# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2025

| FECHA DEL CAMBIO | DESCRIPCIÓN DEL CAMBIO | JUSTIFICACIÓN | VERSIÓN |
|---|---|---|---|
| 21/01/2025 | Elaboración del documento | Elaboración del documento | 01 |

## INTRODUCCION

Este documento busca lograr la implementación en la E.S.E Hospital San Vicente de Paul de Paipa las mejores prácticas dadas por el Departamento Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías e Información en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información; por tanto, el Plan de Seguridad y Privacidad de la Información institucional contiene los lineamientos que apoyan la gestión y administración de los planes y procedimientos de seguridad de la información, dando claridad sobre las prácticas de seguridad aplicadas a la institución, preocupándose por definir lineamientos que permitan mitigar los posibles riesgos para la Información.

El Plan de Seguridad y Privacidad de la Información, pretende lograr en la institución y sus clientes internos, externos y partes interesadas confianza en el manejo de la información garantizando para cada uno la privacidad, continuidad, integralidad y disponibilidad de los datos.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

## 1. OBJETIVO

Diseñar e implementar mecanismos y estrategias que permitan asegurar la confidencialidad, integridad y disponibilidad de la información para soportar la adecuada gestión de los procesos de la E.S.E Hospital San Vicente de Paul de Paipa y que se encuentran contempladas en el Modelo de Seguridad y Privacidad de la Información, de tal forma que se responda de forma oportuna a los eventos que la afecten, de tal manera, que se preserve la confidencialidad, integridad y disponibilidad de la misma.

### 1.1 Objetivos Específicos

- Promover el uso de mejores prácticas de seguridad de la información en la institución
- Optimizar la gestión de la seguridad de la información al interior de la entidad
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales
- Optimizar la labor de acceso a la información pública
- Mejorar la confianza de las partes interesadas en el compromiso institucional de preservar adecuadamente la confidencialidad, integridad y disponibilidad de la información bajo responsabilidad de la entidad.

## 2. ALCANCE

Inicia con todos los datos o registros que se recolectan y a toda la información creada, procesada o utilizada, sin importar el medio, formato o presentación o lugar en el cual se encuentre hasta su divulgación o comunicación.

Las políticas de Seguridad de la Información son aplicables a todos los servidores de la institución independiente del tipo de contratación, que procesan y/o manejan información de la entidad

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

## 3. RESPONSABLES

El Plan de Seguridad y Privacidad de la Información aplica a todos los funcionarios, colaboradores, terceros, procesos, servicios de la E.S.E. Hospital San Vicente de Paul de Paipa.

## 4. SOPORTE LEGAL

**Ley 527 (18 de agosto de 1999):** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y Se establecen las entidades de certificación y se dictan otras disposiciones.

**Ley Estatutaria 1581 (17 de octubre de 2012):** "Por la cual se dictan disposiciones generales para la protección de datos personales."

**Ley 1266 (31 de diciembre de 2008):** "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."

**Ley 1712 (06 de marzo de 2014:** Ley de Transparencia y acceso a la información pública nacional.

**Ley 57 (05 de julio de 1985):** "Por la cual se ordena la publicidad de los actos y documentos oficiales."

**Ley 962 (08 de julio 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."

**Ley 2052 de 2020,** "Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones"

**Decreto Ley 2150 de (05 de diciembre de 1995):** “Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.”

**Decreto 1078 (26 de mayo de 2015):** “Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.”

**Decreto 019 de 2012:** "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".

**Decreto 2364 (22 de noviembre de 2012)**: Firma electrónica.

**Decreto 1747 (11 de septiembre de 2000):** “Por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales”

**Decreto 1078 (26 de mayo de 2015):** “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”

**Decreto 1008 de 2018,** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

**Decreto No. 2106 del 22 de noviembre de 2019**. “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.”

**Resolución 3564 de 2015 (31 de diciembre de 2015):** Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.

**Documento CONPES 3854**, Política Nacional de Seguridad Digital

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

**Documento CONPES 3975,** Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES)

**Norma Técnica Colombiana NTC- ISO/IEC Colombiana 27001:2013.** Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

## 5. DEFINICIONES

Para la adecuada gestión del presente plan, se debe manejar con propiedad los siguientes términos:

**Activo:** cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

**Activo de Información**: recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación).

**Amenaza informática:** situación potencial o actual que tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado

**Antivirus:** programas cuyo objetivo es detectar y eliminar software malicioso.

Análisis de riesgos**:** proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo.

