POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCIÓN

La Información es uno de los activos más importantes para una organización y, por tanto, debe protegerse adecuadamente cualquiera que sea la forma que tome, o los medios por los que se transmita, almacene o procese.

Hoy por hoy, muchas organizaciones nacionales e internacionales desarrollan políticas de seguridad que rigen el uso adecuado de la tecnología y hacen recomendaciones para aprovechar sus ventajas y evitar su uso indebido; previniendo así problemas en el uso de los bienes y servicios informáticos de las entidades.

La ESE Hospital Departamental San Antonio De Padua es consciente de la importancia y del valor de su información, ha desarrollado la siguiente política de seguridad de la información a implementar en la política de seguridad de la información, y quiere dejar constancia de su apoyo, aprobación y asignación de los recursos necesarios para su ejecución a que sea distribuida a todo el personal junto con su documentación asociada, para que la conozca y cumpla.

JUSTIFICACIÓN

La ESE Hospital Departamental San Antonio de Padua, ha establecido un marco de estrategias de seguridad de la información y de tecnologías de la información, alineadas con el PETI, a través del cual se establece como finalidad última mejorar continuamente el servicio a los usuarios y velar por la mejora en la seguridad de la información, formulándose como objetivo general la creación de un servicio más innovador, receptivo, eficiente y de mínimo riesgo, que facilite la actividad de los usuarios, asegurando la disponibilidad del mismo y mejorando el grado de satisfacción de éstos. Este objetivo general sirve de marco de referencia para establecer objetivos concretos de seguridad de la información y servicios TI.

Las distintas áreas y departamentos de la ESE, contemplarán la seguridad desde el mismo momento en que se realiza un tratamiento de datos de carácter personal ("privacy by design"), aplicando para éstos, y para los ya existentes, las medidas de seguridad establecidas, garantizando así su disponibilidad, autenticidad, integridad y confidencialidad ("privacy by default").

ALCANCE

La aplicación del Manual de Políticas de Seguridad Informática, de la ESE Hospital Departamental San Antonio de Padua, acogerá a todos los funcionarios, de planta y contratistas, asistenciales y administrativos que hagan uso de herramientas informáticas y/o estén conectados a la red de la institución.

La Política de Seguridad que se implemente requiere un alto compromiso por parte de cada uno de los funcionarios de la institución, capacidad para detectar fallas y anomalías y el establecimiento de controles continuos para renovar y actualizar dicha política en función del ambiente dinámico, cambiante y evolutivo que nos rodea.

OBJETIVO GENERAL

Elaborar un Manual de Política de Seguridad Informática para la ESE Hospital Departamental San Antonio de Padua, que cree una cultura organizacional de buenas prácticas en el aspecto computacional y fortalecer la protección física y lógica de los activos informáticos de la entidad.

OBJETIVOS ESPECIFICOS

- Establecer normas de cuidado de equipos, periféricos y demás dispositivos físicos.

- Sensibilizar a todos los usuarios de la ESE Hospital Departamental San Antonio de Padua acerca de la necesidad de poner en práctica el Presente Manual.

- Crear mecanismos de protección a partir de la toma de precauciones, básicas pero fundamentales a la hora de utilizar los recursos de red tales como internet o todos aquellos Software Pertenecientes a la Institución.

GLOSARIO

Activo: Conjunto de bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la institución. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administración Remota: Forma de administrar (manejar o controlar) equipos informáticos o servicios físicamente separados.

Amenaza: Evento que puede desencadenar un incidente en la institución, produciendo daños materiales o pérdidas inmateriales en sus activos.

Antivirus: Son una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos.

Área Crítica: Área física donde se encuentra instalado el equipo de cómputo y telecomunicaciones que requiere de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación de la ESE.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Bases de Datos: Conjunto de datos interrelacionados y de programas para accederlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

Cadena: Mensaje que intenta inducir al receptor a realizar algún número de copias de un mensaje de correo para luego pasarlas a uno o más receptores nuevos.

CD (Disco compacto): Soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos).

Comando: Instrucción u orden que el usuario proporciona a un sistema informático, a través de una línea de texto basada en palabras clave.

Confidencialidad: Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.

Control de Acceso: Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria. Característica o técnica en un sistema de comunicaciones que permite o niega el uso de algunos componentes o algunas de sus funciones.

Crack: Programa que realiza una modificación permanente o temporal sobre otro en su código, para obviar una limitación o candado impuesto a propósito por el programador original. Algunas legislaciones consideran este tipo de programas ilegales por facilitar la vulneración de los derechos de autor de códigos no libres o comerciales.

Dirección IP: Es una etiqueta numérica que identifica, de manera lógica y jerárquica, una interface de conexión de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol).

DVD (Disco Versátil Digital): Dispositivo de almacenamiento óptico en forma de disco, similar al CD, pero de mayor capacidad de almacenamiento (4.7 GB).

Equipo de Cómputo: Dispositivo con la capacidad de aceptar y procesar información, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

Equipo de Telecomunicaciones: Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

Estabilizador: Dispositivo para la toma de la tensión de la red eléctrica que alimenta al computador y a la red.

