Moncaleano Perdomo, 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 de ser 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 ESE Hospital Universitario Hernando Moncaleano Perdomo 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 ESE Hospital Universitario Hernando Moncaleano Perdomo

- 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 ESE Hospital Universitario Hernando Moncaleano Perdomo 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 versen 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 ESE Hospital Universitario Hernando Moncaleano Perdomo, recolecta información en base de datos.
- Revocar en cualquier momento la autorización dada para contener información personal en las bases de datos de la ESE Hospital Universitario Hernando Moncaleano Perdomo.
- 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 ESE Hospital Universitario Hernando Moncaleano Perdomo, 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 1581 de 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 ESE Hospital Universitario Hernando Moncaleano Perdomo, mediante la aplicación de su proceso: Gestión y tratamiento de PQRSF.

3.1.34. Política de No Repudio

Objetivo
Propender porque toda la información enviada, trasmitida y/o recibida en desarrollo de los servicios de red de la entidad se puede probar y no pueda ser negada posteriormente.

Referencia normativa
NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – control A8.3.3 “Transferencia de medios físicos”.

Control A9 “Control de acceso”

Control A12.7.1 “Controles de auditoría de sistemas de información.

Declaración

a) Proporcionar protección contra la interrupción, por parte de algunas de las partes implicadas en la comunicación o transferencia de información a que haya lugar.
b) Las directrices de la política de no repudio están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
c) Toda información o aclaración sobre la política para funcionarios y contratistas del área TIC, será solicitada al Oficial de seguridad de la información, quien se encuentra adscrito a la Oficina de sistemas de información.
d) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
e) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
f) La presente política va dirigida a todos los colaboradores o terceros que en razón de sus funciones o relaciones hagan transferencia o comunicación de información y al área TIC como responsables de la administración de los sistemas de información (accesos, gestión), quienes deberán cumplir a cabalidad las directrices contenidas en dicha política.
g) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- El hospital se compromete a generar mecanismos de control incrementales que permitan realizar la trazabilidad en la modificación de los datos en los sistemas de información.
- El usuario que realice intercambio electrónico de información será el responsable directo por la información enviada desde medios institucionales y/o red de la entidad.
- El área TIC debe proveer los respectivos mecanismos de seguridad consignados para el tratamiento de mensajes electrónicos en la Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los

mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las Entidades de certificación y se dictan otras disposiciones", como son entre otros, encriptación de datos y firmas digitales, y en las demás disposiciones legales que rigen la materia.

- El área TIC debe producir, validar, mantener, y poner a disposición del Hospital pruebas o evidencias irrefutables respecto a la transferencia de información trasmitida a través de los canales institucionales (correo electrónico, gestión documental) usados en cada uno de sus procesos a nivel interno y externo, buscando información suficiente sobre la ocurrencia de un evento, el momento en el que ocurrió y las partes que intervinieron (emisor y receptor).
- El hospital en direccionamiento del área TIC debe hacer uso de mecanismos criptográficos como las firmas digitales para trazabilidad de la información enviada y/o recibida que se considere.

3.1.35. Política de disponibilidad de servicios digitales y de la información

Objetivo

Disminuir los posibles efectos de las interrupciones en los sistemas de información o el normal funcionamiento de la infraestructura tecnológica, asegurando la información considerada como crítica con los controles necesarios preventivos y de auto recuperación (Backups); además garantizar los niveles de disponibilidad según los acuerdos de nivel de servicio establecidos, incluyendo la gestión de cambios para el control de los sistemas de información.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A12 “Seguridad de las operaciones”.
Control A17 “Aspectos de seguridad de la información de la gestión de continuidad del negocio”.

