RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

La Gerente del Hospital Departamental Psiquiátrico Universitario del Valle E.S.E. en uso de sus atribuciones legales, y

CONSIDERANDO

Que la constitución Política de Colombia en su Artículo 15 señala que "*Todas las personas tiene derecho a su intimidad personal y familiar y a su buen nombre, y el estado debe respetarlos y hacerlos respetar. De igual modo, tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en banco de datos y en archivos de entidades públicas y privadas*".

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

Que la Ley 1273 de 2009, modificó el Código Penal, creando un nuevo bien jurídico tutelado denominado "*de la protección de la información y de los datos*" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Que la Ley 1341 de 2009 definió los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC.

Que la anterior disposición, fue reglamentada por el Decreto 2573 de 2014, mismo que estableció los lineamientos generales de la Estrategia de Gobierno en línea y definió el alcance y participación de las tecnologías de la información en la gestión de datos públicos e interacción con la comunidad.

Que la Ley 1581 de 2012 estableció el Régimen de Protección de Datos Personales y determinó como deberes de los Responsables del Tratamiento, la adopción de un manual interno de políticas y procedimientos para garantizar el adecuado tratamiento de datos personales y de atención a consultas y reclamos, entre otros.

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

Que la Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, promueve la gestión pública de la información institucional.

Que el Decreto 2609 de 2012, reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Que la NORMA TECNICA NTC-ISO/IEC colombiana 27001, establece criterios y requisitos sobre las Tecnologías de la información, técnicas de seguridad y sistemas de gestión de la seguridad de la información.

Que a través del Decreto Único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

Que MinTIC recopiló en el Modelo de Seguridad y Privacidad de la Información, las mejores prácticas nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea - GEL.

Que el Modelo de Seguridad y Privacidad de la Información - MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

los datos mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca, de la adecuada gestión de riesgos.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC definió guías que apoyan la adopción de la Política General de Seguridad de la Información y otros instrumentos del Modelo de Seguridad y Privacidad de la Información.

Que el Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Que por medio de la Resolución 587 de 30 noviembre del 2020 se adoptó la política de seguridad de la información y uso de los recursos informáticos del Hospital Departamental Psiquiátrico Universitario del Valle E.S.E", y que en sesión realizada el 17 de noviembre del 2022 el Comité Institucional de Gestión y Desempeño aprobó la actualización de la política basado en la guía 5482-G8 Controles de seguridad de Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC y la norma NTCISO27002 en el numeral A 5.1.2 revisión para las políticas de la seguridad de la información.

Que el Hospital Departamental Psiquiátrico Universitario del Valle E.S.E. reconoce la importancia estratégica de la información y los sistemas de información por lo cual es importante generar estrategias que nos permitan garantizar la confidencialidad, disponibilidad e integridad de la información, como herramienta que aporte a la prestación de servicios de manera segura y confiable.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO: Actualizar la POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y USO DE LOS RECURSOS INFORMÁTICOS del Hospital Departamental Psiquiátrico Universitario del Valle E.S.E., en los términos que a continuación se describen:

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y USO DE LOS RECURSOS INFORMÁTICOS

Todo el personal del Hospital se compromete a: Gestionar la seguridad de la información mediante la generación de una Cultura de Seguridad de la información y autocontrol informático y la formulación de estrategias que permitan gestionar los riesgos para garantizar la confidencialidad, disponibilidad e integridad de la información, como herramienta que aporte a la prestación de servicios de manera segura y confiable.

DEFINICIONES

De conformidad con la legislación vigente sobre la materia, entiéndase por:

a) Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de sus datos personales.
b) Aviso de privacidad: Comunicación verbal o escrita, generada por el HDPUV ESE, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
c) Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento y que estén bajo la responsabilidad del HDPUV E.S.E.
d) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
e) Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

f) Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
g) Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, pública ni sensible y cuyo conocimiento o divulgación puede interesar no sólo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general, como el correo electrónico de una persona.
h) Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad de titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, o que promueva intereses de cualquier partido político; o que garanticen los derechos y garantías de partidos políticos de oposición, así como 'los datos relativos a la salud, a la vida sexual y los datos biométricos.
i) Responsable del tratamiento: Persona natural o jurídica, pública o privada que, por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
j) Titular: Persona natural cuyos datos personales sean objeto de tratamiento.
k) Tratamiento: Cualquier operación o conjunto de oraciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
l) Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o los encargados del tratamiento de datos personales, Ubicado en Colombia, envían la información o los datos personales a un receptor que se encuentra dentro o fuera del país y que a su vez es responsable del tratamiento.
m) Activos De Información: Recursos del sistema de información o relacionados con éste, necesarios para que la Entidad funcione correctamente y alcance los objetivos propuestos por su dirección.
n) Cifrado: Es el proceso que se aplica a unos datos para hacerlos incomprensibles. Este proceso o transformación precisa de una clave de cifrado, que es una cadena aleatoria de

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

bits, de una medida determinada (como, se denomina, de una determinada longitud de clave). Sólo aplicando el proceso contrario, denominado descifrado, a los datos cifrados será posible regenerar los datos originales y, por tanto, hacerlas otra vez comprensibles.

o) Clasificación De La Información: Es la decisión para asignar un nivel de sensibilidad a los datos cuando se están creando, corrigiendo, almacenando o transmitiendo. Un esquema de clasificación debe usarse para definir un conjunto apropiado de niveles de protección y comunicar las medidas especiales de tratamiento.

p) Controles: Medidas para garantizar que los riesgos sean reducidos a un nivel aceptable.

q) Dueño De La Información: Es responsable de la información que le sea asignada, así como de la clasificación, control y monitoreo del uso y gestión de la misma. Son Dueños de Información todas aquellas personas del HDPUV que tienen bajo su responsabilidad parte o la totalidad de la información. Los responsables de la información son encargados de preservar los principios de seguridad de la información (integridad, disponibilidad y confidencialidad) y deben coordinar la implementación de políticas con otros dueños de información y con custodios de la información. Los Dueños deben especificar cómo se debe utilizar la información y cómo se debe proteger, además de definir cómo se administrarán los procedimientos de seguridad de la información y cómo se aplicarán los niveles apropiados de protección para cada una de las clases de información (pública, privada y confidencial).

r) Impacto: Daño producido a la Entidad por un posible incidente o evento, y resultado de la agresión sobre un activo, visto como diferencia en las estimaciones de los estados de seguridad y operación, obtenidas antes y después del evento.

s) Incidente: Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos, inesperados o no deseados, de seguridad de la información que tienen una probabilidad significativa de poner en peligro las operaciones y procesos de la Entidad y amenazar la seguridad de la información. Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, sistemas de información, procesos de la Entidad o recursos tecnológicos del HDPUV.

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

t) Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.
u) Infraestructura Tecnológica: Todos los componentes tecnológicos que están al servicio de la entidad.
v) Infraestructura: La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.
w) ISO 27001: Código de práctica para la administración de la seguridad de la información de la Organización Internacional para la Estandarización (ISO).
x) Monitoreo: Es aquella actividad que pretende hacer seguimiento periódico y revisión de ciertas tareas realizadas en los sistemas de información.
y) Norma: Guía general de Seguridad de la Información sobre un tema específico, pero independiente de la plataforma tecnológica. La norma está sustentada en una política y regula parte o la totalidad del objetivo de la misma.
z) Oficial De Seguridad De La Información: Es el responsable de implementar la estrategia de seguridad de la información alineada con los objetivos de la Entidad, dirigir el programa de seguridad de la información y tomar las decisiones que permitan gestionar la seguridad de la información en el marco de control y cumplimiento definido y aprobado por la Entidad.
aa) Proceso: Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.
bb) Riesgo: Es la probabilidad de que una amenaza se concrete sobre uno o más activos causando daños o perjuicios a la Organización por medio de una vulnerabilidad o punto débil.
cc) Rol/Perfil: Conjunto de funciones, normas, comportamientos y derechos definidos en un sistema de información que se espera que un usuario cumpla o ejerza de acuerdo a su nivel adquirido o atribuido en HDPUV.
dd) Seguridad De La Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información; otras características también pueden estar involucradas, tales como la autenticidad, responsabilidad, aceptabilidad y confiabilidad.

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

ee) Sistema De Información: Conjunto de programas o aplicaciones desarrollados en diferentes lenguajes de programación, que facilitan el manejo de la información generada por los diferentes procesos de la Entidad.
ff) Ti: Tecnología de información.
gg) Practicante: Personal que desempeña labores en la empresa bajo contrato de aprendizaje SENA, pasante o practicante universitario y estudiantes de colegio realizando su servicio social obligatorio.
hh) Temporal: Personal contratado por una cooperativa de trabajo asociado trabajando en misión del HDPUV.