Filtro de contenidos web: Herramienta informática que bloquea o permite el acceso a determinados sitios de internet.

FTP (File Transfer Protocol): Protocolo y software que permite la transferencia de archivos entre máquinas conectadas a una red.

Hacking: Acción de infiltrarse ilegalmente a sistemas informáticos y redes de telecomunicación con fines delictivos.

Hardware: Partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

HOAX: (Engaño, mentira, patraña). Mensaje de e-mail con contenido falso o engañoso generalmente proveniente en forma de cadena.

Integridad: Proteger la información de alteraciones no autorizadas por la institución.

Internet: Red de redes de computadoras conectadas a nivel mundial, se emplea para el intercambio de información, el acceso a bases de datos, entre otros fines.

Intranet: Red de computadoras privadas que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información, datos y sistemas operativos.

Keygen: Programa informático, generalmente ilegal, que al ejecutarse genera un código para que un determinado programa software de pago en su versión de prueba pueda ofrecer los contenidos completos del mismo.

Mantenimiento: Acciones que tienen como objetivo mantener un artículo o restaurarlo a un estado original.

Memoria USB: Dispositivo de almacenamiento masivo que utiliza memoria flash para guardar la información que se puede requerir.

Módulo: Parte de un programa de computador.

Periférico: Dispositivos externos que se conectan al computador.

Red: Conjunto de computadoras y elementos interconectados que permiten una comunicación entre sí y forman parte de un mismo ambiente.

Servicio: Conjunto de aplicativos, programas informáticos o sitios web que apoyan la labor administrativa de la institución, sobre los procesos diarios que demanden información o comunicación en la misma.

Software: Conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Software espía: Controla el uso de la computadora sin el conocimiento o consentimiento del usuario. Los software espía pueden grabar la secuencia de pulsación de teclas, el historial de navegación, contraseñas y cualquier otra información confidencial y privada, y enviar estos datos a un tercero vía Internet.

Soporte Técnico: Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores o equipo de oficina dentro de la institución.

SPAM: Mensajes no solicitados, no deseados o de remitente no conocido.

UPS (Uninterrupted Power System): Sistema de Potencia Ininterrumpida, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.

Usuario: Cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga algún tipo de vinculación con la ESE Hospital Departamental San Antonio de Padua.

Virus Informático: Programa software que altera el normal funcionamiento del computador, sin el permiso o el conocimiento del usuario.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

BASE LEGAL Y NORMATIVIDAD

Ley Estatutaria 15 81 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 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, 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 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 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo

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 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.

Ley 1150 DE 2007: Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.

BS 7799-3:2006: Proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI).

NTC 27001:2006: Sistema de Gestión de Seguridad de la Información (SGSI). En 2005, con más de 1700 empresas certificadas en BS7799-2, ISO publicó este esquema como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799 y esta última norma se denomina ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido así como el año de publicación formal de revisión.

ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la Gestión de la Seguridad de la Información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma.

ISO/IEC 27001 2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

Ley 962 DE 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

Modelo Estándar de Control Interno MECI 1000:2005: Proporciona una estructura para el control de la estrategia, la gestión y la evaluación en las entidades, con el orientarlas hacia el cumplimiento de los objetivos institucionales y la contribución de estos a los fines esenciales del Estado Colombiano.

NTCGP1000:2004: Esta Norma establece los requisitos para la implementación de un sistema de gestión de la calidad aplicable a la rama ejecutiva del poder público y otras entidades prestadoras de servicio.

ISO/IEC TR 18044:2004: Ofrece asesoramiento y orientación sobre la Seguridad de la Información de Gestión de incidencias para los administradores de seguridad de la información y de los administradores de sistemas de información.

Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo

a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

VIGENCIA

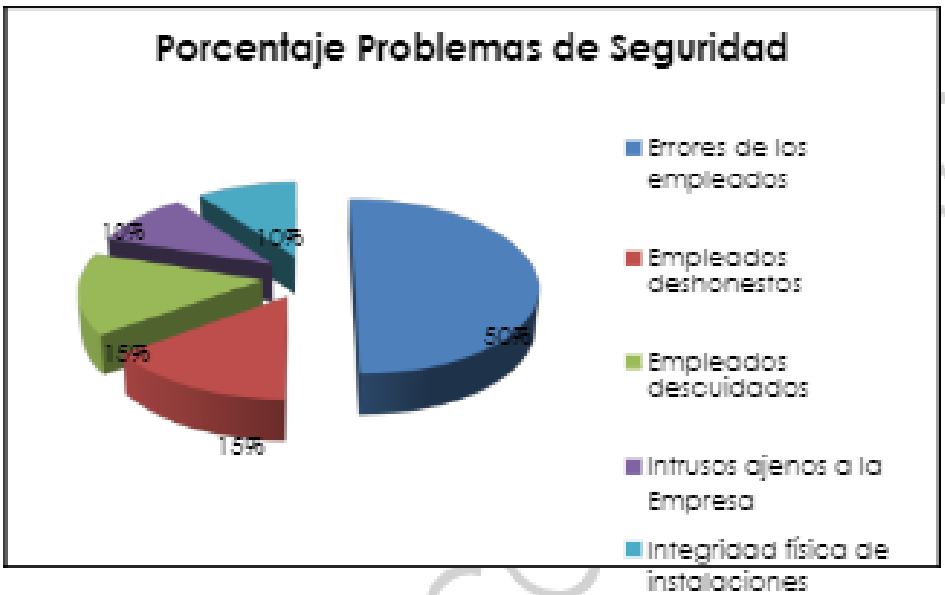
Este documento regirá a partir del momento en que mediante Acto Administrativo sea aprobado por la Gerencia, como documento técnico de seguridad informática, el cual deberá ser revisado y actualizado conforme a las exigencias y necesidades de la ESE Hospital Departamental San Antonio de Padua.