Declaración

h) Asegurar la disponibilidad de la información crítica del negocio y la continuidad de sus operaciones mediante la aplicación de los controles necesarios.
i) Las directrices de la política de disponibilidad de servicios digitales y de la

información están alineadas a la normatividad enunciada anteriormente (Referencia normativa).

j) Toda información o aclaración sobre la política de disponibilidad de servicis digitales y de la información, será solicitada al Oficial de seguridad de la información, quien se encuentra adscrito a la Oficina de sistemas de información.

k) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.

l) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.

m) La presente política va dirigida al área TIC como responsables de la administración de los sistemas de información (accesos, gestión), quienes deberán cumplir a cabalidad las directrices contenidas en dicha política.

n) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- Generar un plan de la continuidad o plan de contingencia del sistema de información y dar seguimiento al mismo.
- Documentar los hallazgos o interrupciones en los sistemas de información para su análisis y búsqueda de mejora continua en el aspecto vulnerado.
- Implementaren las instalaciones de procesamiento de información redundancia suficiente para cumplir los requisitos de disponibilidad.
- Establecer acuerdos de niveles de servicio para los servicios ofrecidos y recibidos por el área TIC y velar por su cumplimiento.
- Propender por la protección de los activos de información del hospital que sean accesibles a personal ajeno a la institución.
- Se debe probar la efectividad del plan de recuperación (restauración de Backups) por lo menos una vez al año.
- Todos los cambios en los servidores y equipos de red del área TIC, incluyendo la instalación de nuevo software, el cambio de dirección IP, la

reconfiguración de routers, y switches, cualquier novedad y/o puesta en producción de servicios tecnológicos en hardware y/o software, deben ser documentados y debidamente aprobados por gestión de cambios. Esto es para prevenir cambios apresurados que puedan causar interrupción de los servicios de red o acceder en forma inadvertida a información confidencial.

3.1.36. Política de registro y auditoría

Objetivo

Auditar periódicamente los sistemas y actividades relacionadas a la gestión de activos de información; así como a almacenar los registros de cualquier evento de seguridad.

Referencia normativa

NTC ISO/IEC 27000 “Marco de Gestión de Seguridad de la Información”.
NTC ISO/IEC 27001 – Anexo A – Control A12 “Seguridad de las operaciones”.

Declaración

o) Dar respuesta a las debilidades asociadas a los sistemas de información a través de una adecuada gestión de los eventos de seguridad para una mejora efectiva del modelo de seguridad.
p) Las directrices de la política de registro y auditoría están alineadas a la normatividad enunciada anteriormente (Referencia normativa).
q) Toda información o aclaración sobre la política de registro y auditoría, será solicitada al Oficial de seguridad de la información, quien se encuentra adscrito a la Oficina de sistemas de información.
r) La presente política es revisada y autorizada por el Comité de seguridad de la información y aprobada por el Gerente en propiedad o encargado cuando haya lugar.
s) Todo hallazgo que afecte la seguridad de la información en relación con el incumplimiento de la presente política tendrá las correcciones necesarias y su posterior plan de lecciones aprendidas que será abordado con el área respectiva, a fin de evitar su ocurrencia.
t) La presente política va dirigida al área TIC como responsables de la
u) administración de los sistemas de información (accesos, gestión) y a cada

una de las áreas usuarias de los sistemas de información para hacer seguimiento al cumplimiento del manual de seguridad de la información.

v) La vigencia de la presente política inicia con la aprobación y/o actualización del Manual de seguridad de la información.

Directrices

- Anualmente se deben revisar los niveles de riesgo de los activos de información del hospital de acuerdo con la matriz definida.
- Cada una de las áreas usuarias debe monitorear los riesgos establecidos en la matriz con la periodicidad establecida y repórtalo al área de TIC.
- El área TIC debe monitorear y registrar los eventos de seguridad de la información.
- La Oficina asesora jurídica revisará la legislación aplicable y de los requisitos contractuales, en conjunto con el manejo de los derechos de propiedad intelectual.
- La Oficina asesora jurídica será apoyo para la verificación legal de la ley de protección y privacidad de datos personales y de la reglamentación de registros.