OBJETIVOS

Objetivo general.

Establecer los lineamientos definidos y aprobados por la alta dirección del Hospital para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, los demás requisitos de ley y las necesidades de las partes interesadas, en pro de mantener vigentes la disponibilidad, integridad y confidencialidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizada, daño, pérdida u otros factores disfuncionales, igualmente el uso adecuado y responsable de todos los recursos informáticos.

Objetivos específicos.

- Brindar orientación y apoyo por parte de la dirección para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
- Proteger la información contra cualquier forma de acceso no autorizado, robo, utilización indebida, copia, publicación o modificación accidental con el fin de garantizar su confidencialidad, integridad y disponibilidad.

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

- Dar cumplimiento a las normas, políticas, procedimientos y medidas preventivas de seguridad definidas para el manejo de equipos de cómputo e información sistematizada.
- Tener claridad sobre la responsabilidad que cada funcionario tiene en relación con el manejo de información y equipos de cómputo.
- Optimizar el manejo de los recursos informáticos minimizando el riesgo por pérdida de información o deterioro de los equipos.
- Desarrollar la cultura de autocontrol Informático en todos y cada uno de los funcionarios de la Hospital.
- Identificar y gestionar los riesgos de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y todas las partes interesadas en el Hospital
- Minimizar el riesgo tecnológico de todos los procesos del Hospital
- Implementar los controles tecnológicos necesarios para la protección de los activos de información del Hospital.

ALCANCE

Esta política rige para todos los funcionarios, estudiantes en práctica formativa y contratistas del Hospital Departamental Psiquiátrico Universitario del Valle ESE, que crea, almacena, procesa, trasmite, elimina información, y utiliza recursos informáticos para el desempeño de su función o labor encomendada. Esta política tiene como propósito reducir el impacto frente a la perdida de información y/o incidentes que comprometan la continuidad de las funciones misionales del Hospital.

RESPONSABILIDADES

La Alta Dirección: se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación de SGSI de manera periódica y también

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

garantizara los recursos suficientes (económicos, tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

Comité de desempeño institucional: asume las funciones del derogado comité de gobierno en línea, y sus principales funciones son:

- Aprobar los lineamientos y estrategias para la implementación de estrategias de seguridad de la información y gobierno digital.
- Asegurar los recursos y toma de decisiones para las estrategias definidas.
- Supervisar y verificar el grado de implementación de las estrategias.

Profesional universitario en sistemas: sus principales funciones son:

- Implementar las estrategias de seguridad de la información y gobierno digital.
- Realizar seguimiento a los planes y estrategias definidas.
- Evaluar, diseñar y coordinar la implantación de los controles administrativos, técnicos y operativos que garanticen un alto nivel de seguridad de la Información que permitan a la organización el normal y eficiente desarrollo de los procesos con información confiable, íntegra, veraz, oportuna y con eficiencia operativa.

Líderes de proceso: sus principales funciones son:

- Tienen la responsabilidad de dar cobertura de los lineamientos de seguridad en los procesos que están a su cargo.

Funcionarios, estudiantes en práctica formativa y contratistas: sus principales funciones son:

RESOLUCIÓN 507
(03 de noviembre del 2022)
"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E."

- Cumplir con todos los lineamientos establecidos en la política de seguridad de la información en todas las actividades que realicen en su función dentro del Hospital

IMPLEMENTACIÓN

El despliegue e implementación de la presente política se realizará a través de los siguientes documentos, los cuales forman parte integral de la misma:

- Manual de seguridad de la información y uso de recursos informáticos.
- Procedimiento de gestión de incidentes de seguridad de la información.
- Acuerdo de confidencialidad.

ARTÍCULO SEGUNDO. - DIVULGACIÓN. Ordénese la publicación y divulgación de la presente política a través de la Profesional de Comunicaciones en los canales internos y externos institucionales.

ARTÍCULO TERCERO. - VIGENCIA Y DEROGATORIAS: la presente resolución rige a partir de su expedición y deroga las disposiciones que le sean contrarias, especialmente la Resolución 587 del 30 de noviembre del 2020.

PUBLÍQUESE Y CÚMPLASE

MARIA FERNANDA BURGOS CASTILLO
Gerente

Proyectó: Marcela Martínez Turriago, Profesional Universitario Sistemas
Revisó: Magali Ramos Calderón, Jefe Oficina Asesora de Jurídica

MANUAL DE SEGURIDAD DE LA INFORMACIÓN Y USO DE LOS RECURSOS INFORMATICOS

MAN-GIN-01

1. OBJETIVO

Establecer los lineamientos definidos y aprobados por la alta dirección del Hospital para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, los demás requisitos de ley y las necesidades de las partes interesadas, en pro de mantener vigentes la disponibilidad, integridad y confidencialidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizada, daño, pérdida u otros factores disfuncionales, igualmente el uso adecuado y responsable de todos los recursos informáticos.

2. OBJETIVOS ESPECIFICOS

- Brindar orientación y apoyo por parte de la dirección para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
- Proteger la información contra cualquier forma de acceso no autorizado, robo, utilización, indebida, copia, publicación o modificación accidental con el fin de garantizar su confidencialidad, integridad y disponibilidad.
- Dar cumplimiento a las normas, políticas, procedimientos y medidas preventivas de seguridad definidas para el manejo de equipos de cómputo e información sistematizada.
- Tener claridad sobre la responsabilidad que cada funcionario tiene en relación con el manejo de información y equipos de cómputo.
- Optimizar el manejo de los recursos informáticos minimizando el riesgo por pérdida de información o deterioro de los equipos.
- Desarrollar la cultura de autocontrol Informático en todos y cada uno de los funcionarios de la Hospital.
- Identificar y gestionar los riesgos de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y todas las partes interesadas en el Hospital
- Minimizar el riesgo tecnológico de todos los procesos del Hospital
- Implementar los controles tecnológicos necesarios para la protección de los activos de información del Hospital.

3. ALCANCE

Este manual rige para todos los funcionarios, estudiantes en práctica formativa y contratistas del Hospital Departamental Psiquiátrico Universitario del Valle ESE, que crea, almacena, procesa, trasmite, consulta y elimina información, y utiliza recursos informáticos para el desempeño de su función o labor encomendada.

4. MARCO LEGAL

Ley Estatutaria 1581 de 2012: y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones

Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones

Decreto 728 de 5 de mayo de 2017: Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.

Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. "Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones
Numerales 4, 5, 21 y 22 del artículo 34 de la a Ley 734 de 2002 que establecen:
Deberes del servidor Público:
4- utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos
5- custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la que tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
21- vigilar y salvaguardar los bienes y valores que han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados.
22- responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.

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

5. RESPONSABLES

La seguridad de la información debe ser una responsabilidad del Hospital Departamental Psiquiátrico Universitario del Valle ESE, incluyendo todos sus colaboradores entre ellos se encuentran:

La Alta Dirección: se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación de SGSI de manera periódica y también garantizara los recursos suficientes (económicos, tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

Comité de desempeño institucional: aprobado por la resolución 115 de febrero de 2018, por medio de la cual se actualiza el modelo integrado de planeación y gestión y se crea el comité institucional de gestión y desempeño del Hospital Departamental Psiquiátrico Universitario del Valle ESE, el cual asume las funciones del derogado comité de gobierno en línea, y sus principales funciones son:

- Aprobar los lineamientos y estrategias para la implementación de estrategias de seguridad de la información y gobierno digital.
- Asegurar los recursos y toma de decisiones para las estrategias definidas.
- Supervisar y verificar el grado de implementación de las estrategias

Profesional universitario en sistemas: sus principales funciones son:

- Implementar las estrategias de seguridad de la información y gobiemo digital.
- Realizar seguimiento a los planes y estrategias definidas.
- Evaluar, diseñar y coordinar la implantación de los controles administrativos, técnicos y operativos que garanticen un alto nivel de seguridad de la Información que permitan a la organización el normal y eficiente desarrollo de los procesos con información confiable, íntegra, veraz, oportuna y con eficiencia operativa.

Líderes de proceso: sus principales funciones son:

- Tienen la responsabilidad de dar cobertura de los lineamientos de seguridad en los procesos que están a su cargo.
- Funcionarios, estudiantes en práctica formativa y contratistas: sus principales funciones son:
- Cumplir con todos los lineamientos establecidos en la política de seguridad de la información en todas las actividades que realicen en su función dentro del Hospital.

