Hospital Departamental
Psiquiátrico Universitario
Del Valle E.S.E.

| | |
|---|---|
| CÓDIGO | MAN-GIN-01 |
| VERSIÓN | 04 |
| VIGENCIA | DICIEMBRE 2021 |

# MANUAL DE SEGURIDAD DE LA INFORMACION Y USO DE LOS RECURSOS INFORMATICOS

MAN-GIN-01

## 1. OBJETIVO GENERAL

Establecer los lineamientos respecto a la disponibilidad, integridad y confidencialidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizada, daño o 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.

## 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:

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 gobierno digital.
- Realizar seguimiento a los planes y estrategias definidas.

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 responsabilidades 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

## 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. SEGURIDAD DEL RECURSO HUMANO

La seguridad de la información se define como la capacidad para preservar su integridad, confidencialidad y disponibilidad por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como el recurso humano que utiliza dichos componentes.

En este sentido, es fundamental educar e informar a todo el personal que ingresa al Hospital Departamental Psiquiátrico Universitario del Valle ESE, contratistas y/o terceros que tengan la posibilidad de acceder a la información de la Institución o a la infraestructura tecnológica para su procesamiento, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

Por otra parte todos los funcionarios del Hospital Psiquiátrico Universitario del Valle ESE, deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la Institución.

### ROLES Y RESPONSABILIDADES

El Hospital Departamental Psiquiátrico Universitario del Valle ESE, ha establecido un manual específico de funciones y de competencias laborales para los empleos de planta de personal, cuyas funciones deberán ser cumplidas por los funcionarios

con criterios de eficiencia y eficacia en orden al logro de la Misión, Objetivos y Funciones que la ley y los reglamentos le señalan.

**SELECCIÓN DE PERSONAL**

El Hospital Departamental Psiquiátrico Universitario del Valle E.S.E regula el empleo público, la carrera administrativa, gerencia, como se encuentra establecido en norma: Ley 909 de 2004 "Artículo 1º. Objeto de la ley. La presente ley tiene por objeto la regulación del sistema de empleo público y el establecimiento de los principios básicos que deben regular el ejercicio de la gerencia pública.

Quienes prestan servicios personales remunerados, con vinculación legal y reglamentaria, en los organismos y entidades de la administración pública, conforman la función pública. En desarrollo de sus funciones y en el cumplimiento de sus diferentes cometidos, la función pública asegurará la atención y satisfacción de los intereses generales de la comunidad.

De acuerdo con lo previsto en la Constitución Política y la ley, hacen parte de la función pública los siguientes empleos públicos:
a) Empleos públicos de carrera;
b) Empleos públicos de libre nombramiento y remoción;
c) Empleos de período fijo;
d) Empleos temporales".

Como regla general, los empleos en vacancia definitiva deberán ser provistos mediante concurso de méritos; sin embargo, mientras se lleva a cabo el proceso de selección, la ley faculta su provisión mediante la figura del Encargo prevista en el Artículo 24 de la Ley 909 de 2004, y conforme a lo establecido en el Artículo 25 de la Ley ibídem, procede la provisión transitoria a través del Nombramiento Provisional, de manera excepcional y únicamente cuando no fuere posible su provisión a través de encargo con servidores públicos de carrera administrativa.

En este sentido, si para la administración surge la necesidad de proveer un empleo de carrera en vacancia definitiva o temporal, deberá verificar el cumplimiento de los requisitos previstos en el Artículo 24 de la Ley 909 de 2004, con el fin de determinar la existencia de un empleado con derecho de carrera sobre el cual pueda recaer el encargo, por lo que no solo es viable sino obligatorio para la administración, dar aplicación a la normatividad vigente.

**TERMINOS Y CONDICIONES LABORALES**

Todo el personal que ingrese al Hospital Departamental Psiquiátrico Universitario del Valle E.S.E como funcionario ya sea por carrera administrativa, libre nombramiento y remoción, período fijo, temporales, contratistas y terceros, deben regirse y acogerse a las políticas de Seguridad de la Información, así como los términos de uso adecuado de los recursos informáticos que le son entregados, responsabilidades extensibles aún fuera de la Institución.

De igual forma todo el personal, contratista y/o tercero y estudiantes en práctica formativa que tengan acceso a información de la Institución o a la Infraestructura tecnológica, debe firmar, previamente, un acuerdo de confidencialidad y no divulgación, en el que se especifique el período por el cual debe mantener el acuerdo y las acciones que se toman cuando se incumpla este requerimiento. Incluye aspectos como propiedad intelectual, protección de la información, leyes aplicables basadas en las Políticas Institucionales, Políticas de Seguridad de la Información, Políticas de tratamiento protección de datos personales.

**PLAN DE SENSIBILIZACION, CAPACITACION Y COMUNICACIÓN SOBRE LA SEGURIDAD DE LA INFORMACION:**

El Hospital Departamental Psiquiátrico Universitario del Valle E.S.E tiene establecido un procedimiento para el ingreso de personal por medio del cual asegura que todos los funcionarios conozcan las políticas institucionales, entre ellas la política de seguridad de la información y uso de los recursos informáticos, además la responsabilidad que adquieren frente a la seguridad

de la información y que cuentan con las competencias para desempeñar sus funciones y con los programas de capacitación y entrenamiento requeridos para ello.

De igual manera, todo el personal, contratista y tercero tendrán un proceso de concientización, mediante el cual se le capacitará sobre las políticas de seguridad de la Institución y los riesgos conocidos a los que se puede ser expuesta.

Los planes de inducción y reinducción, se encuentran diseñados de manera apropiada y relevante para los roles, responsabilidades y habilidades de las personas que deben asistir a ellos.

**PROCESO DISCIPLINARIO**

Cuando sea detectado un incumplimiento a las políticas de seguridad de la información y uso adecuado de los recursos informáticos, el cual pueda poner en riesgo un activo de información, el área de sistemas registrara el evento o incidente en la plataforma "gestión de requerimientos e incidentes de TI", realizara el correspondiente seguimiento e investigación de los hechos para determinar las causas y responsables; posteriormente El Hospital Psiquiátrico universitario del valle E.S.E, tomara las acciones pertinentes para el personal y/o tercero vinculado con el incidente, mediante un proceso disciplinario formal de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la Institución dicho incidente de acuerdo al Procedimiento DE CONTROL INTERNO DISCIPLINARIO.