RIESGOS INFORMÁTICOS

La ISO 27001 (Organización Internacional de Estandarización) define el riesgo Informático como: "***La posibilidad que una amenaza se materialice, utilizando vulnerabilidad existente en un activo o grupos de activos, generándose así pérdidas o daños.***"

En una entidad, los riesgos informáticos, son latentes día a día y pueden afectar gravemente la seguridad y la estabilidad de los sistemas de información, estos pueden presentarse en diversas áreas como lo ilustra la identificación, valoración y seguimiento de riesgos por procesos, Matriz incluida y estipulada en el **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2019.**

Estudios muestran que los problemas de seguridad en sistemas basados en redes se distribuyen de la siguiente manera:



Se puede notar que el 80% de los problemas, son generados por los empleados de la organización, y, éstos se podrían tipificar en tres grandes grupos:

- Problemas por ignorancia
- Problemas por ociosidad
- Problemas por malicia

Entre estas razones, la ignorancia es la más fácil de manejar. Desarrollando tácticas de entrenamiento, capacitación y procedimientos formales e informales son fácilmente neutralizadas. Los usuarios, además, necesitan controles, que les recuerde cosas que ellos deberían conocer.

La ociosidad será siempre un riesgo latente pero, se encuentra que éste es un problema menor cuando los usuarios "chocan" con los límites que ponen los sistemas de seguridad.

La malicia, se debe combatir creando una cultura en la organización que aliente la lealtad de los empleados.

RESPONSABILIDADES DE LA OFICINA DE SISTEMAS DE INFORMACION

- Administrar y coordinar diariamente el proceso de Seguridad Informática de la ESE Hospital Departamental San Antonio de Padua. El Código único Disciplinario (Ley 734 de 2002) Art.34 Num.28. Establece:
  "Son deberes de todo servidor público: Controlar el cumplimiento de las finalidades, objetivos, políticas y programas que deban ser observados por los particulares cuando se les atribuyan funciones públicas."

- Ser el eje para todos los procesos de seguridad y ser capaz de guiar y aconsejar a los usuarios de la institución sobre cómo desarrollar procedimientos para la protección de los recursos.

- Desarrollar procedimientos de seguridad detallados que fortalezcan la política de seguridad informática institucional.

- Promover la creación y actualización de las políticas de seguridad informática, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.

- Atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.

- Establecer vínculos con otras oficinas de sistemas de otras empresas, capacitarse y actualizarse en temas de seguridad con el objetivo de ampliar sus conocimientos y aplicar soluciones a problemas de seguridad del entorno institucional.

QUE SON POLÍTICAS DE SEGURIDAD?

La seguridad informática es en sí mismo un concepto amplio y diverso que abarca numerosas derivadas. La seguridad se puede centrar en la prevención de ataques y situaciones de riesgo para los sistemas de una organización o hacerlo más en los mecanismos de mitigación de los efectos que un ataque pueda ocasionarle a una empresa o particular. Si tuviéramos que definir qué son las políticas de seguridad informática podríamos empezar negando aquello que no son, es decir, afirmar que no son una descripción técnica de mecanismos ni una suerte de código penal que sancione, y al mismo tiempo conduzca, la labor de los empleados. Por el contrario, sí que tienen que ver con una descripción amplia, basada en objetivos globales, de los bienes y valores que deseamos proteger y la motivación de dicho deseo. De seguridad de la información, están orientadas hacia la formación de buenos hábitos.

CLASIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Para efectos de comprensión y estructuración de este documento, la oficina de Sistemas de Información de la ESE Hospital Departamental San Antonio de Padua, ha clasificado las políticas de seguridad en los siguientes grupos:

- **Equipos**: Todo lo relacionado con el hardware, su uso y cuidado.
- **Usuarios**: Concerniente a las personas que utilizan los recursos informáticos de la institución.

- **Software**: los recursos lógicos tales como programas, aplicativos y demás.
- **Redes e Internet**: las medidas que se deben tomar a la hora de utilizar los recursos de telecomunicación.
- **Datos e Información**: Políticas que regulan la manipulación, transporte y almacenamiento de la información de la institución.
- **Administración de seguridad Informática**: Establece la forma en que la Oficina de Sistemas de Información gestiona la seguridad de la infraestructura informática de la ESE Hospital Departamental San Antonio de Padua.