3.2 Capítulo II – Organización de la Seguridad de la Información

3.2.1 Compromiso de la dirección

La Gerencia del Hospital Universitario Hernando Moncaleano Perdomo de Neiva, 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 Gerencia del Hospital Universitario Hernando Moncaleano Perdomo demuestra su compromiso a través de:

- La aprobación de las políticas de seguridad de la información contenidas en este documento.
- La promoción de una cultura de seguridad de la información, enfocadas en planes de sensibilización y capacitación a través de los cuales se busca que todos los funcionarios, contratistas y externos del hospital cumplan de forma

obligatoria con las políticas de seguridad de la información.

- La divulgación del presente manual a todas las partes interesadas.
- La disposición de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.
- La creación y seguimiento al Comité de Seguridad de la Información, con la participación de un representante de la alta gerencia.
- El seguimiento de la aplicabilidad de los procesos disciplinarios y legales de acuerdo con los procedimientos internos de la institución y normatividad referente a la seguridad de la información ante la evidencia del incumplimiento de la Política de seguridad y privacidad de la información y de las contenidas en el Manual de seguridad de la información por parte de algún funcionario o contratista.

3.2.2 Coordinación de la seguridad de la información y ajuste a las políticas

El Hospital Universitario Hernando Moncaleano Perdomo de Neiva ha designado como representante de la alta dirección a la seguridad de la información al Jefe Oficina Asesora Sistemas de Información o quien haga sus veces.

Dentro del Comité de Seguridad de la Información se definirán los responsables, roles y las funciones de los representantes tanto de la alta gerencia como de algunas áreas del hospital 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).

En el evento que se llegue a materializar un incidente en ciberseguridad, el Oficial de seguridad de la información o Líder del área TIC serán los responsables de gestionar las comunicaciones con las autoridades competentes (ver numeral 3.2.5 Autoridades y datos de contacto) para la intervención y seguimiento a los mismos.

Ajustes a las políticas

Los ajustes a las políticas contenidas en el manual de seguridad de la información tienen como objetivo fortalecer la seguridad de los activos de información a través de los siguientes enfoques:

- Entrenamiento en seguridad,

- Administración del acceso a la información
- Protección contra códigos maliciosos
- Monitoreos a los eventos de seguridad
- Establecer procesos seguros para el manejo de sistemas, aplicaciones, información e infraestructura tecnológica.

Todo ajuste basado en algunos de los enfoques anteriores debe realizarse teniendo en cuenta lo siguiente:

- Requerimientos normativos en seguridad de la información o actualizaciones de la normatividad relacionada, en donde se exija el cumplimiento o ajuste a que haya lugar.
- Necesidades de protección de los activos de información.
- Cuando se adicione un nuevo servicio TIC o se identifiquen cambios en el contexto interno o externo en la institución

Para ello, el procedimiento a seguir para el ajuste y aprobación de las políticas será el siguiente:

- Generar en primera instancia los borradores sobre al ajuste a las políticas que requieran.
- Pasar a revisión por parte del Comité de seguridad de la información, quien será el responsable de revisar y autorizar los ajustes.
- Posteriormente, la oficina de planeación y desarrollo institucional se encargará de ajustar el documento de acuerdo al procedimiento de control documental definido por el hospital (versión, ajustes del contenido).
- Por último, el documento pasa a Gerencia para aprobación y desde esta área se emitirá la resolución respectiva con los nuevos documentos ajustados.

3.2.3 Proceso de autorización para servicios de procesamiento de información

Al ingresar nuevos servicios o ajustes a los ya existentes, estos deben ser aprobados por la Oficina Asesora Sistemas de Información 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 Jefe de Oficina Asesora de Sistemas de Información.
- Documento o acta de aprobación de la propuesta por parte del Jefe Oficina Asesora Sistemas de Información.

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

La Oficina Asesora Jurídica del Hospital Universitario Hernando Moncaleano Perdomo de Neiva y el Oficial de seguridad de la información, diseñaran los acuerdos de confidencialidad de acuerdo con los roles de las partes interesadas (funcionarios de planta, contratistas, Outsourcing, prestación de servicios, convenios docencia-servicios, etc.).

Los acuerdos de confidencialidad serán implementados por parte de las Oficinas de Contratación y Talento humano y serán revisados como mínimo de forma anual por la Oficina Asesora Jurídica del Hospital Universitario Hernando Moncaleano Perdomo de Neiva y el Oficial de seguridad de la información para realizar los ajustes a que haya lugar.