**TERMINACION O CAMBIO DE LA CONTRATACION LABORAL**

El Hospital Departamental Psiquiátrico Universitario del Valle E.S.E, cuenta con un procedimiento para el retiro de personal donde establece que tiene dos tipos de empleados: Empleado público y Empleado oficial, los cuales pueden desvincularse de la entidad bajo las siguientes modalidades: por renuncia regularmente aceptada o terminación del contrato; por retiro con derecho a jubilación; por declaratoria de insubsistencia del nombramiento, como consecuencia de calificación no satisfactoria en la evaluación del desempeño laboral; por supresión del cargo; por muerte; por invalidez absoluta; por edad de retiro forzoso; por destitución, desvinculación o remoción como consecuencia de investigación disciplinaria; por declaratoria de vacancia del empleo en caso de abandono del mismo; por revocatoria del nombramiento por no acreditar los requisitos para desempeñar el empleo, de que trata el artículo 5 de la ley 190 de 1995; por orden o decisión judicial, por las demás que determine la constitución política, las leyes y los reglamentos. En todos los casos de retiro mencionados anteriormente, aplica la cláusula tercera establecida en el Acuerdo de confidencialidad "OBLIGACIONES ESPECIALES DEL EMPLEADO PÚBLICO/TRABAJADOR OFICIAL:

- Guardar absoluta confidencialidad, incluso después de terminada la vinculación legal y reglamentaria o el contrato de trabajo respecto a: procedimientos, métodos, características, protocolos de manejo y similares, claves de seguridad, suministros, software, base de datos de cualquier índole, valores de bienes y servicios, información técnica, financiera, económica y demás que el Hospital Departamental Psiquiátrico Universitario del Valle E.S.E. utiliza en el desarrollo de su objeto social frente a usuarios o terceros.
- No ejercer actos de competencia desleal frente al Hospital Departamental Psiquiátrico Universitario del Valle E.S.E., por lo que el Empleado público /Trabajador Oficial se compromete a no utilizar, incluso después de terminado el contrato de trabajo para sí o para beneficio de terceros: la lista de clientes, base de datos de cualquier índole, sus fórmulas químicas biológicas y similares, sus software, o procedimientos, claves secretas, métodos, características, estudios, estadísticas, proyectos, protocolos de manejo y suministros utilizados por el Hospital Departamental Psiquiátrico Universitario del Valle E.S.E., interna y externamente frente a sus clientes o terceros, información técnica, financiera, económica o comercial del Hospital.
- De conformidad con la normatividad vigente es obligación del empleado público / Trabajador Oficial, una vez finalizado el vínculo laboral, legal o contractual con el Hospital hacer entrega de la información a su

cargo tales como: claves, bases de datos, equipos, información técnica, financiera, económica o comercial, fórmulas químicas biológicas o similares que haya recibido para poder ejecutar su labor ".

Responsabilidades en la terminación contractual o cambio de funciones

El área de Talento Humano, La Subgerencia Administrativa y Financiera, en conjunto con el jefe directo del funcionario y/o responsable del tercero, son los encargados de informar y notificar sobre el proceso de terminación de labores y asegurar que todos los activos propios de la Institución sean devueltos, los accesos físicos y lógicos sean eliminados, y la información pertinente sea transferida, de acuerdo con los procedimientos establecidos en el proceso de terminación de contrato.

En caso que un funcionario y/o tercero tenga un cambio de funciones, se debe seguir los mismos procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de los mismos de acuerdo a su rol.

## GESTION DE ACTIVOS

La gestión y clasificación de activos de información que son manejados por cada entidad del estado, son procesos fundamentales para determinar que activos posee la entidad, de cómo deben ser utilizados, los roles y responsabilidades que tienen los funcionarios sobre los mismos y, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele.

La realización de un inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de una entidad.

El HDPUV, debe tener total control y conocimiento sobre los activos que posee como parte importante de la administración y gestión de riesgos. Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- Activos físicos: equipamiento informático (Servidores, Equipos de Almacenamiento, CPU, monitores, computadores de escritorio, computadoras portátiles, módems), equipos de comunicaciones (routers, PBX, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (iluminación, energía eléctrica normal y regulada, voz, datos, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de indicar cómo ha de ser tratada y protegida dicha información.

Teniendo en cuenta lo anterior, el área de Gestión documental en conjunto con el área de sistemas del HDPUV, ha documentado, el inventario de activos de información de las diferentes áreas del hospital, teniendo en cuenta las siguientes definiciones:

**Inventario de activos:** todos los activos deben estar claramente identificados y la entidad debe elaborar y mantener un inventario de los mismos.

**Propiedad de los activos:** los activos de información del inventario deben tener un propietario.

**Clasificación de la información:** La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

**Etiquetado y manipulado de la información:** Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

**Asignación de Activos:** En el inventario de activos del HDPUV se identificará el propietario del activo, quien debe asegurar que la información y los activos asociados con su proceso están clasificados de manera apropiada, así como de establecer controles necesarios para el acceso a éstos de acuerdo con los procedimientos definidos por el preso de gestión documental, gestión de activos y acuerdos de confidencialidad.

Los propietarios de la información deben ser los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea ejecutado de acuerdo a lo establecido en este ítem.

Los activos de información como equipos de escritorio o equipos portátiles, se asignaran de acuerdo a lo establecido en el procedimiento de activos fijos de la institución.

**Devolución de Activos:** Todo el personal, contratista y/o tercero del HDPUV al momento de su retiro o cambio de funciones en la Institución debe hacer entrega a su jefe inmediato de los equipos informáticos asignados a su puesto o lugar de trabajo en buenas condiciones, con toda la información contenida en él y una relación de la misma, según

lo establecido en procedimiento de retiro de personal del área de talento humano, y el procedimiento de activos fijos de la institución.