**Anonimización del dato:** eliminar o sustituir algunos nombres de personas (físicas o jurídicas), direcciones, información de contacto, números identificativos, apodos o cargo por otros datos para evitar la identificación de personas y preservar la confidencialidad de la información.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

**Archivos PST:** son archivos electrónicos creados desde el software de mensajería Outlook con el fin de almacenar de forma local (computadores), copia de elementos de un buzón de correo electrónico

**Autenticación:** mecanismo técnico que permite garantizar que una persona o entidad es la correcta.

**Autenticidad:** Propiedad de que una entidad es lo que afirma ser.

**Back up:** se refiere a una copia de respaldo de información**.**

**Buzón:** espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros**.**

**Canal de comunicación:** medio utilizado para la transmisión de información, por ejemplo: el cableado, fibra óptica y la atmósfera.

**Centro de cómputo:** espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización llamado también *data center* por su término anglosajón.

**Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

**Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.

**Confiabilidad:** persona o cosa en la que se puede confiar.

**Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Control informático:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo reduciendo la probabilidad o impacto del evento.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

**Correo electrónico:** servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica.

**Claves, contraseña o password:** forma de autentificación que utiliza información secreta o confidencial para controlar el acceso hacia algún recurso.

**Custodio de activo de información**: individuo, cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de cumplir y velar por el cumplimiento de los controles que el responsable del activo de información haya definido, con base en los controles de seguridad disponibles en la entidad.

**Datos abiertos:** son datos primarios o sin procesar. Los cuales son puestos a disposición de cualquier ciudadano con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

**Datos biométricos:** parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (ej. huella digital o voz).

**Datos personales 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.

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

**Gestión de claves:** son controles que realizan mediante la gestión de claves criptográficas.

**Gestión de incidentes de seguridad de la información:** proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

**Habeas data:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

**Infraestructura tecnológica:** elementos de hardware, software y comunicaciones que soportan la operación de los diferentes servicios de la entidad, entre los cuales se encuentran: equipos de trabajo, equipos portátiles, impresoras, escáner, videocámaras, wifi, sistemas operacionales, herramientas ofimáticas e internet entre otros.

**Responsable de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado encargado de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados, quien puede designar custodios del activo de información y autorizar a los usuarios para el acceso al activo de información.

**Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.

## 6. DESARROLLO

La seguridad de la información incluye tres dimensiones principales: la confidencialidad, la disponibilidad y la integridad. Con el objetivo de garantizar el procesamiento sostenido, así como su continuidad, y minimizar impactos, la seguridad de la información conlleva la aplicación y la gestión de medidas de seguridad adecuadas que implican la consideración de una amplia gama de amenazas.

### 6.1 METODOLOGIA PARA LA IMPLEMENTACION

Para el desarrollo del Plan de Seguridad y Privacidad de la Información de la E.S.E. Hospital San Vicente de Paul de Paipa, se toma como base la norma ISO – IEC 27001:2013 Sistema de Gestión de la Seguridad de la Información, el modelo de

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

gestión de la seguridad de la información, la metodología PHVA y el Modelo Integrado de Planeación y Gestión MIPG.

**FASES DE IMPLEMENTACION.**

- **Fase de Diagnóstico:** Es la etapa previa a la implementación, en esta, se identifica el estado actual de la institución con respecto a los requerimientos de seguridad y privacidad de la información para alcanzar las metas propuestas (validar el estado actual de la gestión y seguridad de la información al interior de la E.S.E., determinar la efectividad de los controles, identificar los avances en la implementación y evaluar el correcto uso de las buenas prácticas).

- **Fase de Planificación:** Para el desarrollo de esta fase se deben evaluar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información cumpliendo con los objetivos de la institución con el propósito de definir acciones a desarrollar.

- **Fase de Implementación:** Esta fase permite ejecutar las actividades formuladas en la fase anterior.

- **Fase de Evaluación**: Es el proceso de seguimiento y monitoreo con base en los resultados, midiendo la eficiencia, eficacia y efectividad de las acciones implementadas.

- **Fase de Mejora Continua**: Se consolidan los resultados de la evaluación para diseñar el plan de mejoramiento y seguimiento continuo, tomando las acciones oportunas para mitigar las debilidades.

## 6.2 ACTIVIDADES DE SEGURIDAD DE LA INFORMACION

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Se desarrollan y formalizan los procedimientos que permiten gestionar la seguridad y privacidad de la información en cada uno de los procesos de la E.S.E. Hospital San Vicente de Paul de Paipa.

- **Política de Seguridad de la Información.**

La E.S.E Hospital San Vicente de Paul de Paipa, cuenta con la Política de Seguridad de la Información, en donde se compromete a establecer medidas que garanticen la seguridad y confidencialidad de la información, evitando el acceso no autorizado a la información que reposa en los sistemas de la institución (base de datos, sistema asistencial – administrativo), consultas no autorizadas, adulteraciones y perdida de datos para usos distintos a los determinados por la institución.

