POLÍTICA DE SEGURIDAD DIGITAL Y DATOS PERSONALES

1. INTRODUCCIÓN

La ESE Hospital Departamental San Antonio de Padua de La Plata - Huila, comprometida con la prestación de servicios de salud seguros, oportunos y de calidad, reconoce la importancia de la protección de la información digital y se compromete a implementar lineamientos para la recolección, almacenamiento, administración, tratamiento y protección de la información y datos personales que reciba de los usuarios y colaboradores garantizando la protección de los derechos como el Habeas Data, la privacidad, la intimidad, el buen nombre y la imagen de nuestros grupos de valor como un pilar fundamental para el adecuado cumplimiento de su misión institucional.

En este marco, y en alineación con los lineamientos establecidos por el Modelo Integrado de Planeación y Gestión (MIPG) y las disposiciones normativas aplicables, la presente Política de Seguridad Digital y Datos Personales establece los principios, directrices y acciones para garantizar la integridad, disponibilidad, confidencialidad y protección de la información y de los activos digitales de la entidad.

Esta política busca fortalecer la cultura de la seguridad digital y protección de datos de manera segura y confidencial en todos los niveles de la organización, promoviendo el uso responsable de las tecnologías de la información, la privacidad de las personas asegurando la gestión de los riesgos digitales y confidencialidad de acuerdo con la Ley contribuyendo así a la modernización institucional, la transparencia, y la confianza de los usuarios, colaboradores y partes interesadas.

2. JUSTIFICACIÓN

La ESE Hospital Departamental San Antonio de Padua de La Plata - Huila, como entidad prestadora de servicios de salud, maneja información de alto valor que es clave para el cumplimiento de su misión institucional, la protección de los derechos de los usuarios y la adecuada gestión administrativa y asistencial.

En este contexto, la adopción de la Política de Seguridad Digital y Datos Personales se hace indispensable para garantizar el uso adecuado, seguro y confiable de la infraestructura tecnológica y de la información en la protección de datos personales.

La presente política responde a la necesidad de:

- ✓ **Promover el uso adecuado de la infraestructura tecnológica** y los sistemas de información dispuestos por la entidad, asegurando que sean utilizados exclusivamente para el desarrollo de las funciones institucionales y en cumplimiento de las normas vigentes.

- ✓ **Garantizar el respeto y cumplimiento de las disposiciones legales, normativas y organizacionales relacionadas con la seguridad de la información**, preservando la confidencialidad, integridad y disponibilidad de los datos institucionales.

- ✓ **Asegurar que se cumplan las restricciones de acceso definidas en cada uno de los procesos de manejo de la información**, evitando accesos no autorizados, alteración o uso indebido de la información y los sistemas.

- ✓ **Fomentar el compromiso y la corresponsabilidad de todos los colaboradores y usuarios de los sistemas de información,** quienes deben informar de manera oportuna al departamento de Sistemas del Hospital sobre cualquier evento sospechoso o incidente que pueda poner en riesgo la seguridad de la información institucional.

- ✓ **Informar a los pacientes** sobre sus derechos, como el acceso, la rectificación, la cancelación y la oposición al tratamiento de sus datos.

- ✓ **Promueve la transparencia** en la gestión de los datos personales, lo que facilita la rendición de cuentas y la resolución de problemas.

- ✓ **Ayuda a prevenir** incidentes de seguridad y fugas de datos, protegiendo la reputación del hospital y evitando sanciones legales.

De esta forma, la política de seguridad digital y Datos Personales se convierte en un instrumento clave para fortalecer la cultura organizacional en torno a la seguridad de la información, asegurando la continuidad del servicio, proteger los derechos de los pacientes y garantizar la transparencia y eficiencia en la gestión hospitalaria.