**Traslado de activos:** Cualquier traslado de equipos de cómputo se realizará en coordinación con el proceso de gestión de la información, previo diligenciamiento de FORMATO DE NOVEDADES DE ACTIVOS FIJOS establecido en el proceso de ambiente físico.

**Uso aceptable de los activos:** La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad del Hospital Psiquiátrico universitario del valle E. S.E., son activos de la Institución y se proporcionan al personal, contratista y/o tercero autorizado, para cumplir con las funciones o actividades asignadas.

El Hospital Psiquiátrico universitario del valle E.S.E. podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en este manual y en cualquier proceso legal que se requiera.

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso del personal, contratistas y/o terceros determinadas por los líderes de área y Subgerencias.

La consulta de expedientes o documentos que reposan en las diferentes oficinas y/o áreas del Hospital Psiquiátrico universitario del valle E.S.E., se permitirá en días y horas laborales, con la presencia del personal o servidor responsable de los mismos.

El personal, contratista y/o tercero se compromete a cumplir con los procedimientos establecidos para el servicio y consulta de documentos según lo definido en los procedimientos institucionales.

El líder o jefe del área, será quienes determinen el carácter de reserva o restricción de los documentos físicos. Todo el personal, contratista y/o terceros que manipulen información en el desarrollo de sus funciones deberán firmar un Acuerdo de Confidencialidad de la Información, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los lineamientos definidos en las Políticas de Seguridad de la Información y Políticas de tratamiento protección de datos personales y los lineamientos del presente documento. En caso de violación de la información será considerado como un incidente de seguridad y se procederá de acuerdo a lo definido al tratamiento de este tipo de incidentes.

Está PROHIBIDO retirar de las dependencias del Hospital reportes, cartas, memorando, manuales, información confidencial, cds, memorias o dvd con o sin información que sea de propiedad del Hospital. El software comercial (Office, Windows etc.) autorizado para usar en los microcomputadores sólo podrá ser instalado por el área de sistemas.

Está totalmente prohibido utilizar los equipos de cómputo, software y/o periféricos, para realizar actividades diferentes a las estrictamente laborales.

Todos los funcionarios del Hospital son responsables por los recursos informáticos que manejan (Hardware, Software y datos), teniendo la obligación de cumplir con todos los lineamientos que se dan en el presente manual.

## CONTROL DE ACCESO DE USUARIOS

El acceso por medio de un sistema de restricciones y excepciones a la información, es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad de los recursos informáticos.

El HDPUV proporcionará a los funcionarios y contratistas (personas naturales) 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, enrutadores, agendas electrónicas, celulares inteligentes, access point, que no sean autorizados y configurados por el área de sistemas de la entidad.

El acceso a la central de datos del HDPUV es restringido y solo puede ingresar personal autorizado por el área de TI o por la gerencia, para procesos específicos como mantenimiento de equipos por personal especializado o servicio de aseo, lo anterior en compañía de un responsable del área de TI.

Solo usuarios designados por el Área de Sistemas estarán autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones del Hospital.

El HDPUV 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 les dé a las claves asignadas.

El acceso a aplicativos institucionales tanto financieros, administrativos y asistenciales, se concederá teniendo en cuenta el perfil de usuario, al cual se asignara un grupo parametrizado con los permisos a programas, menús y opciones específicos de acuerdo a sus funciones.

Todo trabajo que utilice los servidores del Hospital Psiquiátrico Universitario del Valle E.S.E con información de la entidad, sus funcionarios o contratistas, se debe realizar en sus instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del área de sistemas.

Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación del El Hospital Psiquiátrico universitario del valle E.S.E de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

Las claves o contraseñas deben poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: Fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc. Las claves no deberán ser regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.

## ACCESO A REDES Y SERVICIOS DE RED

El Hospital psiquiátrico Universitario del Valle cuenta con una infraestructura de Red LAN certificada con cableado tipo 6ª, la cual es administrada y gestionada por área de TI de la institución, el acceso a la red y la gestión de usuarios de red se realiza desde un servidor de Dominio por medio de la herramienta Active Directory (directorio activo) de Windows, que es la que nos permite crear los usuarios para el inicio de sesión de los mismos en la red.

Dentro de los servicios de Red establecidos en El Hospital Psiquiátrico universitario del valle E.S.E, para los usuarios se tiene: Acceso red local, Acceso remoto, archivos, Impresión, Correo electrónico, Plataformas de Información Estratégica, Internet y Backups.
La habilitación de las redes y prestación de servicios de red se tramitará únicamente en el área de TI de la institución.

Para el caso de Telemedicina, se establecen los protocolos para el intercambio y transmisión de la información a través de la herramienta de mediación, que permite que se transmita de manera segura la información a la Unidad Remisora y así mismo, recibir la información relevante para el control de la Historia Clínica.

## SERVICIO DE INTERNET

El acceso a internet a través de la red es provisto por el Hospital a sus funcionarios, terceros y/o contratistas para la realización de sus actividades laborales, el uso de este recurso debe cumplir los siguientes criterios:

- Utilizar este servicio exclusivamente para fines laborales.
- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas o practicantes con acceso a este servicio.
- Descargar documentos o archivo tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- La información de Telemedicina que se descarga, cuenta con los respectivos protocolos de seguridad y encriptación, para evitar acceso por personas diferentes a las involucradas en el proceso.

Adicionalmente el Hospital se reserva el derecho de monitorear el correcto uso que los usuarios le den a este recurso, las siguientes actividades están expresamente prohibidas dado que exponen al Hospital y a su servicio de acceso a Internet a riesgos de seguridad informática y/o su consumo de recursos que perjudican la realización de las actividades laborales, entre estos están:

- Acceder a sitios de juegos o apuestas en línea.
- Acceder a sitios de divulgación, descarga o distribución de películas, videos, música, real audio, webcams, emisoras online, etc.
- Acceder y/o descargar material pornográfico u ofensivo.
- Utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por el Ara de Ti del Hospital.
- Compartir en sitios web información propia del Hospital clasificada como reservada o clasificada sus usuarios, funcionarios, contratistas o practicantes.
- Emplear este servicio para la recepción, envió o distribución de información pública clasificada o reservada del Hospital a través de servicios y cuentas de correo públicos.
- Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
- Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.
- Utilizar el servicio de Internet/Intranet para propósitos comerciales ajenos al Hospital.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados.
- Interferir intencionalmente con la operación normal de cualquier website o portal en Internet.
- Comprar o vender artículos personales a través de sitios web o de subastas en línea.
- Acceder a sitios de contenido multimedia (videos, música, emisoras online, etc.) debido al alto consumo de canal de Internet.
- Descargar, instalar y configurar navegadores distintos a los permitidos por el área de TI del Hospital.