- **Seguridad ligada al Talento Humano.**

Todos los funcionarios independientes del tipo de contratación que accedan a los activos de información de la E.S.E. Hospital San Vicente de Paul de Paipa deben ser autorizados previamente y tienen los siguientes deberes:

- Se debe custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidas de la información institucional.

- Se debe proteger los softwares, los aplicativos, los equipos de comunicación y procesamiento de datos, que le han sido asignados para su utilización de acuerdo al uso de las buenas prácticas, de manera racional y de conformidad con los fines a que han sido destinados.

- El acceso a los recursos de información de la organización presupone la aceptación de este documento de políticas de seguridad, así como las respectivas sanciones por su incumplimiento, lo cual se confirma a través de la firma de un acuerdo de responsabilidad que hará parte del contrato prestación de servicios o acto de posesión.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

- Los funcionarios del Hospital, deben garantizar que el acceso a la información y la utilización de la misma sea exclusivamente para actividades relacionadas con las funciones propias de la organización y que esta sea utilizada de acuerdo a los criterios de confidencialidad definidos por la E.S.E Hospital San Vicente de Paul de Paipa.

- **Protección de la Información**

Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida de los activos de la información de la E.S.E. Hospital San Vicente de Paul, La protección debe enfatizar la confidencialidad, integridad y disponibilidad de los activos de información.

Todos los funcionarios, contratistas, o terceras personas que accedan a los activos de información de la E.S.E. Hospital San Vicente de Paul de Paipa deben:

- Definir y ejecutar procedimientos de seguridad para la entrega de información, apoyándose de algunos lineamientos muy claros donde se determine qué información se considera confidencial, restringida o pública.
- La copia de seguridad de información exógena al Sistema de Información Institucional, es responsabilidad de todos los funcionarios, contratistas, o terceras personas que accedan a estos activos informáticos.

- **Protección de los Recursos Tecnológicos**

- La E.S.E Hospital San Vicente de Paul de Paipa asegurará la contratación requerida para mantener actualizadas las licencias de Antivirus, Firewall, el mantenimiento de las redes y equipos, e infra estructuras de las mismas, las cuales permitirán proteger los recursos informáticos contra ataques de virus, ingresos maliciosos y filtrados de contenido de correos, archivos, USB, CD, etc.

- Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida del negocio. Dichos recursos deben ser utilizados exclusivamente para desarrollar las actividades laborales

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

y así mismo, su utilización se hará en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

- La infraestructura de los Servidores y equipos de telecomunicaciones del Hospital, debe estar ubicada en un área protegida o cerrada (Centro de Cómputo) en la cual sólo se permitirá el ingreso de personal autorizado, es decir, a quienes deban cumplir alguna función específica relacionada con dichos equipos.

- **Autorización de usuarios**

- Todos los usuarios deben ser identificados independientemente con permisos de acceso específicamente e individualmente autorizados. Los métodos de acceso de usuarios deben exigir un proceso robusto de autenticación, autorización apropiada y auditoría confiable. Para cumplir con esta política el Profesional de Sistemas del Hospital, debe definir las consideraciones a tener en cuenta para la autorización y permisos de los usuarios.

- **Responsabilidad**

- Los usuarios y custodios de los activos de información de la E.S.E Hospital San Vicente de Paul de Paipa, son responsables por el uso apropiado, protección y privacidad de estos activos. Los sistemas generarán y mantendrán unas apropiadas reglas de auditoría para identificar usuarios, y documentar los eventos relacionados con la seguridad y disponibilidad.

- Los activos de información deben estar disponibles para soportar los objetivos de la E.S.E Hospital San Vicente de Paul de Paipa, se deben tomar medidas adecuadas para asegurar el tiempo de recuperación de toda la información y acceso por personas autorizadas.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

- El área de sistemas del Hospital debe definir el plan de recuperación en conjunto con los usuarios involucrados en el proceso, para garantizar la continuidad del negocio.

- **Integridad**

Los activos de información deben estar adecuadamente protegidos para asegurar su integridad y precisión. Las medidas de validación definidas permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

## 6.3 LINEAMIENTO DE SEGURIDAD.

- **Gestión de activos**

- Las diferentes áreas con el fin de garantizar la administración y control sobre los activos de la entidad, deben mantener un inventario actualizado de los activos que se encuentran dentro del alcance del modelo de gestión de seguridad de la información y que están cargados a cada proceso, el cual debe estar alineado con el inventario general de activos de información.

- En el inventario se identificará el propietario del activo, quien debe asegurar que la información y los activos asociados con su proceso están clasificados de manera apropiada, así como de establecer controles necesarios para el acceso a éstos de acuerdo con los procedimientos definidos.