Cabe resaltar que el área TIC no concederá permisos a ningún Sistema de Información sin que exista el debido acuerdo de confidencialidad firmado por el respectivo usuario.

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.	http://www.ccp.gov.co/ Tel: 57(1) 4266302 https://caivirtual.policia.gov.co/ Tel: 57(1) 5159700
Fiscalía General de la República	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 investigativo de delitos informáticos	caivirtual@delitosinformaticos.gov.co Tel: 57(1)4266301 / 57(1)4266302 Delitos informáticos en el dpto. Huila Numero de celular 3112157043
Hospital Universitario Hernando Moncaleano Perdomo	Buzones para el reporte anónimo por incumplimiento o transgresión de las políticas y procedimientos de seguridad de la información establecidas en el hospital. Habilitado para cliente interno y externo.	seguridaddigital@huhmp.gov.co
colCERT	Grupo de respuesta a emergencias cibernéticas de Colombia	Línea de atención al cliente: (+ 57 1) 295 98 97 Para reportar un incidente o vulnerabilidad deberá escribir directamente a: Correo electrónico: **contacto[at]colcert.gov.co** Clave PGP/GPG: FF433551 Para enviar una muestra de malware se podrá escribir a: Correo electrónico: **malware[at]colcert.gov.co** Clave PGP/GPG: 22732D7B

4. 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 del Hospital Universitario Hernando Moncaleano Perdomo de Neiva, se utilizará el instrumento: auditoria de adherencia en seguridad de la información.

También se dispuso el curso de manual de seguridad de la información en la plataforma de aprendizaje e-learning, para lograr una mayor adherencia y facilitar los medios para el conocimiento del manual a los colaboradores del hospital, la cual cuenta con unas preguntas para evaluar el grado de aprendizaje. Para realizar el curso se puede acceder a través del siguiente ruta: http://formacion.hospitalneiva.gov.co/ dirigiendo se al curso "Manual de Seguridad de la Información"

Lo 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.

5. ANEXOS

Anexo 1. Auditoria de adherencia en seguridad de la información

HOSPITAL UNIVERSITARIO HERNANDO MONCALEANO PERDOMO Empresa Social del Estado	**FORMATO**	META ACREDITACIÓN FECHA DE EMISIÓN: JUNIO 2018
	AUDITORIA DE ADHERENCIA EN SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 01 CÓDIGO:GI-SI-F-001B PÁGINA 1 DE 1

DESCRIPCIÓN

Unidad funcional — Fecha inspección

Nombre quien inspecciona — Cargo

CRITERIOS A AUDITAR	SI	NO	N.A	HALLAZGOS
El usuario tiene conocimiento del contenido del manual de seguridad de la información y de su ubicación para su consulta				
El usuario tiene claro cuales son los niveles de clasificación de la información definidos en el manual de seguridad de la información (3.1.2) * La historia clinica es catalogada como información pública, de uso interno, confidencial o restringida				
El usuario conoce la politica de uso y gestión de correo electrónico institucional (responsabilidades de tratamiento de datos, acceso y condiciones) (3.1.20)				
El usuario tiene claridad sobre qué área debe autorizar el traslado de equipos informáticos entre dependencias (3.1.18)				
El usuario tiene conocimiento de los protocolos de publicación y tratamiento de la información en la pagina WEB institucional (3.1.5)				
El usuario tiene claridad sobre la responsabilidad de los activos de información utilizados diariamente (3.1.9) * Conoce quien es el propietario del activo de información usado a diario				
El usuario tiene claridad sobre la periodicidad de cambio de la contraseña de correo electrónico y/o sistemas y aplicativos (3.1.20)				
Se observa que la informacion critica de la entidad esta siendo respaldada mediante copias de seguridad con el fin de asegurar la continuidad del negocio (3.1.8)				
Se evidencia la utilización de activos de información (hardware y software) solo para fines laborales (3.1.3 - 3.1.10)				
Se evidencia el cumplimiento de la politica de uso de estaciones cliente en cuanto a la prohibición de almacenar y reproducir fotografías, musica, videos o instalación de software no autorizados por el HUN (3.1.11)				
Se evidencia el cumplimiento de la directriz de no tener ni consumir cerca de los equipos de cómputo liquidos o alimentos que puedan ocasionar daño de los mismos (3.1.11)				
Se evidencia que la pantalla del computador es bloqueada por el usuario al momento de retirarse del puesto de trabajo (3.1.19)				
Se evidencia el ingreso a sitios WEB con contenidos contrarios a los establecidos por el hospital (twitter, facebook, youtube, entre otros) (3.1.12)				
Se evidencia al personal destapando cualquier equipo de cómputo o impresoras (3.1.15)				
Se evidencia equipos portátiles personales, celulares inteligentes, agendas electrónicas, entre otros; conectados a puntos de red de datos o de energia regulada				
Se evidencia en el escritorio y la pantalla de escritorio del computador información confidencial visible expuesta a ser copiada o hurtada (3.1.19)				
Se evidencia la conexión de dispositivos móviles extraibles (memorias USB, discos duros, entre otros) en los equipos de cómputo del hospital				