POLITICAS DE SEGURIDAD DE EQUIPOS

La ley 734 de 2002 en su artículo 48, considera una falta gravísima lo siguiente: **"Artículo 48. Faltas gravísimas. Son faltas gravísimas las siguientes: Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas."**

Los equipos son la parte fundamental para el almacenamiento y gestión de la información, La función de la Oficina de Sistemas de Información es velar que los equipos funcionen adecuadamente y establecer medidas preventivas y correctivas

En caso de robo, incendio, desastres naturales, fallas eléctricas y cualquier otro factor que atente contra la infraestructura informática. Comprende las siguientes políticas:

1. Todo equipo de cómputo, periférico o accesorio que esté o sea conectado a la Red de la ESE Hospital Departamental San Antonio de Padua, sea propiedad o no de la institución debe de sujetarse a las normas

y procedimientos de instalación establecidos por la oficina de Sistemas de Información, de lo contrario no le será permitido conectar su equipo o dispositivo. Para los equipos que no sean propios de la ESE Hospital Departamental San Antonio de Padua, se debe diligenciar un formato donde su propietario asuma la total responsabilidad sobre su equipo mientras esté conectado a la red eléctrica y de datos de la institución, ya que esta no se hace responsable de daños físicos o lógicos que puedan sufrir los equipos o periféricos de terceros.

2. La oficina de Sistemas de Información tendrá registro de todos los equipos que son propiedad de la ESE Hospital Departamental San Antonio de Padua, Si se requiere hacer un traslado de computador, periférico o accesorio, debe contar con el consentimiento de la oficina de Sistemas de Información. Si el equipo necesita trasladarse en calidad de préstamo (periodos de horas o días), debe notificarse a la oficina de Sistemas de Información y diligenciar el formato correspondiente.

3. Cualquier equipo, periférico o accesorio de propiedad de la ESE Hospital Departamental San Antonio de Padua que necesite ser retirado de la Institución tendrá que autorizarlo la Oficina de Sistemas de Información.

4. Todo equipo de la Institución, debe estar ubicado en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales adecuadas, seguridad y estabilidad en la parte eléctrica, garantías que deben proporcionarse en conjunto con el área de mantenimiento de la ESE Hospital Departamental San Antonio de Padua En general, todos los equipos.

5. Periféricos y accesorios computacionales de la red de la ESE Hospital Departamental San Antonio de Padua deben estar lejos de dos factores principales: La luz directa del Sol y de humedades, filtraciones y demás medios que puedan hacer que el equipo tenga contacto con el agua.

6. Todo equipo o periférico perteneciente a la red de ESE Hospital Departamental San Antonio de Padua, deberá contar con un dispositivo de protección eléctrica, ya sea estabilizador de corriente o UPS, que resguarde al equipo ante un cambio brusco en la corriente eléctrica de la entidad o del sector donde se ubica. Por lo anterior:

. Todo equipo propiedad de la institución, y que no cuente con alguno de estos dispositivos de protección, no puede ponerse en funcionamiento. Si el funcionario conectara el equipo, será el directo responsable de los daños que puedan ocurrirle a este, y se le aplicará ley 734. Régimen Unico Disciplinario.

. En caso que se necesite poner en funcionamiento un equipo que no tenga UPS o estabilizador, podrá hacerse de manera temporal y con el acompañamiento de un funcionario de la oficina de Sistemas de Información.

7. Los usuarios responsables de los equipos en cada dependencia deberán dar cumplimiento con las normas y estándares de instalación con las que fue entregado el equipo, y deberán pedir aprobación de actualización o instalación de cualquier software, reubicación del equipo, reasignación, y todo aquello que implique cambios respecto a su instalación, asignación, función y misión original. Los equipos de cómputo no deben moverse o reubicarse sin la aprobación previa de la oficina de Sistemas de Información, que evaluará la viabilidad de dicho cambio.

8. La protección física y la limpieza externa de los equipos corresponde al funcionario de sistemas al que se le asigne la tarea, y la custodia y cuidado en el sitio de trabajo le corresponde al funcionario que lo manipula y quien debe notificar las eventualidades, tales como daños, pérdidas y demás en el menor tiempo posible a la oficina de Sistemas de Información de la ESE Hospital Departamental San Antonio de Padua, Está totalmente prohibido

el consumo o ubicación de alimentos cerca de los equipos e impresoras, así como pegar distintivos, calcomanías y demás.

En caso que ocurra un incidente producido por el derrame de algún tipo de alimentos sobre un equipo, periférico o accesorio, este debe apagarse y desconectarse de inmediato e informar oportunamente a la oficina de Sistemas de Información quien hará el mantenimiento necesario he informara a quien corresponda para que se tomen las medidas correctivas necesarias.

9. No se permite el uso de dispositivos de almacenamiento extraíble tales como memorias USB, nuevas tecnologías en los equipos de la ESE Hospital Departamental San Antonio de Padua, salvo en aquellos casos en donde por fuerza mayor se requiera y previamente evaluado y aprobado por la oficina de Sistemas de Información.