Los **funcionarios, estudiantes en prácticas formativas y contratistas**: deben cumplir con todos los lineamientos establecidos en la política y manual de seguridad de la información y uso de los recursos informáticos en todas las actividades que realicen en su función dentro del hospital.

6. DEFINICIONES

Información: Se refiere a toda comunicación o representación de conocimiento con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, la cual puede estar digital, audiovisual, impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: Se refiere al hardware y software operado por la Entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la misma, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan los servicios informáticos.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son Funcionarios de la Entidad, pero que por las actividades que realizan en la misma, deban tener acceso a Recursos Informáticos.

Ataque cibernético: Intento de penetración a un sistema informático por parte de un usuario no deseado, ni autorizado a accederlo, por lo general con intenciones insanas, perjudiciales o dañinas.

Evaluación de Riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones.

Administración de Riesgos: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Responsable de Seguridad Informática: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los usuarios de la Entidad, que lo requieran.

Incidente de Seguridad: Un incidente de seguridad es un evento adverso en un sistema o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, accesibilidad legalidad y confiabilidad de la información puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Información Pública: Información de dominio general, a la cual puede tener acceso cualquier persona.

Información Privada: Información para uso interno solamente; solo los funcionarios de la Entidad que intervienen en un proceso y/o trámite o los que pertenecen al área de competencia de dicho trámite pueden conocerla.

Confidencial: Información de uso exclusivo de un funcionario o grupo de funcionarios de la Entidad, que en caso de ser divulgada sin autorización afecta negativamente los intereses y deberes de la misma. Esta información requiere controles restrictivos y especial cuidado en el acceso, tránsito y almacenamiento.

Reservada: Es aquella que por disposición legal expresa tiene reserva, sólo tienen acceso directo ciertas personas (sujetos calificados), en razón de su profesión u oficio.

Confidencialidad: El HDPUV establece para la información no autorizada o confidencial, la determinación de su no divulgación correspondiente.

Integridad: El HDPUV procura que la información que circula y salvaguarda en la Entidad sea precisa, coherente y completa desde su creación hasta su destrucción o eliminación.

Disponibilidad: El HDPUV determina la disponibilidad de la información en el momento que es solicitada, para el correcto funcionamiento de los procesos, para fundamentar decisiones gerenciales o requerimientos.

Accesibilidad: El HDPUV determina el acceso a la información con las limitaciones legales y establece el grado en el que los funcionarios y usuarios pueden utilizar los activos de la información de forma satisfactoria.

7. DESCRIPCION

POLÍTICAS O NORMAS DE SEGURIDAD DE LA INFORMACIÓN DEL HOSPITAL [A.5 - NTC-ISO-IEC 27001 2013]

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra organización. Sin ellos nos quedamos rápidamente fuera de la Entidad y por tal razón los miembros de la Alta Dirección, tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales, garantizar la no obsolescencia de la Tecnología (software, hardware y redes).

Los distintos líderes de proceso, están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. En todo caso, cada año el Comité de Desempeño llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará al final de cada año un informe para la Gerencia y la Alta Dirección, que muestre el estado actual de la Entidad en cuanto a Seguridad de la información.

A todos los empleados, consultores y contratistas debe proporcionárseles capacitación, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Entidad. Debe hacerse hincapié en que la seguridad de la información es una actividad tan vital para la Entidad como lo son otros procesos como los financieros, contables o de nómina.

1.1. Políticas Específicas del Sistema de Gestión de Seguridad de la Información

- El Sistema de Gestión de Seguridad de la Información del Hospital se implementa dentro del marco de la norma NTC ISO/IEC 27001 - 2013 o sus versiones posteriores.
- El presente documento, así como todas las políticas y procedimientos de seguridad de la información que se deriven del SGSI deben ser comunicadas a todos los funcionarios del Hospital.

1.2. Revisión de la Política de Seguridad

El Oficial de seguridad de la Información o quien ejerza sus funciones es responsable por la actualización permanente del documento de Políticas de Seguridad de la Información del Hospital, los principios rectores, políticas específicas, procedimientos,

estándares y guías de uso. La actualización debe ser (mandataria) en la medida en que ocurra alguno (o varios) de los siguientes eventos:

a) Cambios en el ambiente de negocios o estrategia organizacional (ejemplo: nuevas estrategias de mercado, nuevos servicios, cambios de prioridades, fusiones o cesiones, cambios en la estructura organizacional, nuevas gerencias, etc.)
b) Cambios en la infraestructura de riesgos de seguridad de información de la entidad. Estos cambios pueden ser como consecuencia de un análisis de riesgos y vulnerabilidades o por aparición de nuevas vulnerabilidades y/o amenazas que cambien el perfil de riesgo de la infraestructura técnica de la Organización.
c) Nuevas obligaciones legales y/o reglamentarias o cambio de las existentes que afecten el procesamiento de la información, intercambio de información con terceros, etc.
d) Avances en las mejores prácticas de seguridad de la Información registradas en el código de prácticas ISO/IEC 27002:2013 o cambios en la norma ISO/IEC 27001:2013, o las que apliquen en su momento y que previamente evaluadas sean necesarias para la organización.
e) Aplicación de nuevos controles identificados como resultado de los análisis de los incidentes de seguridad de la información o el resultado de auditorías de IT.

Es responsabilidad del Oficial de Seguridad de la Información o quien ejerza sus funciones informar a la Entidad y terceros la actualización y publicación de nuevas versiones de este documento.

ORGANIZACIÓN DE SEGURIDAD [A.6 - NTC-ISO-IEC 27001 2013]

La Gerencia del Hospital, se encargará de dar una dirección estratégica al sistema de Gestión de Seguridad de la Información acorde con los lineamientos de la entidad y aprobará los principios rectores, políticas específicas y procedimientos que hacen parte de este documento, pero delega las responsabilidades de gestión y mejora continua de la Seguridad de la Información al Comité de Gestión y Desempeño Institucional, el cual estará conformado por los siguientes integrantes:

a. Gerente del Hospital o delegado
b. Jefe de Oficina Asesora de Planeación o quien haga sus veces
c. Jefe de la Oficina Jurídica o quien haga sus veces
d. Líder del Programa de Gestión de Talento Humano o quien haga sus veces
e. Líder del Programa de Intervención Social y Comunitaria o quien haga sus veces
f. Profesional Universitario de Sistemas
g. Profesional encargado el proceso de SIAU
h. Técnico Administrativo de Gestión Documental
i. Asesor de Control Interno (como invitado permanente con voz, pero sin voto)
j. Los otros cargos en calidad de invitados con voz, pero sin voto.

La Gerencia revisará periódicamente las actas e informes del Comité de Gestión y Desempeño Institucional y coordinará las actividades relacionadas con la administración y operación del Sistema de Gestión de Seguridad de la Información.

Otras responsabilidades del Comité de Gestión y Desempeño Institucional (frente a la seguridad de la información) son:

a) Revisar y aprobar la Política de Seguridad de la Información del Hospital, los principios rectores, políticas especificas, procedimientos, estándares y guías de uso de los temas relacionados a seguridad informática.
b) Evaluar, revisar, aprobar e implementar los controles de seguridad de la información.
c) Identificar las tendencias y los cambios importantes de los riesgos de seguridad informática de la Organización y proponer los cambios de políticas y procedimientos adecuados con el fin de controlar las vulnerabilidades identificadas.
d) Asegurar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios.
e) Establecer mecanismos de control que permitan medir el cumplimiento de las Políticas y Procedimientos de Seguridad de la Información.
f) Recomendar acciones correctivas a los incidentes de seguridad reportados.
g) Hacer seguimiento a los incidentes de seguridad reportados.
h) Establecer mecanismos de control de la información confidencial de la Entidad
i) Gestionar las sanciones aplicables por incumplimiento a las Políticas de Seguridad de la Información, principios rectores, políticas específicas, procedimientos, estándares y guías de uso de los temas relacionados a seguridad informática.
j) Coordinar revisiones periódicas al Sistema de Gestión de Seguridad de Información, realizadas por consultores externos o internos, cuando el nivel de experiencia y capacitación lo permita
k) Realizar reportes periódicos a la Gerencia de la Entidad indicando el nivel de seguridad obtenido mediante la ejecución de los controles del Sistema de Gestión de Seguridad de Información.
l) Desarrollar programas de concientización y capacitación a todos los funcionarios que enfaticen la importancia del cumplimiento del Sistema de Gestión de Seguridad de la información y su contribución al logro de los objetivos de la Entidad.
m) El comité realizará sus reuniones en el evento en que ocurra uno (o varios) de los siguientes eventos:
    - Ocurrencia de un incidente de seguridad que requiera una sesión especial del comité
    - Ocurrencia de un evento por el cual sea necesaria la declaración de contingencia técnica y/u operativa.