3. OBJETIVO

3.1 OBJETIVO GENERAL

Establecer y aplicar lineamientos, controles y buenas prácticas en seguridad digital y datos personales que garanticen la **confidencialidad, integridad y disponibilidad** de la información digital y datos personales del Hospital, asegurando la protección de los datos de los pacientes, colaboradores y procesos institucionales, así como la continuidad de los servicios de salud, en cumplimiento de la normatividad vigente y la mejora continua en ciberseguridad y protección de datos personales.

3.2 OBJETIVOS ESPECIFICOS

- Proteger la información digital garantizando confidencialidad, integridad y disponibilidad.
- Integrar la gestión de riesgos digitales en los procesos del hospital.
- Asegurar la continuidad de los servicios mediante la protección tecnológica.
- Promover una cultura de seguridad digital en el talento humano.
- Cumplir con la normatividad de protección de datos y ciberseguridad.
- Monitorear y mejorar continuamente la seguridad digital.
- Establecer normas de cuidado de equipos, periféricos y demás dispositivos físicos.
- 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.
- Garantizar que los datos personales y de salud de los pacientes sean tratados de forma segura y confidencial, evitando accesos no autorizados o usos indebidos.

- Definir los procedimientos para la recolección, almacenamiento, uso, divulgación y eliminación de datos personales.

- Dar a conocer a los pacientes los derechos que tienen sobre sus datos personales y los procedimientos para ejercerlos, como el acceso, la rectificación, la supresión y la revocación de la autorización para el tratamiento de sus datos.

4. META

La E.S.E Hospital Departamental San Antonio de Padua de la Plata, busca consolidar un entorno digital seguro y confiable, implementando medidas para proteger los datos sensibles de las personas donde la protección de la información y los activos digitales sea un pilar estratégico, garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de los datos. Esto se logrará mediante la implementación de controles, procesos y prácticas de ciberseguridad, alineadas con los lineamientos de MIPG y el marco de seguridad digital del Estado colombiano.

5. ALCANCE

La política cubre la información personal de todas las personas relacionadas con el hospital, incluyendo pacientes, empleados, proveedores, contratistas y visitantes.

6. VALORES Y PRINCIPIOS ORIENTADORES

- ✓ **Confidencialidad:** Garantizar que la información clínica, administrativa y financiera sea accedida únicamente por personal autorizado, protegiendo los datos sensibles de los pacientes, colaboradores y proveedores, cumpliendo con la normatividad vigente en protección de datos personales.

- ✓ **Disponibilidad:** Asegurar que los sistemas de información y los datos digitales estén disponibles en el momento oportuno para los usuarios autorizados, garantizando la continuidad de los servicios asistenciales y administrativos.

- ✓ **Integridad**: Preservar la exactitud, confiabilidad y completitud de la información, evitando alteraciones no autorizadas, errores o

manipulaciones indebidas que puedan afectar la calidad de la atención en salud.

- ✓ **Cumplimiento Normativo:** Cumplir con los lineamientos legales nacionales (Ley 1581 de 2012, Ley 527 de 1999 y demás normas aplicables) y las directrices institucionales sobre gestión y seguridad de la información.

- ✓ **Mejora Continua**: Promover la evaluación permanente de riesgos digitales y la actualización de medidas de protección, adaptándonos a los cambios tecnológicos y a las amenazas emergentes en ciberseguridad.

- ✓ **Consentimiento:** En la mayoría de los casos, se requiere el consentimiento informado del titular para el tratamiento de sus datos personales.

- ✓ **Responsabilidad:** El hospital es responsable de garantizar el cumplimiento de la política de datos personales y de responder por cualquier incumplimiento.

- ✓ **Confidencialidad:** El personal del hospital debe mantener la confidencialidad de los datos personales, incluso después de finalizar su relación laboral.

- ✓ **Principio de legalidad:** En el uso, captura, recolección y tratamiento de datos personales, se aplicará las disposiciones constitucionales, legales y reglamentarias vigentes y aplicables que rigen la materia y demás derechos fundamentales conexos.

- ✓ **Principio de Finalidad:** la captura, recolección, tratamiento y uso de datos personales a los que tenga acceso y sean acopiados y recogidos por la ESE.