Dentro de las responsabilidades de los Usuarios de Internet tenemos:

- Conocer, adoptar y acatar esta política cada vez que haga uso de este servicio.
- Dar aviso al área de TI del Hospital de cualquier fallo de seguridad de su cuenta, incluyendo su uso no autorizado, pérdida de la contraseña, bloqueo, etc.
- Los usuarios del servicio deben considerar que algunos sitios web no son seguros, especialmente los que hacen suplantación de entidades a los bancos y/o emisores de tarjetas de crédito (PHISHING) por lo que se recomienda confirmar esta información directamente con las mismas entidades.
- Igualmente no se debe proveer información personal ni laboral a sitios de dudosa validez.
- El Hospital no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al acceder a sitios de suplantación o al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al hacer el uso de este servicio.

## CORREO ELECTRONICO/INTRANET

El correo electrónico institucional es una herramienta de comunicación o intercambio de información oficial dentro del Hospital psiquiátrico universitario del valle E.S.E, son deberes de los funcionarios:

- Todos los mensajes que se envían a través de correo electrónico deben estar enmarcados en normas mínimas de respeto.
- El sistema de correo electrónico debe ser utilizado únicamente para la transmisión de información relacionada con asuntos laborales del usuario y/o asuntos de interés común que inciden en la buena marcha y en el mejoramiento de la armonía laboral del Hospital.
- Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

El sistema de correo electrónico puede ser utilizado para el intercambio de información, administración de libreta de direcciones, manejo de contactos, administración de agenda y el envío y recepción de documentos, relacionados con las responsabilidades institucionales. Las siguientes actividades están expresamente prohibidas dado que exponen el normal funcionamiento del servicio y su disponibilidad:

- Envío de mensajes desde el correo de un usuario con firma de otro.
- Intentos de acceso y/o accesos no autorizados a otra cuenta de correo.
- Intentos de acceso y/o accesos no autorizados a carpetas.
- Transmisión de mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización.
- Cadenas de mensajes que congestionen la red.
- Transmisión de mensajes obscenos.
- Cualquier actividad no ética que afecte al Hospital.

Recomendaciones a tener en cuenta para el manejo eficiente del servicio:

Para evitar la pérdida de información se recomienda tener una buena disciplina para la organización de los mensajes en la medida en que se reciban. Utilice las Carpetas Personales para Guardar los mensajes de mayor importancia y que necesita utilizar en cualquier momento.

- Evitar al máximo los archivos adjuntos. En lo posible incluya el contenido del mensaje directamente en el área de edición del mensaje, en lugar de hacerlo en documentos que adjunta al mismo
- Eliminar elementos antiguos y que ya no se necesiten.
- Trate de organizar los mensajes recibidos de tal manera que solo conserve la información que le interesa y que está vigente.
- No deje congestionar su “Bandeja de Entrada”, ya que mientras más mensajes tenga, más difícil identificar lo útil de lo inservible.
- Trate de deshacerse de lo inservible tan pronto como pierda vigencia, no deje esta tarea pendiente en ninguna de las carpetas que hacen parte del buzón como: Bandeja de Entrada, Calendario, Contactos, Diario, Tareas, Bandeja de Salida, Elementos Eliminados, Elementos Enviados y Notas.

El envío de información institucional debe ser realizado exclusivamente desde la cuenta de correo bajo el dominio @psiquiatricocali.gov.co y cumpliendo con las normas para el uso del correo electrónico institucional del Hospital psiquiátrico universitario del valle E.S.E.

## GESTION DE ACCESO DE USUARIOS

La gestión de acceso de usuarios a aplicativos institucionales, bases de datos, herramientas en línea, inicio de sesión de Windows y recursos compartidos, es realizada por el área de TI del Hospital, quien es el responsable de velar por la confidencialidad y disponibilidad de los activos de información institucional mencionados anteriormente, es importante tener en cuenta lo siguiente:

- Entregar a los usuarios un detalle escrito de sus derechos de acceso. (Actas de Entrega de Servicio con responsabilidades de uso).
- Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del Hospital o sufrieron la pérdida/robo de sus credenciales de acceso.
- Efectuar revisiones periódicas con el objeto de: cancelar identificadores y cuentas de usuario redundantes inhabilitar cuentas inactivas por más de un periodo determinado (no mayor a 60 días) eliminar cuentas inactivas por más de un periodo determinado (no mayor a 120 días)
- En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
- Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o terceros, que prestan un servicio intentan accesos no autorizados.
- Para telemedicina se establecen los protocolos de seguridad entre las entidades de tal manera que se garantice la confidencialidad de la información compartida entre el Centro de Referencia y la Entidad Remisora.

Es importante tener en cuenta que el acceso a aplicativos institucionales, bases de datos, herramientas en línea, inicio de sesión de Windows y recursos compartidos, debe ser autorizado por escrito por el área de Talento Humano o por el jefe inmediato.

## ADMINISTRACION DE PRIVILEGIOS

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- Identificar los privilegios asociados a cada producto del sistema, por ej: sistema operativo, de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados.
- Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Establecer un período de vigencia para el mantenimiento de los privilegios, con base en la utilización que se le dará a los mismos, luego del cual los mismos deben ser revocados.
- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios innecesarios a los usuarios.
- Los Propietarios de Información deben ser los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual debe ser supervisado por el Responsable de Seguridad Informática.