DISPOSITIVOS MOVILES Y TELETRABAJO [ISO/IEC 27002:2015 A.6.2]

Computación móvil: [ISO/IEC 27002:2015 A.6.2.1] Se desarrollaran procedimiento adecuados para estos dispositivos, que abarquen la protección física necesaria, el acceso seguro a los dispositivos, la utilización de los dispositivos en lugares públicos, el acceso a los sistemas de información y servicios del Hospital a través de dichos dispositivos, las técnicas criptográficas a utilizar para la transmisión de información clasificada, los mecanismos de resguardo de la información contenida en los dispositivos y la protección contra software malicioso.

Trabajo remoto: [ISO/IEC 27002:2015 A.6.2.2] El trabajo remoto solo será autorizado por el jefe de área, a la cual pertenezca el usuario solicitante, conjuntamente con el responsable de seguridad informática, cuando se verifique que son adoptadas todas las medidas que corresponde en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Como quiera que del HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E tiene las aplicaciones CORE de su negocio locales; es muy importante para la seguridad de la labor de los colaboradores del hospital que se tengan en cuenta medidas mínimas de seguridad de la información, para asi cumplir con el objetivo de mantener disponibilidad, confidencialidad e integridad de la información de la entidad.

En los casos que se requiera que un funcionario este en modo trabajo remoto es importante que éste trabaje con el equipo local y activo de la compañía y solo en casos especiales sea aprobado trabajar con equipos que no son de la compañía siendo un requisito que estos cumplan con las medidas de seguridad mínimas que esta política contempla.

Para que un funcionario este en modo trabajo remoto es un requisito que se tengan las mínimas medidas de seguridad para estar protegido frente a las principales amenazas de Internet, estas son:

- Disponer de un antivirus licenciado y actualizado.
- Utilizar un equipo con sistema operativo legal licenciado y actualizado

Para prácticamente cualquier otro tipo de conexión que requiera acceso a la red interna de la organización, lo más importante es activar una conexión VPN, con un usuario y clave válida dentro de la red de la compañía, horarios de uso, así como contar con los permisos respectivos de su jefe o director de área.

Para casos especiales cuando el colaborador no puede usar un equipo de la compañía, éste permiso deberá ser avalado por un directivo de la misma y este colaborador deberá firmar un documento de responsabilidad para el cumplimiento de la política en cuanto a que el equipo a usar no debe ni puede tener menos de las medidas de seguridad descritas en esta política y que la responsabilidad de los eventos de seguridad que pasen en la infraestructura por el incumplimiento de la misma será su responsabilidad. Para la activación de la VPN el jefe inmediato enviara a través de correo o impreso el formato activar e inactivar usuarios (FOR-GIN-42).

SEGURIDAD DEL PERSONAL [A.7 - NTC-ISO-IEC 27001 2013]

Cumplimiento del Sistema de Gestión de Seguridad de la Información

- Es obligación de los usuarios, sin excepción alguna, conocer, respetar, cumplir y hacer cumplir las políticas de seguridad de la información del Hospital.
- La responsabilidad de seguridad es parte de los términos y condiciones del empleo. La violación o no cumplimiento de cualquiera de las directrices documentadas en las políticas de seguridad de la información establecidas por Hospital, serán argumentos para la aplicación de acciones disciplinarias.

Acuerdos de Confidencialidad

- Todos los empleados, sin importar el tipo de contrato, ya sea a término fijo o indefinido, deben firmar un acuerdo de confidencialidad en el momento en que ingresan al Hospital.
- Todo el personal vinculado con el Hospital como contratista, trabajador en misión, contrato de aprendizaje, practicante, etc., también debe firmar un acuerdo de confidencialidad en el momento del inicio de sus labores en Hospital.

Procesos Disciplinarios

El funcionario que viole las políticas de seguridad de la información, de manera consciente o deliberada, será requerido por su Jefe inmediato sin perjuicio del proceso disciplinario a que haya lugar, es decir, se remitirá el informe respectivo con las evidencias existentes a la Oficina de Control Disciplinario para lo de su competencia.

Es deber del funcionario como servidor público, informar a su Jefe inmediato o en su defecto, a la Oficina de Control Disciplinario, de cualquier anomalía o irregularidad que tenga conocimiento sin necesidad de agotar un conducto regular.

Conocimiento, educación y Entrenamiento de seguridad de la información

a) La oficina de Talento Humano con asesoría del área de sistemas de información, deben desarrollar estrategias de sensibilización, entrenamiento y educación en seguridad de la información, para promover conocimiento constante a todos los empleados, temporales, contratistas y practicantes. La estrategia de sensibilización de seguridad debe consistir en entrenamiento y resúmenes impresos constantes.
b) Todo el personal debe participar en las sesiones de concientización frente a temas de seguridad de la información. Un resumen impreso de las medidas de seguridad básicas de la información se debe proporcionar a cada empleado, temporal, contratista o practicante y guardar una copia firmada en archivo.

Terminación o Cambio de Empleo de los Funcionarios

a) El personal que se retira del Hospital debe recibir por parte del Jefe de Área un recordatorio acerca de los compromisos legales y éticos adquiridos con respecto a mantener la confidencialidad de la información a la cual tuvo acceso en el curso de su empleo.
b) Consideraciones similares deben ser aplicadas cuando un funcionario del Hospital cambie de funciones en una misma área o en áreas diferentes. En este caso, los líderes involucrados en la transferencia del personal, deben tramitar que el acceso a la información confidencial de las áreas involucradas esté protegido de accesos o modificaciones no autorizadas.
c) Todo el personal, sin importar el tipo de vinculación laboral, que se retire del Hospital, debe entregar al jefe de área y/o a quien ejerza las funciones de coordinación del área de Sistemas de Información los activos informáticos asignados para su cargo (incluyendo documentos, archivos digitalizados, computadores, información de Pacientes, proveedores o terceros de la entidad, almacenada en teléfonos móviles o computadores de mano, dispositivos de almacenamiento USB, etc.).
d) Cada Jefe de proceso y/o área talento humano debe informar las novedades (ingresos, retiros, reemplazos, traslados, vacaciones, etc.) de las personas a su cargo al Profesional Universitario solicitando la asignación, modificación o desactivación de los permisos y perfiles de cada usuario, según sea el caso por los medios de comunicación oficiales que están a disposición de los funcionarios desde el área de sistemas de información, atreves del FOR-GIN-42.
e) El acceso a la información, computadores, redes de datos e instalaciones físicas, deben ser revocadas de inmediato cuando un funcionario o un tercero se retira del Hospital.

Investigación de Empleados

La oficina de Talento Humano debe realizar una investigación a todo candidato potencial que pueda llegar a ser empleado del Hospital. Esto puede incluir pruebas psicológicas, referencias personales y laborales, verificación de la educación, entre otros. Si el empleado se está buscando a través de terceros o una agencia apropiada, debe seguirse como mínimo los mismos análisis definidos para la investigación los cuales deben ser llevados a cabo por la agencia.

Los empleados contratados para cargos en los cuales deban tener acceso a información confidencial de la Entidad deben tener investigación adicional de acuerdo con las necesidades definidas en las leyes o regulaciones.

GESTIÓN Y ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN [A.8 - NTC-ISO-IEC 27001 2013]

Responsabilidad de los Activos de Información

a) Los propietarios o responsables de los activos de información deben ser claramente designados por la Gerencia del Hospital o los líderes respectivos de cada área. Los propietarios serán los responsables de la protección de los activos de información contra incidentes de seguridad.
b) Los propietarios de los activos de información, son responsables por la clasificación de sus activos y la definición y auditoria constante de las restricciones de acceso y otros controles de seguridad de la información

Inventario de los Activos de Información

Los responsables de los activos de información deben realizar un inventario de los datos o información almacenados en las estaciones de trabajo y bases de datos de los servidores, así como de los documentos en medio físico necesarios para el desarrollo de las actividades.