- ✓ **Principio de libertad:** El tratamiento solo puede ejercerse con el consentimiento, previo, expreso e informado del Titular.

- ✓ **Principio de veracidad o calidad:** La información sujeta a tratamiento será veraz, completa, exacta, actualizada, comprobable y comprensible.

- ✓ **Principio de trasparencia**: En el tratamiento de la Información y datos personales, se garantiza el derecho del Titular a obtener de la ESE HDSAP en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

- ✓ **Principio de Confidencialidad:** Todas las personas de la ESE HDSAP que intervengan en el tratamiento de datos personales que no tenga naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada se relación con algunas de las labores que comprendan el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas.

6. DEFINICIONES

- ➢ **Seguridad Digital**

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 interfaz 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 softwares 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.

- **Datos Personales**

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de sus datos personales.

Aviso de privacidad: Comunicación verbal o escrita, generada por la ESE HDSAP, dirigida al titular para el tratamiento de sus datos personales.

Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento y que estén bajo la responsabilidad de la ESE

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato público: Es el dato que no sea semiprivado, privado o sensible

Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, pública ni sensible y cuyo conocimiento o divulgación puede interesar no sólo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general, como el correo electrónico de una persona.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, o que promueva intereses de cualquier partido político, o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Responsable del tratamiento: Persona natural o jurídica, pública o privada que, por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o los encargados del tratamiento de datos personales, ubicado en Colombia, envían la información o los datos personales a un receptor que se encuentra dentro o fuera del país y que a su vez es responsable del tratamiento.

7. RESPONSABLE

- El propio Hospital Departamental San Antonio de Padua de la Plata Huila

  Una entidad externa:

- Si el Hospital contrata a otra empresa para gestionar los datos, esta empresa podría ser el encargado del tratamiento, pero el hospital sigue siendo el responsable final.

8. ESTRATEGIA

- **Seguridad Digital**

Estrategia de Educación y Capacitaciones: Desarrollar y ejecutar jornadas de formación y sensibilización en seguridad digital dirigido a colaboradores y actores clave, promoviendo buenas prácticas, identificación de amenazas y protección de datos personales.

Estrategia de Controles y Auditorías: Implementar controles técnicos y administrativos para proteger la información digital y realizar auditorías periódicas.

Estrategia de Comunicación: Establecer un canal institucional de comunicación interna y externa para divulgar políticas, alertas de seguridad, buenas prácticas y resultados de gestión en materia de seguridad digital, fomentando la cultura de ciberseguridad en todos los niveles.

Estrategia de Evaluación y Mejora Continua: Realizar evaluaciones periódicas de riesgos, incidentes y niveles de cumplimiento de la política, asegurando que los resultados alimenten un ciclo de mejora continua que fortalezca la seguridad digital y la capacidad de respuesta ante amenazas.

Entrega formal y documentada: de todos los asuntos relacionados con el cargo, incluyendo la copia digital de toda la documentación del área, ya sea del equipo propio de la E.S.E o del equipo personal, garantizando un backup en los servidores de la institución.

- **Datos Personales**

Transparencia y consentimiento: Informar a los ciudadanos sobre cómo se recopilan, utilizan y protegen sus datos personales, obteniendo su consentimiento explícito para el tratamiento de los mismos.

Políticas de privacidad robustas: Establecer políticas claras y concisas que describan cómo se manejan los datos personales, asegurando su protección y cumplimiento de la legislación vigente.

Minimización de Datos: Recopilar solo la información necesaria para los fines específicos, evitando la acumulación de datos innecesarios que puedan ser vulnerables.

Formación: Educar a los colaboradores y a la ciudadanía sobre la importancia de la protección de datos y cómo prevenir su uso indebido.

Participación Ciudadana: Involucrar a la ciudadanía en el diseño y la implementación de políticas de protección de datos, fomentando la confianza y la transparencia.