## CLAVES DE ACCESO

Para los equipos donde se utilizan claves de acceso (password) para el ingreso del usuario a diferentes ambientes de trabajo tenga en cuenta:

- Que el manejo de la(s) clave(s) implica responsabilidades sobre su uso.
- Siempre que ingrese o digite la clave de acceso en el sistema tenga especial cuidado de que no haya sido observada por otra(s) persona(s), si tiene dudas proceda a su cambio.
- La clave es personal e intransferible, manténgala siempre en secreto y no la dé a conocer a otros funcionarios
- No utilice claves prestadas o de personas ya retiradas del Hospital.
- Cambie la(s) clave(s) periódicamente.
- La clave del personal retirado del Hospital debe eliminarse y no reasignarse a otro empleado.
- Cierre la sesión de trabajo de la terminal o microcomputador cuando se vaya a almorzar, se retire temporalmente de su sitio de trabajo y/o cuando se retire al finalizar su trabajo.
- Si usa claves de acceso en el computador, NO utilice claves fáciles de identificar o débiles, tales como: Nombres, apellidos, sobrenombres, códigos de terminal o estación, iníciales de nombres y apellidos, fechas, nombres de archivos.
- Si posee claves de acceso o diferentes sistemas, no utilice la misma para todos, use una diferente para cada aplicativo.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Si suspende temporalmente el trabajo, sale a almorzar o a finalizar el día y deja activa la clave de acceso en su estación de trabajo o microcomputador personal, facilita que toda persona la pueda utilizar inadecuadamente, quedando la operación registrada como si hubiera sido realizada por usted.
- El acceso a los equipos debe ser solo permitido a personal autorizado y calificado.
- Para el módulo de Telemedicina, igual se asigna una clave de acceso que permite el ingreso a la herramienta de mediación para extraer la información requerida por la Entidad Remisora.

## SEGURIDAD FISICA Y DEL ENTORNO

Todos los equipos que hacen parte de la infraestructura tecnológica del HDPUV tales como servidores, equipos de comunicaciones, centros de cableado, UPS, subestaciones eléctricas, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, agua, polvo, vandalismo, entre otros.

Cualquier persona “interna o externa”, que ingresa a la entidad con equipos de cómputo portátiles o de escritorio, debe realizar el respectivo registro de los equipos en los puestos de vigilancia.

### Seguridad centro de datos

- El acceso a la central de datos del Hospital Psiquiátrico universitario del valle E.S.E, es restringido y solo puede ingresar personal autorizado por el área de TI o por la gerencia, para procesos específicos como mantenimiento de equipos por personal especializado o servicio de aseo, se realizara en compañía de un responsable del área de TI.
- Las áreas seguras, dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo y áreas de recepción y entrega de correspondencia, deberán contar con mecanismos de protección física y ambiental, y controles de acceso que pueden ser mediante tarjeta de proximidad o puertas con cerradura.
- En las áreas seguras, bajo ninguna circunstancia se podrá fumar, comer o beber.
- Las actividades de limpieza en las áreas seguras deberán ser controladas y supervisadas por un Colaborador del proceso. El personal de limpieza deberá ser instruido acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohibirá el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

### Ubicación y Protección de los equipos

La infraestructura tecnológica (Hardware, software y comunicaciones) deberá contar con medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

### Cuidado del equipo

- No fume, ni consuma alimentos y/o bebidas cerca de los equipos de cómputo, y periféricos.
- Evite instalarlo cerca de las ventanas, en sitios húmedos, poco ventilados y/o expuestos a los rayos del sol.
- El ruido que producen algunos aparatos eléctricos distorsionan la información. Evite instalar estos equipos cerca del computador.

- La electricidad estática puede ocasionar daños a los componentes electrónicos de los equipos; para ello es aconsejable que antes de iniciar sus labores en el computador toque cualquier elemento metálico para descargar dicha electricidad.
- Si el equipo de cómputo no está conectado a un estabilizador de voltaje y hay tormenta, apague y desconecte el equipo.
- Cuando el equipo se moje no lo encienda, si está encendido apague y desconéctelo inmediatamente.
- Si traslada o mueve un equipo de cómputo que se encuentre enchufado y encendido, se puede dañar físicamente. Antes de hacerlo apáguelo y desconéctelo.
- Cuide el teclado del equipo de Cómputo. Es un dispositivo que se puede dañar fácilmente, si es golpeado, maltratado o rayado.
- Si el equipo está encendido, conectar o desconectar la impresora, modem y/o mouse, puede ocasionar cortos circuitos en los componentes electrónicos internos del equipo. Apáguelo mientras hace conexiones o desconexiones.
- Cuando se coloca la impresora demasiado cerca al computador, puede afectar el funcionamiento del equipo.
- Mantenga las rejillas del computador destapadas cuando este encendido. El equipo debe tener una adecuada ventilación para su correcto funcionamiento.
- Si su computador es portátil la falta de uso de la batería por períodos superiores a un mes le genera deterioros irremediables al equipo.
- Cuide su computador portátil y/o mouse, éstos tienen mucho “amigos” dado su tamaño pueden ser hurtados fácilmente de las dependencias del Hospital; por esto es necesario, que una vez termine su uso, lo guarde en un lugar seguro, preferiblemente con llave.
- Mantener su equipo limpio y aseado en sus partes exteriores, no use líquidos o elementos extraños para limpiar su monitor.

**Seguridad de los equipos fuera de las instalaciones**

- Los equipos portátiles que contengan información clasificada como CONFIDENCIAL o RESERVADA, deberán ser controlados mediante el cifrado de la información almacenada en sus discos duros, utilizando la herramienta definida por el Grupo de Trabajo de Infraestructura y Soporte de TI.
- Los equipos portátiles no deberán dejarse a la vista en el interior de los vehículos. En casos de viaje siempre se deberán llevar como equipaje de mano.
- En caso de pérdida o robo de un equipo portátil se deberá informar inmediatamente a la Subgerencia administrativa y se deberá poner la denuncia ante la autoridad competente y allegar copia de la misma.
- Los equipos portátiles deben estar asegurados (cuando los equipos estén desatendidos) con una guaya, dentro o fuera de las instalaciones del HDPUV
- Los puertos de transmisión y recepción de infrarrojo y “Bluetooth” deberán estar deshabilitados.
- Cuando un equipo de cómputo deba retirarse de las instalaciones del Hospital Psiquiátrico universitario del valle E.S.E se deberá utilizar el formato y procedimiento correspondiente.