Los datos mínimos que debe contener el inventario de los datos (físicos y magnéticos) son:

- Nombre del archivo o documento
- Ubicación (carpeta física o lógica)
- Responsable
- Custodio
- Clasificación de la información de acuerdo a los criterios de esta política.
- Existencia de alguna copia.
- Identificar quien o quienes tienen acceso a la información

El inventario de los datos (activos de información) debe ser actualizado en la medida en que ocurra uno o varios de los siguientes casos:

- Cambios en el ambiente de negocios o estrategia organizacional.
- Nuevas obligaciones legales o reglamentarias.
- Pasado un año después de la última actualización del inventario.

Quien ejerza las funciones de líder y/o coordinación del área de sistemas de información debe realizar el inventario de los aplicativos y programas bajo licencia con que cuenta la organización. Los datos que debe incluir el inventario son:

- Nombre del aplicativo o software
- Versión
- Número de licencias adquiridas por la Organización
- Número de licencias instaladas

Quien ejerza las funciones de líder y/o coordinación del área de sistemas de información debe realizar el inventario de los activos de información tangibles (computadores, impresoras, equipos de comunicaciones, etc.). Los datos mínimos que debe contener el inventario de activos son:

- Nombre del equipo
- Marca
- Modelo
- No. De serie
- No. De activo
- Ubicación
- Usuario a cargo

El inventario de los activos de información tangibles debe ser actualizado en la medida en que ocurra uno o varios de los siguientes casos:

- Cambios en el ambiente de negocios o estrategia organizacional
- Renovación o actualización tecnológica.
- Desarrollo o compra de un sistema de información (aplicativo)
- Pasado un año desde la última actualización del inventario.
- Depreciación y amortización de activos (software, hardware licencias, etc.).

Clasificación de la Información

Los responsables de la información en medio físico y magnético deben realizar la clasificación de acuerdo a los criterios de confidencialidad, sensibilidad, riesgo de pérdida o compromiso, aspectos legales, requerimientos de retención y facilidad de recuperación que deben ser empleados.

Los requerimientos legales, estatutarios y regulatorios deben ser considerados al momento de evaluar la clasificación de la información.

La clasificación de la información debe ser realizada simultáneamente con el inventario.

Los criterios para clasificar la información son:

Información de uso público o informativo:

- Su divulgación no requiere de autorización especial dentro y fuera de la entidad y su función es de comunicación del personal en general.
- Puede darse a conocer al público en general a través de carteleras, Intranet, memorandos, etc. No se requiere brindar las garantías para que no existan problemas de disponibilidad o de denegación en su consulta.
- Su modificación debe ser realizada exclusivamente por los autores y el personal asignado para esas tareas.

Información de uso interno o privada

- Su divulgación no autorizada, principalmente fuera de la entidad sería inadecuada o inconveniente, debe ser de conocimiento únicamente por parte de los funcionarios de la organización.
- Puede ser compartida entre áreas dada su necesidad para la operación diaria y no consolida resultados finales de gestión

Información de uso confidencial

- Sustenta estrategias de la Entidad, información financiera consolidada, informes de gestión para junta y gerencia, registros para toma de decisiones, información de pacientes y competencia, información de personal y cualquier otra que pueda comprometer la seguridad de la entidad o de las personas.
- Su divulgación no está autorizada, incluso dentro de la organización, por el impacto de daño que puede causar a la entidad. Debe ser usada únicamente por ciertos funcionarios de la Entidad quienes son responsables de su manejo.
- La Entidad determina que la información de los pacientes es clasificada como confidencial, por lo tanto, su manejo debe ser exclusivo para personas debidamente autorizadas y está limitado a actividades propias de la entidad, está totalmente prohibida su divulgación a personas no autorizadas.
- La información no puede desclasificarse o disminuir su nivel de clasificación sin llevar a cabo un análisis de los riesgos que esto implica, y una aprobación por el responsable de la información. Este determinará si su información puede moverse a una clasificación más baja o más alta basado en las definiciones de clasificación desarrolladas por Hospital.

Rotulación y tratamiento de la Información

- La información impresa debe ser rotulada en cada página con la clasificación de la información definida para dicho documento. Los documentos electrónicos deben tener la etiqueta de clasificación en el encabezado o en el pie de cada página.
- Todos los documentos que contienen información altamente sensible deben tener una portada o etiqueta donde se identifique su clasificación.

Controles para la Información Clasificada como Confidencial

- El envío a un tercero (incluyendo los pacientes) de información clasificada como confidencial debe ser autorizado por el responsable de la información.
- La información clasificada como confidencial que sea necesario enviar a un tercero (incluyendo los pacientes), debe ser transmitida utilizando mecanismos de seguridad que eviten el acceso no autorizado.
- La información confidencial en medio físico debe ser almacenada en áreas con acceso físico controlado, de tal forma que se garantice que solamente el personal autorizado tiene acceso a ella.
- Se debe llevar un log que permita realizar una trazabilidad de los cambios realizados a la información confidencial almacenada en medios magnéticos. El log debe identificar el responsable, fecha y hora del cambio.
- Cualquier información electrónica eliminada de sistemas informáticos y documentos impresos deben ser destruidos de tal forma que se proteja la confidencialidad de la información para lo cual debe diseñarse e implementarse un procedimiento al respecto

CONTROL DE ACCESO [A.9.1 - NTC-ISO-IEC 27001 2013]

Política de Control de Acceso Lógico

a) Todos los recursos informáticos y/o aplicativos del Hospital deben usar controles de acceso lógico, con el fin de prevenir el acceso no autorizado a la información confidencial de la Organización.

b) El acceso lógico a los recursos informáticos del Hospital debe ser controlado en función de los requerimientos de la Organización.
c) El control de acceso a la información debe ser definido, aprobado y documentado por los responsables de la información y deben estar basados en requerimientos específicos de la Entidad.
d) Se deben crear perfiles de acceso asociados a roles que tienen responsabilidades y cumplen con actividades comunes (cargos); estos perfiles deben permitir el acceso mínimo y suficiente para el adecuado desempeño de las actividades de los usuarios (política de menor privilegio). Los permisos de acceso a los aplicativos deben ser garantizados por cargos líderes y no por funcionarios.
e) Los permisos de acceso a las redes, servicios y sistemas de información del Hospital, serán otorgados mediante un proceso de aprobación que asegure el tener acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.
f) Todos los empleados y personal externo que acceden a los sistemas de información quedarán registrados y dispondrán de credenciales personales e intransferibles, con lo cual será responsable de mantener su confidencialidad y asegurar su correcto uso.
g) Se deben deshabilitar o actualizar los privilegios de acceso a los recursos informáticos inmediatamente se presente la novedad correspondiente o cuando se genere un cambio de privilegios en un rol o perfil.
h) Cuando un empleado o un usuario externo deja la Institución o cambia de posición, se deben eliminar o reasignar sus privilegios de acceso a los recursos informáticos del Hospital.
i) El responsable de la Información debe realizar una comparación periódica entre los requerimientos de acceso de los usuarios a los aplicativos y el nivel de acceso con que realmente cuentan y verificar que los usuarios que efectivamente acceden la información corresponden a los autorizados previamente por él.
j) Los aplicativos deben ser el único vehículo para acceder a los datos de producción del Hospital.
k) Está totalmente prohibido el uso de usuarios compartidos en los sistemas de información.
l) La Coordinación del área de sistemas de información debe garantizar que todos los usuarios que tienen acceso a cuentas privilegiadas tengan sus propias cuentas personales para el uso diario. El uso de estas cuentas debe ser rastreado y monitoreado periódicamente

Registro de Usuarios

a) A cada funcionario (usuario) interno y/o externo de la Organización que requiera acceso a los sistemas de información, se le asignará un único usuario, el cual es de carácter personal e intransferible.
b) Los usuarios de los recursos informáticos del Hospital no deben compartir su código de usuario / contraseña o cualquier mecanismo otorgado para su identificación y autenticación. La responsabilidad que un usuario del Hospital adquiere al recibir su código de usuario / contraseña o cualquier mecanismo de identificación y autenticación se extiende a todo tipo de interacción que ese identificador tenga con el sistema.
c) La creación, modificación y eliminación de cuentas de usuarios debe ser realizada mediante un procedimiento formal y debe ser autorizada por el responsable de los datos (PRO-GIN-09 y FOR-GIN-42).
d) Está totalmente prohibido que las áreas utilicen los códigos de usuarios de funcionarios que se encuentren ausentes (vacaciones, licencias, etc) de La Empresa. En caso de que se requiere el acceso a un aplicativo, es necesario hacer la solicitud formal para otro funcionario mediante el procedimiento establecido (PRO-GIN-09).
e) La eliminación de accesos y servicios de red asociados a un código de usuario debe ser realizada inmediatamente el usuario ha finalizado su vinculación laboral, contractual o comercial con Hospital o ha cambiado de rol dentro de la entidad y no se requiere que acceda a estos recursos informáticos. La oficina de Talento Humano es responsable por reportar al área de sistemas las novedades presentadas con los funcionarios sin importar el tipo de vinculación laboral

con el Hospital (temporales, de planta, practicantes SENA, etc.). Los líderes de las áreas son responsables por reportar al área de sistemas las novedades de usuarios pertenecientes a consultores, asesores, estudiantes, auditores externos y otros terceros que tengan acceso a los sistemas de información.

f) El área de sistemas debe conservar un registro de la solicitud, entrega y eliminación de los usuarios.