Acuerdos de Confidencialidad: Estos acuerdos son herramientas legales que establecen las obligaciones de las partes involucradas en el manejo de información

confidencial, incluyendo los datos personales esto aplica para personal de Planta, OPS y Agremiados, al momento de la firma del contrato se debe dejar una cláusula o apartado donde se consideren las cláusulas específicas sobre cómo se tratarán, almacenarán y protegerán estos datos, incluyendo medidas de seguridad técnicas, administrativas y organizativas.

Cláusula de Confidencialidad: Establece que la información personal será tratada con carácter confidencial y no será divulgada sin autorización.

Cláusula de Tratamiento de Datos: Define cómo se utilizarán los datos personales, con qué fines y en qué condiciones.

9. MARCO LEGAL

- **Seguridad Digital**

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.

- **Datos Personales**

Ley 1581 de 2012: conocida como la Ley de Habeas Data. Esta ley establece los lineamientos para garantizar el derecho fundamental de las personas a conocer, actualizar y rectificar la información que se encuentra en bases de datos o archivos, tanto públicos como privados.

Decreto 1377 de 2013: Modifica parcialmente la Ley 1581 y reglamenta aspectos como la autorización para el tratamiento de datos y las políticas de tratamiento de datos personales.

Artículo 11. DECRETO 1377 DE 2013: Limitaciones temporales al Tratamiento de los datos personales. Los Responsables y Encargados del Tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el

tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

Artículo 11. Ley 1581 de 2013: Suministro de la información. La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

Decreto 1499 de 2017: Faculta a la entidades a utilizar los datos demográficos de los ciudadanos como insumo valioso para mejorar la calidad de los servicios que se ofrecen.

El artículo 15 de la Constitución Política de Colombia protege los derechos a la intimidad, buen nombre y al habeas data. De esta disposición constitucional, se desprenden las demás normas que reglamentan la protección de datos en Colombia

10. PROPOSITO

La Política de Seguridad Digital y Datos Personales de la E.S.E Hospital Departamental San Antonio de Padua de La Plata - Huila tiene como propósito establecer los lineamientos y directrices necesarias para proteger la información institucional y garantizar el uso seguro, adecuado y responsable de la infraestructura tecnológica y de los sistemas de información, como establecer las reglas y lineamientos para el tratamiento de la información personal de los individuos por parte de una entidad, garantizando el respeto a sus derechos y la seguridad de sus datos, asegurando la transparencia y la confianza entre la entidad y los titulares de los datos.

11. LINEAS DE INTERVENCIÓN

11.1 Seguridad Digital

Fortalecimiento Tecnológico

Objetivo: Garantizar la implementación y actualización de infraestructura tecnológica segura y confiable para proteger la información y los sistemas críticos de la ESE.

Sensibilización y Capacitación de los Colaboradores

Objetivo: Fomentar una cultura de seguridad digital entre los funcionarios, contratistas y demás colaboradores, promoviendo comportamientos seguros y la gestión responsable de la información.

Gestión de Riesgos Digitales

Objetivo: Identificar, valorar y gestionar los riesgos asociados a la seguridad digital, en coherencia con la Política de Gestión de Riesgos Institucional.

A. EJECUCIÓN

La ESE Hospital Departamental San Antonio de Padua establece su Política de Seguridad Digital con el objetivo de proteger la información, garantizar la confidencialidad de los datos y asegurar la continuidad operativa de los servicios de salud. Para ello, se implementan las siguientes estrategias:

POLITICA	ESTRATEGIAS/METAS	PRODUCTO/ EVIDECIA	INDICADOR
SEGURIDAD DIGITAL	Realizar actualizaciones periódicas de software de seguridad.	Registro de actualizaciones realizadas en los sistemas.	Porcentaje de actualizaciones de seguridad completadas según el plan de mantenimiento
	Monitorear continuamente los procesos asistenciales y administrativos.	Registros de monitoreo de los eventos (requerimientos)	Porcentaje de requerimientos gestionados.