**Seguridad en la reutilización o eliminación de los equipos**

- Cuando un equipo de cómputo sea reasignado o dado de baja, se deberá realizar una copia de respaldo de la información que se encuentre almacenada. Luego el equipo deberá ser sometido a un proceso de

eliminación segura de la información almacenada y del software instalado, con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma.

**Escritorio limpio y pantalla limpia**

- El personal del HDPUV debe conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- El personal del Hospital Psiquiátrico universitario del valle E.S.E, debe bloquear la pantalla o cerrar la sesión de su computador, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo. Al finalizar sus actividades diarias, deberán salir de todas las aplicaciones y apagar la estación de trabajo.
- Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deberá reutilizar papel que contenga información CONFIDENCIAL.
- En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar la información CONFIDENCIAL protegida bajo llave. Esto incluye: documentos impresos, CD´s, dispositivos de almacenamiento USB y medios removibles en general.

## SEGURIDAD DE LAS OPERACIONES

**Procedimientos de operación documental**

Se debe contar con procedimientos, registros e instructivos de trabajo debidamente documentados y actualizados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica del HDPUV. Cada procedimiento debe tener un responsable para su definición y mantenimiento y debe garantizar la disponibilidad del mismo.

**Control de cambios**

Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado adecuadamente, y debe ser sometido a una evaluación que permita identificar los riesgos, que pueden afectar la operación del negocio de acuerdo con los lineamientos establecidos.

Los cambios estructurales que se planteen realizar sobre las plataformas críticas deben ser revisados por el Comité de desempeño institucional, el cual debe establecer los requerimientos de seguridad necesarios conforme a las políticas establecidas por el Hospital psiquiátrico universitario del valle E.S.E, que tengan como fin evitar un impacto adverso en las operaciones del negocio.

La Gestión de Cambios debe contener como mínimo la identificación, justificación y evidencia de los cambios que se vayan a realizar sobre la infraestructura tecnológica, el alcance, autorización, el plan de trabajo para la definición de pruebas funcionales, responsabilidades definidas, la evaluación apropiada sobre el impacto potencial que estos pueden generar, un plan alternativo para abortar cambios no satisfactorios (Rollback), eventos imprevistos y cualquier otro aspecto que se considere importante por los responsables del cambio.

**Gestión de capacidad**

Asegurar la disponibilidad de los recursos necesarios para la operatividad de los sistemas de información contemplando necesidades actuales y futuras.

- El Grupo de TI definirá las actividades específicas para monitorear, proyectar y asegurar la capacidad de la infraestructura de procesamiento de información, con el objeto de garantizar el buen desempeño de los recursos tecnológicos necesarios para la ejecución de los procesos.
- La capacidad de los recursos debe ser ajustada periódicamente para garantizar la disponibilidad y eficiencia requerida de acuerdo a las necesidades actuales y futuras del Hospital psiquiátrico universitario del valle E.S.E.
- El monitoreo y gestión de la capacidad debe hacerse considerando la criticidad de la información y los sistemas que soportan, para lo cual se utilizará la criticidad determinada durante el levantamiento del inventario de activos de información. Aquellos componentes que soporten activos con criticidad alta siempre deben estar sujetos a monitoreo y gestión de capacidad.
- Se debe tomar las acciones adecuadas para minimizar o evitar la dependencia de elementos o personas claves para la prestación de un servicio. Dentro de las acciones se deben contemplar: redundancia de elementos, arquitecturas de contingencia o de alta disponibilidad, técnicas de gestión de conocimiento sobre la operatividad de la infraestructura, etc.
- Los umbrales de óptimos de capacidad se puede obtener incrementando la capacidad o reduciendo la demanda, lo cual incluye las siguientes posibles acciones que deberán ser llevadas a cabo por el Grupo de TI: Eliminación de información obsoleta, supresión de aplicaciones, bases de datos o ambientes en desuso, optimización de procesos o tareas automáticas, afinamiento de consultas a bases de datos o lógica de aplicaciones, restricción de ancho de banda para servicios con alto consumo de capacidad que no sean misionales, etc.

**Ambientes de desarrollo, pruebas y producción**

Para la gestión de los sistemas de información en El Hospital Departamental Psiquiátrico Universitario del Valle ESE la Entidad cuenta con ambientes de:

- Desarrollo
- Pruebas
- Producción.

**Ambiente de Desarrollo:** Aunque no se cuenta con un proceso de desarrollo de software como tal, este ambiente comprende el entorno de desarrollo de aplicaciones, herramientas, reportes e informes. A este ambiente, puede acceder solo personal autorizado y tienen los privilegios para crear, modificar y eliminar los artefactos que componen o compondrán el sistema; deben estar restringidos los accesos a los usuarios finales o cualquier otro usuario diferente al equipo de desarrollo.

Estas prácticas, aplican tanto para los repositorios de datos como para servidores de aplicación.

**Ambiente de Pruebas:** El ambiente de pruebas es utilizado para desplegar el sistema una vez se tenga desarrollada una nueva funcionalidad y se encuentre en condiciones de ser probada por el usuario final, esto como paso previo a su puesta en producción.

Se establece como condición para el despliegue en este ambiente, la validación por parte del equipo de desarrollo de la inexistencia de errores de codificación, así como el manejo de excepciones no previstas que se puedan presentar.

El entorno de pruebas debe ser lo más cercano en el aspecto técnico al ambiente de producción, de manera que se pueda desplegar en producción la misma configuración y obtener en las pruebas los datos de rendimiento esperados en producción así como detectar en este entorno los posibles problemas.

Cada desarrollo puede contar con uno o más ambientes de pruebas, de tal forma que se puedan tener más de una versión del sistema para pruebas. El ambiente se compone tanto del repositorio de datos, datos de pruebas así como los componentes de software.