6. CONTROL DE RESPONSABILIDADES

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Ormalia Vargas Montero	**NOMBRE:** Alejandro Polania Cárdenas	**NOMBRE:** Emma Constanza Sastoque Meñaca
CARGO: Jefe Oficina Asesora Sistemas de Información Hospitalaria.	**CARGO:** Jefe Oficina de Oficina de Planeación, Calidad y Desarrollo Institucional (E)	**CARGO:** Gerente E.S.E.
FECHA: Diciembre 2020	**FECHA:** Diciembre 2020	**FECHA:** Diciembre 2020

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
01	Abril 2016	Emisión del documento.
02	Julio 2018	Se adicionaron o modificaron las siguientes Políticas para dispositivos móviles, Política de escritorio, pantalla limpia y de equipos desatendidos, Política de control de acceso a sistemas y aplicativos, Política para dispositivos móviles, Política de transferencia de información, Política para revisión de los derechos de acceso a usuarios, Política para disposición final de medios cuando no se requieran, Política de devolución de activos, Política de seguridad para relación con proveedores, Política para la gestión de proyectos, Política para desarrollo externo de software, Política para seguridad de equipos y activos fuera de las instalaciones, Política para seguridad de oficinas, recintos e instalaciones, Política de tratamiento y protección de datos personales.
03	Agosto 2019	Se adicionaron o modificaron las siguientes Políticas de no repudio, Política de disponibilidad de servicios digitales y de la información y Política de registro y auditoría, además se incrementó en el ítem Autoridades y datos de contacto en cuanto a los buzones y a la cuenta de correo de seguridaddigital@huhmp.gov.co

04	Diciembre 2020	Se realizó ajuste a la Política de seguridad de la información contenida en el MSI (3.1.1). Se realizan ajustes a las directrices de la Política de Clasificación de la información (3.1.2 del MSI) y se ajustó el nombre de la política de la siguiente manera: Política de Clasificación y etiquetado de la Información. Se hicieron ajustes y se adicionaron directrices a la política de seguridad para los usuarios de los activos de información (3.1.3) Se adicionan directrices a las siguientes políticas; política específica para Webmaster (3.1.5 del MSI); política de gestión de activos de información (3.1.9); política para mensajería instantánea y redes sociales (3.1.13 del MSI); política de correo electrónico (3.1.20 del MSI). Se realizó ajuste al objetivo y adición de las directrices de la Política para seguridad de oficinas, recintos e instalaciones (3.1.32 del MSI). Se adicionaron compromiso de la dirección, del manual 3.2.1 que corresponde a los compromisos de la dirección. Se relacionan los datos de la autoridad de contacto Grupo de respuesta a emergencias cibernéticas de Colombia (COLCERT) En el espacio de evaluación, se relaciona el curso de seguridad de la información.