Así mismo, las metas y ejecución de la Política de Seguridad Digital y Datos Personales estarán ligadas a la ejecución y seguimiento del Plan de Mejora Integrado MIPG proyectado para la política en cada vigencia, de acuerdo con la detección de hallazgos FURAG y a las recomendaciones que emita el Departamento Administrativo de la Función Pública para la entidad.

B. EVALUACIÓN

La evaluación de la Seguridad Digital de la ESE Hospital Departamental San Antonio de Padua de La Plata se realizará de forma periódica, a través de la oficina de Planeación quien monitorea la ejecución de las actividades proyectadas para garantiza la óptima implementación de la política, y socializando el resultado del seguimiento respectivo en el comité Institucional de Gestión y Desempeño.

INDICADORES

Para medir el cumplimiento, efectividad y mejora continua de la Seguridad Digital, la ESE Hospital Departamental San Antonio de Padua de La Plata, implementará indicadores que permitirán evaluar el estado de cumplimiento.

Porcentaje de *actualizaciones* de seguridad completadas según el plan de mantenimiento

$$\frac{\text{Número de actualizaciones de seguridad aplicados en el periodo a evaluar}}{\text{Número de actualizaciones de seguridad liberados a aplicar en el periodo a evaluar}} \textbf{ X 100}$$

Porcentaje de requerimientos gestionados

$$\frac{\text{Número de Requerimientos gestionados en el periodo a evaluar}}{\text{Número de Requerimientos solicitados por el personal Asistencial y Administrativo}} \textbf{ X 100}$$

C. 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.**

D. RESPONSABILIDADES DE LA OFICINA DE SISTEMAS DE INFORMACIÓN

- Administrar y coordinar diariamente el proceso de Seguridad Informática de la ESE Hospital Departamental San Antonio de Padua. Establece: El Código único Disciplinario (Ley 734 de 2002) Art.34 Num.28.

"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 digital, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.

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

- 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.

E. ¿QUÉ ES LA SEGURIDAD DIGITAL?

La seguridad digital 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 es la 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.

F. CLASIFICACIÓN DE LA SEGURIDAD GITAL

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 política 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.

G. 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:

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 Único Disciplinario.

- En caso de 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.

- 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.

- 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 de 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.

- 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.

- 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.

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

- 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.

- 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.

- 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.

- Los servidores centrales de la red de la ESE Hospital Departamental San Antonio de Padua deben 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.

- 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).

- 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.

- 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.

- 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.

H. 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.

- 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.

- 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 indebido de 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.

- 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.

- 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).

- 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."**

- 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.

- 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."

- 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."

- 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.

- 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.

- 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.

I. Seguridad de Software

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

- 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.

- 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.

- 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.

- 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.

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

- 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.

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

J. Seguridad de la Red e Internet

- 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.
- 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 Núm. 24

"Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley."

- 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.

- 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:

K. 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 extralaboral.

- 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 Núm. 9: "A todo servidor público le está prohibido: Ejecutar en el lugar de trabajo actos que atenten contra la moral o las buenas costumbres."**

- 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.

- 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.

- 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.

- Los mensajes y la información contenida en los buzones de correo son de propiedad del Hospital. Los buzones no deberán contener mensajes con más 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 imagen corporativa definidos por el Sistema de Gestión Documental y conservar todas las normas de legalidad de los documentos.

L. 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.

- 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.

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

- Una copia de seguridad diaria, que será almacenada en la nube y además en un disco duro, de acuerdo con los requerimientos necesarios para dicho fin ubicado en un sitio, donde ninguna persona sin previa autorización puede acceder a ella, además siendo distante del área de trabajo. Estas copias deben ser monitoreadas a diario con el objetivo de garantizar la correcta realización y funcionamiento de estas. La ubicación de los medios de almacenamiento como lo son en un disco duro portable deberá estar alejada del polvo, humedad o cualquier contacto con material que produzca corrosión.

- Las copias de seguridad son exclusivas del software Dinámica Gerencial Hospitalaria y demás información que sea solicitada por parte de las áreas, para respaldo y/o verificación.