**Ambiente de Producción:** En este entorno se despliegan los componentes de software ejecutables que pasan a ser utilizados por los usuarios finales. Solo se pasan a este ambiente los desarrollos que hayan superado la fase de pruebas, para esto el área usuaria o su representante deberá formalizar el paso a producción con una aprobación del desarrollo.

Para realizar el despliegue en producción de los componentes compilados o ejecutables se tomarán las versiones probadas y aceptadas del ambiente de pruebas.

Para el módulo de Telemedicina, como parte de los componentes de software, se permite el despliegue de la información a través de la seguridad por roles y permisos establecidos.

El Grupo de TI, es el responsable de la administración de la aplicación o el sistema en este ambiente, para cada uno de los módulos, incluyendo el de Telemedicina.

**Protección contra códigos maliciosos**

El Hospital ha establecido medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos, las cuales se describen a continuación:

- Toda la infraestructura de procesamiento de información debe contar con un sistema de detección/prevención de intrusos, sistema anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos. Así mismo, se restringirá la ejecución de aplicaciones y se mantendrá instalado y actualizado un sistema de antivirus, en todas las estaciones de trabajo y servidores del HDPUV.
- Se restringirá la ejecución de código automático, aplicando políticas en el sistema operacional, en el software de navegación de cada máquina y en el sistema de control de navegación.
- Los usuarios de los servicios TIC del HDPUV, son responsables de la utilización de programas antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos y/o removibles y/o los archivos y/o el correo electrónico que esté autorizado a emplear.

- El HDPUV contará permanentemente con los programas antivirus de protección a nivel de red y de estaciones de trabajo, contra virus y/o código malicioso, el servicio será administrado por el Grupo de TI.
- Los programas antivirus deben ser instalados por el Grupo de TI en los equipos centralizados de procesamiento y en las estaciones de trabajo que estén activados durante su uso. Las instalaciones nuevas de estaciones de trabajo o servidores que sirvan al propósito operativo del Hospital Departamental Psiquiátrico Universitario del Valle ESE, deben contar con un programa de antivirus previo a la instalación de cualquier otro programa sobre el sistema operativo.
- Se debe actualizar periódicamente las versiones de los componentes de los diferentes sistemas de seguridad operativos, incluidos, motores de detección, bases de datos de firmas, software de gestión en el lado cliente y servidor, etc.
- Los Colaboradores del Hospital Departamental Psiquiátrico Universitario del Valle ESE, pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los Colaboradores siempre podrán consultar al Grupo de TI sobre el tratamiento que debe darse en caso de sospecha de malware.
- Los Colaboradores del Hospital Departamental Psiquiátrico Universitario del Valle ESE, no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus y/o de detección de código malicioso, en los equipos o sistemas en que estén instalados.
- El único servicio de antivirus autorizado en del Hospital Departamental Psiquiátrico Universitario del Valle ESE, es el asignado directamente por el Grupo de TI, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.
- El Grupo de TI del Hospital Departamental Psiquiátrico Universitario del Valle ESE, es el responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los computadores y/o equipos informáticos
- El Grupo de TI del Hospital Departamental Psiquiátrico Universitario del Valle ESE, se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, tramitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.
- El Grupo de TI del Hospital Departamental Psiquiátrico Universitario del Valle ESE, se reserva el derecho de filtrar los contenidos que se trasmitan en la red para evitar amenazas de virus.

**Copias de respaldo (Backups)**

El Hospital Departamental Psiquiátrico Universitario del Valle ESE, debe Proporcionar medidas de respaldo adecuadas para asegurar que la información esencial y el software asociado se puedan recuperar después de una falla. Por lo anterior se debe tener en cuenta:

- La información de cada sistema de información debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, CD, DVD, de acuerdo a su nivel de criticidad identificada en el inventario de activos de información. La información con criticidad mayor debe estar sujeta a una mayor frecuencia de tareas de respaldo. Los medios se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo, incendio, humedad, y mecanismos de control de acceso físico.
- Se deben realizar pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

- El Custodio de cada activo de información es el responsable de verificar que los backups se ejecuten correctamente y de acuerdo al tipo y frecuencia acordados.
- El administrador de las Bases de Datos y el Oficial de Seguridad de la Información son los responsables de definir la frecuencia de respaldo, el tipo, el medio de almacenamiento y los requerimientos de seguridad de la información, de acuerdo a las disposiciones definidas en la Guía de Clasificación y Etiquetado de la Información. Estos aspectos de configuración se deben registrar en el Formato de Definición de Backups de Información.
- Las copias de respaldo se deben guardar con el objetivo de restaurar el sistema luego de una infección de virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, contaminación de los datos y por requerimientos legales.
- Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica, el responsable de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
- Es responsabilidad de cada colaborador realizar periódicamente una copia de seguridad de la información almacenada en el disco duro del equipo que le fue asignado, para ello solicitara al grupo de TI los medios necesarios, los cuales entregara para que sean resguardados de acuerdo con las medidas de protección y seguridad física apropiados.

**Registro y seguimiento**

Asegurar el registro de los eventos y las operaciones realizadas sobre los sistemas de información del Hospital Departamental Psiquiátrico Universitario del Valle ESE, permitirá contar con evidencia necesaria para la gestión de incidentes de seguridad de la información.

**Registro de eventos**

- Todos los accesos de usuarios a los sistemas, redes de datos y aplicaciones del Hospital Departamental Psiquiátrico Universitario del Valle ESE, deben ser registrados. Para ello se debe habilitar los log de eventos requeridos y deben ser revisados con regularidad.
- La información generada por los logs o eventos monitoreados, se deben proteger y guardar evitando el acceso o manipulación no autorizada.

**Registro del administrador y del operador**

- Todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información del Hospital Departamental Psiquiátrico Universitario del Valle ESE deberán estar debidamente registradas.
- Los administradores de la infraestructura de procesamiento de información tendrán asignada una cuenta de usuario única, a través de la cual se realizarán las actividades de administración.