Para garantizar lo anterior, la oficina de Sistemas de Información bloquea los puertos USB (solamente para el uso de memorias), si algún usuario necesita que ese bloqueo sea levantado, deberá solicitarlo a la oficina de Sistemas de Información, que a su vez hará llegar la solicitud a la Gerencia para su evaluación y decisión. Esta medida aplica para funcionarios y contratista que laboren en la Institución y que de una u otra manera tengan acceso a los equipos del Hospital.

9. Toda instalación de equipo, mantenimiento o proceso de soporte técnico a nivel de hardware, sin importar su nivel de complejidad, debe ser única y exclusivamente realizado por personal de la oficina de Sistemas de Información de la ESE Hospital Departamental San Antonio de Padua. Bajo ningún concepto se autoriza que personal ajeno a la oficina de Sistemas de Información manipule los equipos de la ESE Hospital Departamental San Antonio de Padua.

10. Para solicitar servicio de mantenimiento a un equipo, periférico o accesorio, se debe diligenciar un formato anexo.

11. Los equipos de cómputo de la ESE Hospital Departamental San Antonio de Padua no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) bajo ninguna causa. (Ley 734). Está totalmente prohibido a los usuarios destapar o desarmar los equipos o impresoras bajo cualquier motivo, sin exclusión. El único personal autorizado para esta labor, es el de la oficina de Sistemas de Información. De detectarse que se está presentando esta conducta se informara y se tomaran las medidas correctivas necesarias.

12. No se puede dar mantenimiento o soporte técnico a nivel de hardware a un equipo de cómputo que no es propiedad de la ESE Hospital Departamental San Antonio de Padua.

13. Los funcionarios de La oficina de Sistemas de Información de ESE Hospital Departamental San Antonio de Padua son los únicos autorizados para manejar, mantener y velar por la integridad y seguridad de los servidores centrales de la institución, a su vez de mantener las claves de estos.

14. Los servidores centrales de la red de la ESE Hospital Departamental San Antonio de Padua debe estar ubicado en un lugar exclusivo, sin acceso de personas ajenas a la oficina de Sistemas de Información, y con las condiciones adecuadas de espacio, temperatura, iluminación, entre otras.

15. Los equipos propiedad del Hospital deben usarse solamente para las actividades propias de la ESE Hospital Departamental San Antonio de Padua, por lo tanto los usuarios no deben usarlos para asuntos personales. (Delito contra los bienes de la administración pública).

16. La adquisición de nueva infraestructura de procesamiento de la información (hardware, software, aplicaciones e instalaciones físicas) o la actualización de la existente, deberá ser autorizada por la Oficina de Sistemas de Información y el jefe de la oficina afectada.

17. Todo equipo que sea asignado a un funcionario o contratista, deberá ser entregado al responsable de este, en las mismas condiciones en que lo recibió, como parte de las actividades definidas en la terminación del contrato o cambio de cargo.

18. Todo equipo de cómputo que este asignado a áreas asistenciales y requiera ser retirado del servicio para mantenimiento, reparación, reubicación o reemplazo, debe previamente pasar por un proceso de desinfección en sitio, con el fin de prevenir posible contaminación.

POLITICAS DE SEGURIDAD DE USUARIOS

Los usuarios son las personas que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información. La oficina de Sistemas de Información establece normas que buscan reducir los riesgos a la información o infraestructura informática. Estas normas incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, protocolos y todo lo necesario que permita un buen nivel de seguridad informática.

Todos los funcionarios y contratistas, deberán cumplir con estos requerimientos de seguridad de la Información. Igualmente durante el proceso de vinculación deberán recibir inducción sobre lo establecido en este Documento y sobre la responsabilidad del cumplimiento de las políticas, procedimientos y estándares definidos por el Hospital.

La información almacenada en los equipos de cómputo del Hospital es propiedad de la ESE Hospital Departamental San Antonio de Padua y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad. No es permitido divulgar, alterar, borrar, eliminar información sin la debida autorización.

Toda información en formato electrónico o impreso del Hospital debe estar debidamente identificada mediante rótulos o etiquetas, lo que permitirá su identificación y clasificación. Con esto se alimenta el inventario y clasificación de los archivos de información.

Las claves o los permisos de acceso que les sean asignados a los funcionarios y/o contratista, son responsabilidad exclusiva de cada uno de ellos y no deben utilizar la identificación o contraseña de otro usuario, excepto cuando los funcionarios de Sistemas la soliciten para la reparación o el mantenimiento de algún servicio o equipo.

1. Los permisos a usuarios son personales e intransferibles y serán acordes a las funciones que desempeñen y no deberán tener permisos adicionales a estos. Estos permisos se conceden a solicitud escrita del jefe de la Oficina quien debe velar por su adecuado manejo.