- 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.

- 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.

- 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:

- 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.

M. Administración de Seguridad Informática

- 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 Ginecobstetricia	4	Tesorería
5	Servicio de Consulta Externa	5	Cartera
6	Servicio de Pediatría	6	Facturación y Glosas
7	Servicio de Terapia Física	7	Gerencia - Contratación -Calidad

- Las auditorías de uso de los recursos informáticos a cada dependencia deberán realizarse periódicamente de acuerdo con el 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.

- 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.

- 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.

11.2 DATOS PERSONALES

A. Principios Relacionados con la obtención de datos personales

- la obtención de datos personales se enfoca en garantizar la legalidad, transparencia, minimización, exactitud y seguridad en el tratamiento de la información. Estos principios buscan proteger la privacidad y los derechos de las personas al tiempo que permiten el uso legítimo de los datos.

- Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

- Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

- Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

- Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos por los correspondientes datos rectificados o completados, siempre y cuando el Titular de la información así lo solicite.

B. Finalidad del Tratamiento de Datos

De Manera General

Para todos los usuarios, colaboradores, proveedores, clientes.

- Conocer de manera prospectiva las necesidades de sus grupos de interés con el fin de innovar en la prestación de sus servicios.

- El cumplimiento de las obligaciones derivadas de las relaciones contractuales existentes con sus grupos de interés.

- La seguridad de los pacientes, visitantes, colaboradores y de la comunidad general.

- El control y la prevención del fraude y lavado de activos.

- Informar sobre cambios en la política de Seguridad Digital y Datos Personales

C. Contratistas y Proveedores

- Se utilizarán para complementar el desarrollo de los contratos de prestación servicios.

- Los contratistas tienen derecho a saber qué información personal está siendo tratada por la empresa o entidad, incluyendo datos como nombre, dirección, teléfono, etc.

- Si los datos personales o la empresa del proveedor son incorrectos o están desactualizados, tienen derecho a solicitar su rectificación o actualización.

- Establecer cláusula de confidencialidad del manejo, custodia de la información en todos los contratos de la institución, para garantizar la seguridad de la información.

D. Colaborares y Profesionales de Salud

La información contenida en nuestras bases de datos de ex-empleados, empleados, futuros candidatos a empleo, y profesionales de la salud pasados, actuales o futuros, se utilizará para que el Hospital realice los procesos de promoción interna, verificación de títulos, solicitud de información a otras empresas o instituciones educativas, capacitaciones, contacto directo en caso de ser requerido y en general para realizar todas las gestiones administrativas y financieras relacionadas directamente con la labor para la cual será contratado.

E. Casos en que NO es necesario la Autorización

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

- Casos de urgencia médica o sanitaria.

- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

- Datos relacionados con el Registro Civil de las personas.

F. Personas a las cuales se les puede Suministrar la Información

- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.

- A los terceros autorizados por el Titular o por la ley

- A los proveedores para las finalidades autorizadas por el titular o las previstas en la ley.

G. Deberes de la E.S.E Hospital Departamental San Antonio de Padua

El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

- El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
- Los derechos que le asisten como Titular; La identificación, dirección física o electrónica y teléfono del responsable del tratamiento.
- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.
- Conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.

H. Derechos como Titular de Datos Personales

- Conocer, actualizar y rectificar sus datos personales frente a la institución.
- Quien ejerza el habeas data deberá suministrar con precisión los datos de contacto solicitados, para efecto de tramitar y atender su solicitud.

- Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

- Solicitar la eliminación de tus datos personales cuando ya no sean necesarios para los fines para los que fueron recolectados.

I. Videovigilancia

- La información recolectada por estos mecanismos se utilizará para fines de seguridad y trazabilidad de los bienes, instalaciones y personas que se encuentren en éstas, o como prueba en cualquier tipo de proceso interno, judicial o administrativo, siempre con sujeción y cumplimiento de las normas legales.

- Las imágenes solo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explicitas, y que hayan justificado la instalación de las cámaras o videocámaras.