Política de Administración de Contraseñas

a) Las contraseñas deben cumplir con el siguiente estándar:
   - Longitud mínima de 10 caracteres
   - Alfanumérica
   - Debe contener mayúsculas y minúsculas.
   - Debe contener por lo menos 1 caracteres especiales.
   - No debe contener datos relacionados con la persona

b) La contraseña expira cada 60 días y debe ser cambiada por los usuarios. El sistema avisará días antes que se debe cambiar la contraseña

c) El sistema debe solicitar el cambio de la contraseña de manera obligatoria la primera vez que se ingrese al sistema.

d) Los sistemas de información deben permitir que los usuarios puedan crear y modificar sus propias contraseñas.

e) Los sistemas de información deben exigir que los usuarios confirmen su contraseña.

f) Los sistemas deben almacenar y transmitir las contraseñas de modo seguro.

g) El área de sistemas debe asegurar que las computadoras, las bases de datos y aplicaciones que almacenan la cuenta de usuario y la contraseña, restringen el acceso sólo al personal autorizado. Este acceso debe ser revisado trimestralmente y debe coincidir con la revisión técnica del empleado, contratista, temporal, practicante; del servidor y el usuario utilizados.

h) Los usuarios internos y externos que presenten 3 intentos fallidos en el momento de digitar la contraseña, la cuenta debe ser bloqueada y no pueden tener acceso al sistema de información al cual está intentando acceder. Estas cuentas deben ser desbloqueadas manualmente por la Mesa de Servicio. La identidad de los usuarios que solicitan restablecer la contraseña debe ser verificada antes de restablecer la contraseña.

i) Los usuarios deben asegurar que las contraseñas no están escritas o almacenadas en los sistemas de información en archivos no protegidos. Los usuarios no deben copiar nombres de usuarios y/o contraseñas en los scripts o archivos de texto claro, trabajos por lotes o la documentación de procesos.

j) El área de sistemas, debe garantizar que las cuentas de usuario que no hayan sido utilizadas por 90 días se deshabiliten automáticamente.

Inicio de sesión seguro

a) El área de sistemas debe garantizar que, en el momento de ingresar a los sistemas de información, se le informa al usuario que:
   - El sistema debe ser utilizado únicamente por usuarios autorizados
   - Mediante el uso del sistema, el usuario acepta que él o ella es un usuario autorizado
   - Es consciente que está siendo monitoreado al utilizar este sistema.

b) El área de sistemas, debe garantizar que los sistemas operativos o sistemas de información que proveen servicios de autenticación no transmiten las contraseñas en texto claro

c) El área de sistemas, debe garantizar que los sistemas de información no ofrecen a los usuarios toda la información sin antes haber iniciado sesión. El proceso de acceso no debe ofrecer ninguna 'Ayuda' o revelar que característica de la secuencia de inicio de sesión (ID de usuario o contraseña) es incorrecta

Restricciones en el período de uso de las sesiones

a) El área de sistemas debe garantizar que las sesiones del sistema operativo que se encuentran inactivas durante 10 minutos, son automáticamente cerradas.

Política de Uso del Correo Electrónico

a) El servicio de correo electrónico es para uso exclusivo de las actividades relacionadas con el trabajo de cada funcionario.
b) El envío de información clasificada como confidencial, debe ser aprobado por el Jefe de Área o el Dueño de la Información. Para el envío de esta información, es recomendable utilizar algún mecanismo de cifrado o protección mediante password.
c) Se prohíbe la difusión no solicitada de puntos de vista personales referentes a temas políticos, raciales y religiosos, al igual que la inclusión de mensajes sobre creencias, frases célebres, convocatorias políticas entre otros, al igual que usar el email para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular
d) Se prohíbe fomentar el envío de cadenas de mensajes, recepción o envío de mensajes con archivos adjuntos con extensiones .exe, .avi, .mp3, .vbs, .mpg, .jpg los cuales corresponden a archivos de video, música, gráficos, juegos, ejecutables, etc.
e) Este servicio no debe usarse para enviar SPAM o mensajes no solicitados ni tampoco para enviar material obsceno e ilegal o relacionado a pornografía infantil o cualquier clase de pornografía.
f) Está prohibido configurar reglas en los buzones de correo electrónico que reenvíen los mensajes a servidores públicos de Internet como Hotmail, Yahoo!, etc.
g) No se puede utilizar el correo electrónico, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas de La Empresa.
h) No se puede usar para la transmisión, distribución, almacenamiento de cualquier material protegido por las leyes vigentes. Esto incluye sin limitación alguna, todo material protegido por derechos de autor (copyright), Marcas registradas, secretos comerciales u otros de propiedad intelectual
i) El tamaño de los archivos adjuntos no debe exceder el estándar definido por el área de sistemas, este tamaño puede ser chequeado por medio de las propiedades de cada archivo. Si el archivo adjunto excede este tamaño, es necesario comprimir el archivo.
j) El nivel de almacenamiento de los buzones no puede exceder el estándar definido por el área de sistemas, por lo tanto, el usuario debe eliminar periódicamente los mensajes leídos de modo tal que no exceda esa cuota. En caso de que el usuario requiera ampliación de esta capacidad, debe ser autorizada por el área de sistemas.
k) La firma predeterminada solo puede contener nombre y apellidos, cargo, extensión y nombre de la entidad.
l) Está prohibido adjuntar firmas escaneadas.
m) En caso de recibir un mensaje bajo sospecha de virus, (de personas desconocidas con asuntos desconocidos o sospechosos) no se debe abrir y se debe reportar de inmediato al área de sistemas y/u Oficial de Seguridad de la información.
n) No está permitido el uso de cuentas de correo personales como Hotmail, Yahoo, Gmail, etc., para transmitir o intercambiar información referente o perteneciente al Hospital.

Políticas de Uso de Internet

a) El acceso a internet está restringido únicamente a páginas de información financiera, técnica, comercial, médicas, de innovación e investigación, cultural, etc., a las cuales por desarrollo de las actividades propias de cada cargo sea necesario ingresar para consultar información que faciliten las labores relacionadas al cargo.

El acceso a internet NO puede ser utilizado para los siguientes propósitos:

a) Actividades relacionadas a juegos online por internet
b) Ingreso a cualquier material considerado como pornográfico, ofensivo, discriminatorio o ilegal según las normas internas de La Empresa y la legislación
c) Ingreso a páginas de pornografía infantil
d) Ingreso a Redes sociales como Facebook, Twitter, LinkedIn, Youtube, etc para actividades de ocio. Nota: el área de mercadeo y comunicaciones si tienen acceso a estas redes sociales.
e) Descargar música, videos, fotos, fondos de pantalla, programas, juegos etc. los cuales representan un alto riesgo de virus y daños al computador y de legalidad en su uso por derechos de autor.
f) Utilizar los servicios de RADIO y TV por demanda.
g) Utilizar los servicios de Internet para enviar archivos que sean confidenciales y de propiedad exclusiva del Hospital
h) Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocios particulares.
i) Utilizar los servicios de internet para la transmisión, distribución o almacenamiento de cualquier archivo protegido por las leyes vigentes. Esto incluye todos los archivos protegidos por derechos de autor, marcas registradas, secretos comerciales u otros de propiedad intelectual.
j) El acceso no autorizado a cualquier intento de prueba, verificación o rastreo (scan) de vulnerabilidades de un sistema o red, violando las medidas de seguridad o de autenticación sin la expresa autorización del propietario del sistema o la red.
k) No se podrán utilizar los servicios de internet corporativo para establecer comunicaciones vía chat sin el VoBo del líder correspondiente.

Nota: Si se requiere alguna de las redes sociales restringidas por un periodo de tiempo para llevar a cabo alguna actividad, el jefe inmediato debe de enviar al área de sistema la solicitud con la siguiente información: Nombre del funcionario al que se le va a dar el permiso, Tiempo de uso y nombre de la aplicación.