2. Los usuarios deben renovar periódicamente su clave de acceso al sistema, esto deben solicitarlo a la oficina de Sistemas de Información quienes le facilitarán el acceso y lo acompañarán en el proceso. Está totalmente prohibido: El intento o violación de los controles de seguridad establecidos; El uso sin autorización de los activos informáticos; El uso no autorizado o impropio de la conexión al
Sistema; el uso indebido de la las contraseñas, firmas, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma

3. El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones o instalaciones realizados por él que no fueran informadas o consultadas a la oficina de Sistemas de Información de ESE Hospital Departamental San Antonio de Padua.

4. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario. Si detectan actividades irregulares con su código o número de identificación, tienen solicitar una auditoría a la oficina de Sistemas de Información que se encargará de dar soporte e informar al usuario la actividad completa en el período y módulos solicitados y de igual manera informara qué medidas se deben tomar al respecto. (Investigación preliminar, cambio de usuario, proceso disciplinario).

5. Informar inmediatamente a la oficina de Sistemas de Información cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intente distribuir este tipo de información interna o externamente.

A cualquier infracción a la política de seguridad informática cometida por un funcionario y/o contratista de ESE Hospital Departamental San Antonio de Padua, se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24:**"Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley."**

6. En caso de presentarse un problema crítico a nivel informático en horario no laboral afectando el normal funcionamiento de la ESE Hospital Departamental San Antonio de Padua, la oficina de Sistemas de Información dispone de un funcionario para atender y solucionar estos inconvenientes que está debidamente reportado en la oficina de Regionalización médica quien es el encargado de localizarlo.

7. Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos de acceso a internet (cambio de dirección IP, cambio de nombre de equipo, etc.) o introducir intencionalmente software malintencionado que impida el normal funcionamiento de los sistemas. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24:**"Son deberes de todo servidor público:**

Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley."

8. Todo funcionario que utilice los recursos informáticos, tiene la responsabilidad de velar por su integridad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información es crítica. Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 22: "**Son deberes de todo servidor público:**

Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización."

9. La oficina de Sistemas de Información es la única encargada y responsable de capacitar a los usuarios en el manejo de las herramientas informáticas que son exclusivas de la misión y función de la institución.

10. Los usuarios de la red recibirán capacitación para el manejo de las herramientas desarrolladas en la institución. La asistencia a la capacitación es obligatoria y requisito indispensable para acceder al sistema de información de lo contrario no se le asigna claves y contraseñas. Está totalmente prohibido el uso de contraseñas o claves de otro usuario.

11. No se permitirá el almacenamiento y/o procesamiento de información propiedad del Hospital, en equipos o dispositivos de propiedad de los funcionarios o contratistas. Todos los contratistas y funcionarios deben firmar una cláusula de confidencialidad, que permita al Hospital proteger la información.

POLITICA DE SEGURDAD DE SOFTWARE

1. La oficina de Sistemas de Información es la única responsable de la instalación de software informático y de telecomunicaciones.

2. En los equipos de cómputo de la ESE Hospital Departamental San Antonio de Padua no se permite la instalación de software que no cuente

con el licenciamiento apropiado. Está prohibido el uso de aplicaciones ilegales y el uso de "Cracks", "Keygens" y demás aplicativos.

3. Está totalmente prohibido la instalación de juegos, programas de mensajería o aplicativos que no estén relacionados con las labores institucionales que se realizan en la ESE Hospital Departamental San Antonio de Padua.

4. Con el propósito de proteger la integridad de los equipos y sistemas informáticos y de telecomunicaciones, es obligatorio que todos y cada uno de estos dispongan de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.

5. las medidas de protección lógica (a nivel de software) son responsabilidad del personal de sistemas de información y el correcto uso de los sistemas corresponde a quienes se les asigna y les compete notificar cualquier eventualidad a la oficina de Sistemas de Información.

6. La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario y requerimientos que sean propuestos por la oficina de Sistemas de Información y a la disponibilidad presupuestal con el que se cuente.

7. Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar respaldo correspondiente a la Oficina de sistemas sobre la generación copias de seguridad ya que se considera como un activo de la institución que debe preservarse. Las copias de respaldo a la información generada por el personal y los recursos informáticos de la institución deben estar resguardados en sitios debidamente adecuados para tal fin.

8. La oficina de Sistemas de Información administrará los diferentes tipos de licencias de software y vigilará su vigencia de acuerdo a sus fechas de caducidad.

POLITICAS DE SEGURIDAD DE LA RED E INTERNET

1. Toda cuenta de acceso al sistema, a la red y direcciones IP, será asignada por la oficina de Sistemas de Información de la ESE Hospital Departamental San Antonio de Padua previa solicitud por escrito.

2. Se prohíbe utilizar la red y los equipos de ESE Hospital Departamental San Antonio de Padua para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24: **"Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley."**

3. En lo relacionado con el uso de correo electrónico, no está permitido el uso del correo personal. Los correos institucionales deben ser para uso exclusivo de las actividades de la ESE Hospital Departamental San Antonio de Padua.

4. Para garantizar la seguridad de la información y el equipo informático, la oficina de Sistemas de Información establece filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad:

Se prohíbe:

. Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar o insultar a otras personas, o interferir con el trabajo de los demás.