J. Implementación del Formato

Se establecerá un Formato escrito para el ejercicio del derecho de Habeas Data en la E.S.E Hospital Departamental San Antonio de Padua.

K. Plazo de Respuestas

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

12. BENEFICIOS

Seguridad Digital

- **Protección de Datos:** una seguridad digital robusta protege la información confidencial de la empresa y de los clientes contra accesos no autorizados y pérdidas de datos.
- **Prevención de Ataques:** Ayuda a identificar y mitigar vulnerabilidades, reduciendo el riesgo de ataques cibernéticos y sus consecuencias.
- **Cumplimiento Normativo:** Facilita el cumplimiento de leyes y regulaciones relacionadas con la protección de datos, evitando sanciones y multas.
- **Adaptabilidad:** Una seguridad digital bien diseñada puede adaptarse a los cambios tecnológicos y a las nuevas amenazas, manteniendo la protección efectiva.
- **Cultura de Seguridad:** Una seguridad digital promueve una cultura de concienciación y responsabilidad en toda la organización, involucrando a todos los colaboradores en la protección de la información.

Datos Personales

- **Protección de la Privacidad:** Una política de datos personales garantiza que la información personal de las personas se maneje de manera segura y responsable, respetando su derecho a la privacidad.
- **Mayor control sobre sus datos:** Permite a las personas conocer qué datos se recopilan, cómo se utilizan y con quién se comparten, dándoles mayor control sobre su información personal.
- **Mejora de la reputación:** Demuestra el compromiso de la organización con la protección de los datos personales, lo que puede generar una mejor reputación y fortalecer la confianza de los usuarios.

- **Cumplimiento legal:** Permite a las organizaciones cumplir con las leyes y regulaciones sobre protección de datos, evitando multas y sanciones.

- **Optimización de recursos:** Al gestionar los datos de manera eficiente y segura, las organizaciones pueden reducir costos y mejorar la toma de decisiones

13. BIBLIOGRAFIA

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

- **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.

- https://www1.funcionpublica.gov.co/documents/34645357/34703120/Politica_tratamiento_datos_personales.pdf/b697c1b1-e899-4149-9415-ebe810cb13ca?t=1537181695604

- https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

14. CONTROL DE VERSIONES

VERSIÓN	FECHA	COMENTARIO
01	27/01/2021	Implementación de la Política
02	10/08/2021	Actualización segunda versión
03	04/09/2023	Actualización tercera Versión Res. 203 de 10 agosto 2021
04	19/05/2025	Actualización cuarta Versión, alienado Plataforma Estratégica y Plan Desarrollo Institucional 2024 2028 y lineamientos del instructivo elaboración de documentos institucionales.
05	14/08/2025	Se realiza el cambio de nombre de la política de seguridad digital, a Política de Seguridad Digital y Datos Personales, teniendo en cuenta que la política seguirá vinculada al proceso de MIPG y será objeto de medición cada año en el FURAG, este proceso se establece para dar cumplimiento a la Ley 1581 de 2012.

Elaborado por: **Nombre: EDWIN FABIÁN CASTRO** **Cargo:** Ing. Sistemas Agremiado **Firma:**	**Fecha:** 10/08/2021
Actualizado por: **Nombre: EDWIN FABIÁN CASTRO** **Cargo:** Ing. Sistemas Agremiado **Firma:**	**Fecha:** 02/05/2025
Actualizado por: **Nombre: NELSON F TIERRADENTRO QUINTERO** **Cargo:** Apoyo Profesional Esp. Planeacion Agremiado **Firma:**	**Fecha:** 05/08/2025
Revisado por: **Nombre: LORENA AROCA TAMAYO** **Cargo:** Profesional de Apoyo MIPG **Firma:**	**Fecha:** 08/08/2025
Aprobado por: **Nombre: JOSÉ ANTONIO MUÑOZ PAZ** **Cargo:** Gerente **Firma:**	**Fecha:** 14/08/2025