**Gestión de vulnerabilidades técnicas**

Gestionar las vulnerabilidades técnicas asociadas a la plataforma tecnológica del Hospital Departamental Psiquiátrico Universitario del Valle ESE, reducirá la posibilidad de existencia de amenazas informáticas, para ello el grupo de TI, se encargará de identificar las vulnerabilidades técnicas de la plataforma tecnológica, basado en diferentes estrategias:

- Monitoreo sobre la plataforma tecnológica.
- Reportes de fabricantes y proveedores.
- Servicios de seguridad informática contratados.
- Reportes de usuarios internos y externos.

Las salvaguardas a implementar para minimizar el riesgo ante el hallazgo de vulnerabilidades técnicas, serán comunicadas a cada uno de los responsables de los activos de información al igual que su implementación o tratamiento.

## SEGURIDA DE LAS COMUNICACIONES

### Gestión de seguridad de las redes

Se deben finir los controles necesarios para proteger la información del Hospital Departamental Psiquiátrico Universitario del Valle ESE, transportada a través de la red interna y a través de la red de conexión hacia terceros, por lo cual:

- Se establecerá un conjunto de controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de garantizar el buen uso de los mismos y mantener los niveles de seguridad establecidos.
- El Hospital Departamental Psiquiátrico Universitario del Valle ESE, proporciona a los Colaboradores todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones/actividades para las cuales fueron contratados, por tal motivo no se permite conectar a las estaciones de trabajo o a los puntos de acceso corporativos, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por el Grupo de TI.
- El acceso remoto a la red de datos del Hospital Departamental Psiquiátrico Universitario del Valle ESE, se permitirá de acuerdo a las políticas institucionales.

### Transferencia de información

Se debe Proteger la información del Hospital Departamental Psiquiátrico Universitario del Valle ESE que es intercambiada o transferida en razón de las actividades propias de la Entidad, para ello se tiene en cuenta:

- Se debe firmar Acuerdos de Confidencialidad con Colaboradores y terceros que por diferentes razones requieran conocer o intercambiar información no PUBLICA que se encuentre en custodia del Hospital Departamental Psiquiátrico Universitario del Valle ESE.
- Se debe considerar la normatividad aplicable para el intercambio de información no PÚBLICA con terceros. Específicamente se debe considerar el mecanismo, por ejemplo: Convenios Interadministrativos, definido por la Oficina Asesora Jurídica para formalizar los intercambios de información.

### Acuerdo de confidencialidad

- Todos los Colaboradores deben firmar el Formato “Acuerdo de Confidencialidad de la Información” definido por el Hospital Departamental Psiquiátrico Universitario del Valle ESE, y este debe ser parte integral de cada uno de los contratos o de la carpeta de documentos de posesión de los funcionarios.
- El encargado de asegurar el trámite de firma, custodia y mantenimiento de los acuerdos, será el área de Talento Humano.

- Los formatos de Acuerdos de Confidencialidad, serán revisados y aprobados por el Grupo de TI.

## ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Se debe considerar la seguridad de la información como un componente transversal en la totalidad del ciclo de desarrollo de sistemas de información.

Requisitos de seguridad de los sistemas de información

- La construcción y modificación de sistemas de información o la implementación de nuevos módulos a los sistemas de información misionales o de apoyo, desarrollados al interior de la entidad o contratados con terceras partes, deben contemplar un completo análisis de requerimientos en cuanto a seguridad de la información, análisis de riesgos y posibles escenarios de riesgos asociando los controles respectivos para la mitigación de los mismos.
- Todas las solicitudes para compra, actualización y/o desarrollo de software deberán ser direccionadas, orientadas, con el acompañamiento y bajo los estándares definidos por el Grupo de TI.
- Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.
- Únicamente está permitido el uso de software autorizado por el Grupo de Trabajo de TI.
- El acceso de los usuarios a los sistemas de información misionales y de apoyo se restringirá mediante autenticación por usuario y clave de acceso, para cada usuario se delimitaran los perfiles de acceso y procesamiento de información según las necesidades.
- La definición de los tipos de perfiles será determinada por los administradores de los sistemas de información de cada uno de los procesos.

## RELACION CON LOS PROVEEDORES

Todos los proveedores que por actividades internas tengan un contrato con el Hospital Departamental Psiquiátrico Universitario del Valle ESE, deberán acogerse a los siguientes lineamientos:

- En los Contratos o Acuerdos con terceras partes y que implique un intercambio, uso o procesamiento de información de la Entidad, se debe contemplar la posibilidad de celebrar Acuerdos de Confidencialidad en el manejo de la información. Estos acuerdos deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio. El contrato o acuerdo debe definir claramente el tipo de información que intercambiaran las partes.
- Los proveedores deberán hacer reporte de las debilidades de seguridad que puedan encontrar durante la ejecución del contrato con el Hospital Departamental Psiquiátrico Universitario del Valle ESE.

## GESTION DE INCIDENTES

El Hospital Departamental Psiquiátrico Universitario del Valle ESE, debe gestionar adecuadamente los incidentes de seguridad de la información reportados, para ello es importante tener en cuenta:

- Es responsabilidad de cada uno de los Colaboradores de la entidad y terceras partes, reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información; esto con el fin de proceder con el tratamiento respectivo.

- Todos los incidentes de seguridad reportados, se les debe dar el tratamiento y seguimiento respectivo, realizando el respectivo trámite ante las instancias correspondientes.
- Se deben implementar herramientas para el registro y seguimiento de los incidentes reportados.

## 8. 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.

| Actualizado por: | Revisado por: | Aprobado por: |
|---|---|---|
| *ORIGINAL CON FIRMA* | *ORIGINAL CON FIRMA* | *ORIGINAL CON FIRMA* |
| **Marcela Martinez Turriago**<br>Profesional Universitario Sistemas | **Berenice Rivera Trujillo**<br>Líder ISC | **Gloria Elizabeth Ruiz Garcia**<br>Subgerente Administrativa y Financiera |
| **Fecha:** 13 de diciembre de 2.021 | **Fecha:** 14 de diciembre de 2.021 | **Fecha:** 15 de diciembre de 2.021 |

| 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 |