. Utilizar los recursos de la ESE Hospital Departamental San Antonio de Padua para el acceso no autorizado a redes y sistemas remotos.

. Acceder remotamente a los equipos de la ESE Hospital Departamental San Antonio de Padua, los únicos funcionarios autorizados para realizar estas prácticas son los de la oficina de Sistemas de Información, al momento de dar soporte a los usuarios en horario extra laboral.

. Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas, mediante técnicas, comandos o programas a través de la red.

. Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizado.

. Poner información en la red que infrinja el derecho a la intimidad de los demás funcionarios y/o contratistas.

. Utilizar los servicios de la red para la descarga, uso, intercambio y/o instalación de juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables.

. El intercambio no autorizado de información de propiedad del Hospital, de sus usuarios y/o sus funcionarios, con terceros.

. El acceso a cuentas de correos personales de ningún tipo desde la red del Hospital y solo se podrán utilizar las cuentas de correo electrónico suministradas por la Institución. Algunos ejemplos de los sistemas de correos electrónicos personales no autorizados son yahoo, Hotmail, gmail.

. Utilizar los servicios para acceder a páginas de radio o TV en línea, descargar archivos de música o video, visitar sitios de pornografía, ocio, entre otros que estén fuera de las funciones del usuario. **Código Único Disciplinario (Ley 734 de 2002) Art. 35 Num. 9: "A todo servidor público le está prohibido: Ejecutar en el lugar de trabajo actos que atenten contra la moral o las buenas costumbres."**

5. La oficina de Sistemas de Información tiene habilitado un equipo con acceso total a internet, en el cual, los usuarios puedan realizar consultas o actividades personales, de corta duración. La oficina de Sistemas de Información no se responsabiliza por pérdidas de información en ese equipo, ya que es de uso público y periódicamente se está eliminando información ajena a la institución. La oficina de sistemas realizará monitoreo permanente de tiempos de navegación y actividades realizadas a páginas vistas por parte de los funcionarios y/o contratistas

6. Los servicios bancarios vía web a nombre de la ESE Hospital Departamental San Antonio de Padua, solamente podrán ser utilizados por el jefe de tesorería y únicamente en el equipo que este tenga asignado. La oficina de Sistemas de Información, tendrá habilitado otro equipo para esta tarea a fin de dar apoyo y soporte cuando se solicite.

7. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoría de seguridad y un reporte de los hallazgos a la oficina
de Control Interno y Control Interno disciplinario para que se tomen las medidas pertinentes.

11. Los mensajes y la información contenida en los buzones de correo son de propiedad del Hospital. Los buzones no deberán contener mensajes con mas de un año de antigüedad. Pero se debe dejar un histórico del registro de los mensajes. Todos los mensajes enviados deben respetar los formatos de imàgen corporativa definidos por el Sistema de Gestión Documental y conservar todas las normas de legalidad de los documentos.

POLITICAS DE SEGURIDAD DE DATOS E INFORMACIÓN

La información es en uno de los elementos más importantes dentro de una organización. La seguridad informática debe evitar que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando datos errados o incompletos. El objetivo de esta política es la de asegurar el acceso a la información en el momento oportuno.

1. Toda información de relevancia debe contar con copia de seguridad y un tiempo de retención determinado, por lo cual, la información no se debe guardar indefinidamente en un archivo activo ocupando espacio innecesario de almacenamiento, el usuario debe establecer cuándo su información pasará a ser inactiva. Aplicación de la Ley 594 de 2000 Ley de Archivos. Tablas de Retención Documental.

2. La copia de seguridad de la base de datos central de la ESE Hospital Departamental San Antonio de Padua se genera así:

Una copia semanal en disco, que será almacenada de acuerdo a los requerimientos necesarios para dicho fin ubicado en un sitio distante del área de trabajo. Estas copias deben ser monitoreadas a diario con el objetivo de garantizar la correcta realización y funcionamiento de las mismas. La ubicación de los medios de almacenamiento, deberá estar alejada del polvo, humedad o cualquier contacto con material que produzca corrosión.

3. El propietario de la información, con la participación de un funcionario de la oficina de Sistemas de Información son los encargados de la

creación y seguimiento de las copias de seguridad realizadas a la información previamente seleccionada por el usuario.

4. Cualquier aplicación, archivo desconocido o sospechoso que aparezca en la información del usuario (ya sea en el equipo local, correo electrónico), no debe ser abierto o ejecutado sin antes contar con la asesoría de la oficina de Sistemas de Información, que se encargará de examinar y determinar si la aplicación o archivo es potencialmente peligrosa para el equipo o la red de la entidad.

s. La Ley 594/00 Ley General de Archivos, en sus Artículos 19 y 21 establece: Art. 19 ". Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de su «sic» archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos: a) Organización archivística de los documentos; b) Realización de estudios técnicos para la adecuada decisión, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema.

PARAGRAFO 1o. Los documentos reproducidos por los citados medios gozarán de la validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por las leyes procesales y se garantice la autenticidad, integridad e inalterabilidad de la información.