SEGURIDAD FÍSICA Y DEL ENTORNO [A.11 - NTC-ISO-IEC 27001 2013]

Áreas de Acceso Restringido

Se define como aquellas áreas que necesitan autorización previa para permitir el ingreso de personas ajenas al área, por la naturaleza de la información confidencial que se maneja o los procesos que allí se realizan. Dentro de la Entidad fueron identificadas las siguientes

- Datacenter
- Gerencia
- Caja
- Tesorería

- Archivo central
- Almacén
- Archivo Historia Clínica

Control de Acceso Físico a las dependencias del Hospital

a) El ingreso de dispositivos de grabación de audio, fotos y video a las áreas de acceso restringido o áreas seguras está totalmente prohibido.
b) El Hospital debe asegurar que los derechos de acceso a todas las instalaciones sean revisados anualmente. El acceso a lugares considerados áreas seguras, debe ser revisado regularmente.
c) Todos los visitantes, empleados, temporales, contratistas y practicantes deben ser autorizados para la entrada física a las instalaciones la Hospital
d) Los funcionarios de la Hospital deben portar en un lugar visible el carnet de identificación como funcionarios
e) Los visitantes temporales, contratistas y practicantes deben portar un STICKER que los identifica como visitantes ocasionales.
f) La autorización del acceso de visitantes a las áreas seguras está en cabeza de la Gerencia o el delegado de ésta, de acuerdo al procedimiento establecido según corresponda.
g) Una vez autorizado el ingreso del visitante, el funcionario visitado deberá recogerlo y acompañarlo todo el tiempo durante el recorrido o su permanencia en el área segura.
h) Todos los visitantes a las áreas seguras deben tener previa autorización del líder del área antes de ingresar al área.

Protección de la Central de Datos

a) La central de datos o Datacenter del Hospital, deben incorporar medidas de protección para reducir al mínimo la posibilidad y las repercusiones de incidentes como incendios, inundaciones, terremotos, explosiones, disturbios civiles, etc.
b) El sistema eléctrico de la central de datos debe contar con un sistema de UPS, así como de condiciones eléctricas acordes a las normas internacionales.
c) Las instalaciones de la central de datos se deben supervisar 24 horas al día. Esta supervisión puede ser realizada por medio de las cámaras de video, puertas de emergencia y ventanas, personas de vigilancia en los centros, o una combinación de lo antes nombrado.
d) Los operadores, administradores y visitantes frecuentes a la central de datos, deben ser capacitados en los procedimientos que deben seguir cuando se presente un evento de origen físico que afecte la continuidad en la operación normal de la central de datos.
e) Los equipos y dispositivos que son utilizados para soportar las funciones de la Entidad, deben estar en un área de acceso restringido y separadas del ambiente de las oficinas y puntos de atención.
f) Está totalmente prohibido fumar y consumir alimentos en la central de datos.
g) Cuartos que contienen el cableado o el equipo de comunicaciones (armarios de cableado, cuartos de PBX, etc.) debe tener siempre con acceso restringido y solamente a personal autorizado.

Seguridad del Cableado

a) Debe haber un monitoreo periódico sobre las redes de cableado estructurado de voz y datos y los gabinetes de cableado, para detectar, eliminar o prevenir el uso de dispositivos no autorizados conectados a los cables

b) El Profesional Universitario debe asegurar que todas las conexiones de red que existan en un lugar que no está siendo utilizado de manera permanente están deshabilitadas.
c) Los conductos de cableado de red deben ser protegidos contra interferencia o interrupción. Esto incluye evitar cableado en áreas públicas, segregación de cableado de energía para eliminar interferencia y el rotulado claro para la identificación de los equipos.
d) Los cuartos asignados para los gabinetes de cableado estructurado deben contar con acceso físico restringido y no se debe almacenar ningún tipo de material inflamable.

Mantenimiento de Equipos

a) El área de sistemas con el apoyo de la Gerencia, debe garantizar que el acceso al mantenimiento preventivo y/o correctivo de software o hardware es realizado por funcionarios debidamente autorizados e identificados. Ningún funcionario del Hospital debe permitir la manipulación de equipos y/o software por personal que no esté identificado y autorizado por el área de sistemas. Si el equipo debe ser sacado de las instalaciones para realizar las reparaciones, la confidencialidad e integridad de cualquier información debe ser garantizada.
b) Todos los recursos de TI (hardware y software) que soportan la operación de los procesos de la organización, así como la atención de los pacientes en los diferentes canales de servicio, deben contar con un contrato de mantenimiento preventivo y correctivo por parte del fabricante o proveedor.
c) En caso de presentarse un daño sobre algún elemento de trabajo por causas como: golpes, derrame de bebidas, elementos extraños, o alguna causa atribuible al usuario, el costo de la reparación o reposición debe estar a cargo del responsable del activo tecnológico.

Protección y Ubicación de Equipos

a) Para prevenir el acceso, la duplicación y la transmisión no autorizada de información confidencial, todas las impresoras, copiadoras, y máquinas de fax se deben situar en áreas seguras.
b) Todos los equipos tecnológicos del Hospital deben ser ubicados o localizados de tal forma que se reduzcan al mínimo los riesgos o amenazas. Esto incluye amenazas como hurto o vandalismo, fuego, explosión, humo, agentes químicos, pérdida de servicios de soporte como energía, comunicación, agua o cualquier otra amenaza física.
c) Los cuartos adyacentes a las instalaciones de procesamiento de información no se deben utilizar para propósitos que pueden implicar altos riesgos
d) Fumar, beber y comer en instalaciones de procesamiento de información está terminantemente prohibido.
e) El Hospital debe asegurar que cualquier equipo de procesamiento de datos que haya contenido información privada o información confidencial y que vaya a ser reutilizado experimente un proceso de limpieza lógica antes de ser utilizado nuevamente. El proceso de limpieza lógica debe consistir en la destrucción de la información que reside en el equipo y la validación del proceso, para asegurar que ningún dato se deja en el equipo o pueda ser recuperado. Lo anterior debe ejecutarse de acuerdo al PRO-GIN-11 Organización archivos de gestión.
f) El Hospital debe asegurar que para cualquier equipo de procesamiento de datos que haya contenido información privada o información confidencial y vaya a ser dado de baja, sus dispositivos de almacenamiento de información (disco duro, memoria RAM, memoria FLASH, etc.) sean destruidos físicamente antes de su disposición final.

Seguridad de Equipos Móviles

a) Todo equipo de propiedad del Hospital que esté fuera de las instalaciones de la Organización, no debe ser desatendido por su responsable en lugares públicos.

b) La Gerencia debe asegurar a través de pólizas de seguro las computadoras portátiles, módems celulares o dispositivos móviles como celulares o smartphones.
c) El área de sistemas debe velar porque los estándares de seguridad documentados dentro de la política se apliquen a todos los equipos y la información que en ellos se almacena, sin importar la localización de los mismos.
d) El jefe de Área del funcionario a quien le sea asignado un portátil, debe solicitar la compra e instalación de guayas de protección para los portátiles

Retiro de equipos de las Instalaciones

En caso de retiro de un equipo de las instalaciones del Hospital, se debe solicitar permiso (utilizando el formato establecido) al profesional universitario de activos fijos y debe quedar el registro de la fecha y hora de salida en el libro de seguridad, también debe registrarse el nombre del responsable a cargo del equipo.

Suministros de Equipos de Soporte Energético

- El área de sistemas debe asegurarse que las fuentes de alimentación continuas (UPS) son utilizadas en los equipos que apoyan las operaciones de negocio críticas para facilitar la disponibilidad de los sistemas y su correcto apagado. Las UPS deben ser revisadas periódicamente para asegurar que tienen la capacidad adecuada y aprobada, de acuerdo con las recomendaciones del fabricante.
- El área de sistemas, en apoyo del departamento de servicios generales debe realizar un estudio anual de las cargas en los circuitos eléctricos, para que, en una eventual falla del suministro de energía eléctrica, la planta electica envíe los voltajes adecuados, para sostener el sistema de corriente ininterrumpido en la corporación

Política de Escritorio Limpio

Físico

a) Está prohibido el uso unidades de almacenamiento externo (USB, CDROM, DVD, etc.) en las estaciones de trabajo de las áreas asistenciales (urgencia, consulta externa, salas de hospitalización, hospital día, bellavista, farmacia, entre otras) asignadas para el cumplimiento de las funciones. Las estaciones de trabajo de las áreas administrativas se les relacionara una única USB bajo la autorización del jefe inmediato.
b) Esta prohibido el uso de dispositivos con cámaras fotográficas que evidencien la intensión de extraer información (asistencial y/o administrativa) sensible del Hospital.
c) La información clasificada confidencial que no esté siendo utilizada por personal autorizado, debe permanecer siempre bajo llave y no debe ser desatendida en ninguna ubicación no controlada.
d) Todos los funcionarios que tengan bajo su responsabilidad información confidencial, deben garantizar su almacenamiento bajo llave en las instalaciones de la Entidad.