PARAGRAFO 2o. Los documentos originales que posean valores históricos no podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio.

ARTICULO 21. PROGRAMAS DE GESTION DOCUMENTAL. Las entidades públicas deberán elaborar programas de gestión de documentos, pudiendo contemplar el uso de nuevas tecnologías y soportes, en cuya aplicación deberán observarse los principios y procesos archivísticos.

PARAGRAFO. Los documentos emitidos por los citados medios gozarán de la validez y eficacia de un documento original, siempre que quede garantizada su autenticidad, su integridad y el cumplimiento de los requisitos exigidos por las leyes procesales

Acuerdo 060/2001 del Archivo General de la Nación. **POR EL CUAL SE ESTABLECEN PAUTAS PARA LA ADMINISTRACIÓN DE LAS COMUNICACIONES OFICIALES EN LAS ENTIDADES PÚBLICAS Y LAS PRIVADAS QUE CUMPLEN FUNCIONES PÚBLICAS.** "Comunicaciones por E-mail **ARTICULO DÉCIMO TERCERO: Comunicaciones oficiales por correo electrónico:** Las entidades que dispongan de Internet y servicios de correo electrónico, reglamentarán su utilización y asignarán responsabilidades de acuerdo con la cantidad de cuentas habilitadas. En todo caso, las unidades de correspondencia tendrán el control de los mismos, garantizando el seguimiento de las comunicaciones oficiales recibidas y enviadas. Para los efectos de acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales se deben atender las disposiciones de la Ley 527 de 1999 y demás normas relacionadas.

CODIGO PENAL **Artículo 257.** *Del acceso ilegal o prestación ilegal de los servicios de telecomunicaciones.* El que acceda o use el servicio de telefonía móvil celular u otro servicio de comunicaciones mediante la copia o reproducción no autorizada por la autoridad competente de señales de identificación de equipos terminales de éstos servicios, derivaciones, **o uso de líneas de telefonía pública básica conmutada local, local extendida o de larga distancia no autorizadas**, o preste servicios o actividades de telecomunicaciones con ánimo de lucro no autorizados, incurrirá en prisión de dos (2) a ocho (8) años y multa de quinientos a mil (1.000) salarios mínimos legales mensuales vigentes. **Texto resaltado declarado EXEQUIBLE por la Corte Constitucional mediante** Sentencia de la Corte Constitucional 311 de 2002.

POLITICAS EN ADMINISTRACIÓN DE SEGURIDAD INFORMATICA

1. El nivel de prioridad de cada servicio en cuanto a seguridad y estabilidad informática, deberán estar bajo monitoreo permanente y se define en el siguiente orden:

N°	ASISITENCIALES	N°	ADMINISTRATIVAS
1	Servicio De Urgencias	1	Sistemas De Información
2	Servicio De Cirugía	2	Archivo Y Correspondencia
3	Servicio De Hospitalización	3	Área Financiera
4	Servicio De Consulta Externa	4	Tesorería
5	Servicio De Ginecobstetricia	5	Cartera
6	Servicio De Terapia Física	6	Facturación Y Glosas
7	Servicio De Pediatría	7	Gerencia y contratación

2. Las auditorías de uso de los recursos informáticos a cada dependencia deberán realizarse periódicamente de acuerdo al calendario que establezca la Oficina de sistemas de información. Los hallazgos encontrados serán reportados a la oficina de Control Interno, Control Interno Disciplinario y Gerencia para que se establezcan los correctivos necesarios.

3. Toda la información almacenada en los equipos de cómputo, puede ser auditada por funcionarios de la oficina de Sistemas de Información en la verificación del cumplimiento de las políticas de seguridad establecidas. Los hallazgos encontrados serán reportados a la oficina de Control Interno, Control Interno Disciplinario y Gerencia para que se establezcan los correctivos necesarios.

4. Los jefes de oficina son los responsables en la implementación y garantía inicial del cumplimiento de políticas que hayan sido publicadas, modificadas o adicionadas recientemente. Cualquier violación a las políticas y normas de seguridad establecidas en este documento y aprobadas mediante acto administrativo será sancionada disciplinaria o penalmente. Para las infracciones más graves, se acatará lo estipulado en la ley 1273 de 2009 de delitos informáticos, y Ley 734 de 2002 Código Único Disciplinario.

BIBLIOGRAFIA

- https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- **UNIVERSIDAD NACIONAL DE COLOMBIA.** Guía para elaboración de políticas de seguridad [en línea]www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf

- Manual de seguridad en redes [en línea]. COORDINACIÓN DE EMERGENCIA EN REDES TELEINFORMÁTICAS DE LA ADMINISTRACIÓN PÚBLICA.

APROBACIÓN

Responsable	Nombres y Apellidos	Cargo	Firma
Elaboró	Diego Alejandro Campo Bernal	Técnico Sistema Administrativo	
Revisó	Sahira Piedad Valencia	Profesional Desarrollo Institucional	
Aprobó	Javier Mauricio Bahamón Salas	Gerente	