Digital

a) Que todos los funcionarios deben tener su escritorio digital del computador libre de información de carácter confidencial o sensible a la vista la cual puede ser observada o accedidas por personas ajenas al área.

b) Lo únicos iconos que deberían de permanecer en el escritorio digital del computador son: aplicaciones institucionales instaladas, papelera reciclaje, plataforma documental, Intranet, eventos adversos, oficina virtual de talento humano, resultado de laboratorios.

Política de Equipos Desatendidos

a) Cuando un funcionario se retire temporalmente de su puesto de trabajo, debe hacer un logout de la sesión del aplicativo y activar el bloqueo del escritorio de trabajo del computador mediante la opción de protector de pantalla.
b) Durante cualquier reubicación del espacio de trabajo de un empleado, el empleado debe asegurar que todos los activos de información están protegidos durante el proceso de reubicación. Esto incluye, pero no se limita a, el equipo y los archivos impresos.
c) Durante cualquier reubicación del espacio de trabajo del empleado, la información altamente sensible debe ser trasladada por el dueño de la información.

CUMPLIMIENTO DE LOS REQUISITOS LEGALES [A.18.1 - NTC-ISO-IEC 27001 2013]

Identificación de la legislación aplicable

Todos los requisitos legales, contractuales, o regulatorios que sean aplicables a la Organización, deben ser documentados y definidos por la Oficina Jurídica. Los requisitos y las responsabilidades específicas de controles u otras actividades relacionadas, con estas regulaciones legales, deben ser delegadas a la unidad de negocio apropiada

Derechos de Propiedad Intelectual

a) Todo el software instalado en las estaciones de trabajo y servidores del Hospital debe ser licenciado y los usuarios deben cumplir con las leyes y las restricciones de derecho de autor definidas por el fabricante. Adicionalmente, todo el software instalado en los recursos informáticos de la Entidad debe ser aprobado por el Profesional Universitario y/u Oficial de Seguridad de la Información. Cualquier software introducido en el ambiente de producción, debe ser analizado y aprobado por estas áreas.
b) Está prohibido el almacenamiento y uso de archivos con extensiones .avi, .mp3, .mpg, .Jpg los cuales corresponden a archivos de video, música, gráficos, juegos, etc. Que no estén debidamente licenciados por la Empresa.
c) La instalación de software o el uso de información externa en los recursos informáticos del Hospital debe ser previamente autorizada por la Gerencia o su delegado y debe cumplir con los requerimientos legales que faciliten su utilización.
d) El software que reside en los computadores del Hospital sólo podrá ser autorizado por la Gerencia. No se podrá instalar en los computadores de La Empresa software que no esté registrado y autorizado.
e) El Profesional Universitario del Hospital realizará revisiones periódicas al software instalado en las estaciones de trabajo y eliminará sin previo aviso todos los aplicativos y archivos que no estén autorizados previamente. Los responsables de la instalación, descarga y/o uso de software que viole los acuerdos de licenciamiento serán sujetos de las acciones disciplinarias definidas por parte de la alta gerencia.
f) El área de sistemas deben aprobar todo el shareware, freeware y software libre para ser usados en los recursos de cómputo de la Entidad con el fin de asegurar que en el software no esté presente código malicioso y/o que no cumpla con las necesidades de la Entidad o de seguridad.
g) Las violaciones de los derechos o políticas de propiedad intelectual de la Entidad están sujetas a acciones disciplinarias.

h) La compra o uso de software de terceros debe cumplir con los acuerdos de licenciamiento definidos por el fabricante. Estos acuerdos pueden detallar restricciones específicas del usuario (ej.: el número de copias instaladas permitidas, número de máquinas donde es posible instalar el software o número de usuarios concurrentes que pueden conectarse al software). Los niveles de soporte al Hospital (en sitio o por teléfono) se pueden también especificar dentro del acuerdo.

Propiedad Intelectual

Todos los desarrollos de productos realizados por funcionarios de la entidad, contratados o producidos bajo acuerdos que le asignen la propiedad intelectual del trabajo a Hospital son de propiedad del Hospital.

Prevención del mal uso de las instalaciones de procesamiento de información

- El monitoreo de los sistemas de información y/o estaciones de trabajo se realizará exclusivamente por los organismos de control interno de la entidad y se debe llevar a cabo de acuerdo a las leyes y regulaciones locales.
- Los recursos de tecnología (hardware y software) son para uso exclusivo de la Entidad. El uso no adecuado de cualquier recurso de tecnología de la Entidad o para otros propósitos diferentes a los definidos por el negocio está prohibido. Cualquier actividad no autorizada debe ser reportada a la gerencia.
- Los usuarios deben ser notificados, mediante mensajes escritos o a través de mensajes de alerta al obtener acceso a sistemas, que la actividad está siendo monitoreada.

Protección de registros de la Entidad

a) Los estándares para la recolección, custodia, manejo y destrucción de registros deben ser desarrollados para cualquier información cubierta por estatutos legales o regulatorios. El cronograma de retención para este tipo de información debe ser definido y divulgado. Dicho cronograma debe contener, sin limitar:
   - Tipo de información.
   - Estatutos reguladores relacionados.
   - Inventario de fuentes de este tipo de información.
   - Período de retención de registro.
   - Requerimientos apropiados de almacenaje y manejo.
   - Métodos apropiados de destrucción.
   - Cualquier requisito especial implementado que no esté definido en la política de seguridad de la Entidad.

b) Es responsabilidad del dueño de la información definir el cronograma de retención de cada registro documental.

Regulación de controles criptográficos

La seguridad criptográfica, incluyendo el uso de hardware o software, implementados en los sistemas corporativos deben cumplir con cualquier legislación local o internacional

8. CUMPLIMIENTO

a) Los jefes de procesos y áreas deben llevar a cabo los procedimientos de escalamiento y reporte cuando se observa el incumplimiento o se genera una excepción de la política de seguridad de la Entidad.

b) Los jefes de procesos y áreas deben revisar regularmente los procesos y procedimientos dentro de su área para asegurar que las responsabilidades y deberes de seguridad se realizan apropiadamente. Los resultados de esta revisión y las acciones correctivas deben ser documentados.
c) El área de sistemas debe revisar el cumplimiento con las prácticas de seguridad de la Entidad. Las situaciones que dan como resultado el incumplimiento de las prácticas, deben ser reportadas a la gerencia apropiada. Las actividades de revisión deben incluir el monitoreo operacional del cumplimiento, análisis individual del sistema, revisiones de terceros, pruebas de conformidad internas, y/o revisiones de los procedimientos.
d) La violación deliberada de las políticas de seguridad de la información y/o del incumplimiento de regulaciones, será sancionada mediante un proceso disciplinario ejecutado por la Jefe Oficina Asesora de Control Interno Disciplinario para el caso de funcionarios de La Empresa o a través de contratos o procesos jurídicos en caso de terceros.

9. ANEXOS

- FOR-GIN-14 Formato Hoja de vida de equipos informáticos
- FOR-GIN-45 Formato de mantenimiento de equipos informáticos
- FOR-GIN -16 Formato seguimiento bitácora ingreso central de datos
- PRO-GIN-09 Procedimiento para solicitud de usuarios y permisos en los softwares institucionales
- FOR-GIN-42 Formato de activar o inactivar usuarios.

Actualizado por:	Revisado por:	Aprobado por:
MARCELA MARTINEZ TURRIAGO Profesional Universitario Sistemas	**BERENICE** RIVERA TRUJILLO Líder ISC	**GLORIA ELIZABETH RUIZ GARCIA** Líder ISC
Fecha: 04 de noviembre de 2.022	**Fecha:** 15 de noviembre de 2.022	**Fecha:** 17 de noviembre de 2.022

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA DE VIGENCIA
01	Creación del documento	Agosto 2016
02	Actualización del documento	Abril 2019
03	Actualización del documento incluyendo lo referente a telemedicina	Agosto 2019
04	Actualización de formatos	Diciembre 2021
05	Actualización lineamiento con la política basado en la ISO 27001:2013	Noviembre 2022