- **Uso aceptable de los activos**

- La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, entre otros) propiedad de la E.S.E. Hospital San Vicente de Paul de Paipa, son activos de

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

la Institución y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con los propósitos de la institución.

- La E.S.E. Hospital San Vicente de Paul de Paipa, podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en este plan y en cualquier proceso legal que se requiera.

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

- Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un “Acuerdo de Confidencialidad de la Información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los lineamientos definidos en la Política de Información de la E.S.E Hospital San Vicente de Paul de Paipa y los lineamientos del presente documento. En caso de violación de la información será considerado como un incidente de seguridad y se procederá de acuerdo a lo definido al tratamiento de este tipo de incidentes.

- **Uso adecuado de internet**

La E.S.E. Hospital San Vicente de Paul de Paipa, consciente de la importancia del servicio de internet como una herramienta para el desempeño de las labores, proporcionará los recursos necesarios para asegurar su disponibilidad al personal que así lo requiera para el desarrollo de sus actividades diarias en la entidad.

Pautas para tener en cuenta:

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

- El área de sistemas debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet.
- Se deben establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música y productos que de alguna forma atenten contra la propiedad intelectual de sus autores, por tanto, se debe asegurar el buen uso del recurso.
- No está permitido el intercambio no autorizado de información propiedad de la institución, por parte de los funcionarios con terceros.
- En general, cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

- **Correo electrónico**

- El correo electrónico corporativo es una herramienta de comunicación o intercambio de información oficial entre personal o instituciones, no es una herramienta de difusión indiscriminada de información.

- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del Hospital.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la E.S.E. Hospital San Vicente de Paul de Paipa y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- El tamaño de envío y recepción de mensajes, sus contenidos y demás características propias de estos deberán ser definidos e implementados por el área de Sistemas.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que la E.S.E. Hospital San Vicente de Paul de Paipa proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal dentro de la institución.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la institución y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- Los archivos que se adjuntan en los mensajes de correo en lo posible deben comprimirse para evitar la saturación en las diferentes cuentas de correos.
- El usuario que tiene asignada una cuenta de correo electrónico es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre, por lo tanto, el Hospital no se hace responsable por lo que diga o haga. Esta información se incluirá en todos los mensajes que se envíen.
- El correo electrónico corporativo es la única vía de remisión o envío de documentos de carácter administrativo interno en el hospital.

**No está permitido:**

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico de la E.S.E. Hospital San Vicente de Paul de Paipa, como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Instagram, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

- **Copias de seguridad**

Toda información institucional que sea de interés para un proceso asistencial, administrativo o de misión crítica debe ser respaldada mediante copias de seguridad,

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

las cuales se deben conservar en lugar seguro de tal forma que en caso de ser necesarias se conserven correctamente.

## 6.4 ACUERDOS SOBRE CONFIDENCIALIDAD

Todos los funcionarios, colaboradores y/o terceros que presten sus servicios a la E.S.E. Hospital San Vicente de Paul de Paipa, deberán aceptar los acuerdos de confidencialidad definidos por la institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para los contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la E.S.E. Hospital San Vicente de Paul de Paipa, a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Los controles que se establezcan como necesarios a partir del análisis de riesgos deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

## 6.5 CLASIFICACIÓN DE LA INFORMACIÓN

La E.S.E. Hospital San Vicente de Paul de Paipa con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de sus funcionarios, contratistas, proveedores o clientes, ha establecido niveles para la clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, verbal o que sea transmitida por cualquier medio.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Toda la información de la E.S.E. Hospital San Vicente de Paul de Paipa debe ser identificada, clasificada y documentada de acuerdo con los criterios de clasificación establecidos. Los niveles de clasificación de la información definidos en la E.S.E. Hospital San Vicente de Paul de Paipa son:

- EXTERNA
- CATEGORÍA PÚBLICA
- PÚBLICA USO INTERNO
- PÚBLICA CLASIFICADA
- PÚBLICA RESERVADA

## 6.6 SEGURIDAD DE LOS RECURSOS HUMANOS

Todos los funcionarios de la E.S.E. Hospital San Vicente de Paul de Paipa contratistas y terceros que tengan la posibilidad de acceder a la información de la organización y a la infraestructura para su procesamiento, son responsables de conocer y cumplir con las políticas y procedimientos establecidos en el Modelo de Gestión de Seguridad de la Información de la institución. De igual forma, son responsables de reportar por medio de los canales apropiados, el incumplimiento de las políticas y procedimientos establecidos.

Todos los funcionarios de la E.S.E. Hospital San Vicente de Paul de Paipa deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la organización.

## 6.7 EDUCACIÓN, FORMACIÓN Y CONCIENTIZACIÓN SOBRE LA SEGURIDAD DE LA INFORMACIÓN

La E.S.E. Hospital San Vicente de Paul de Paipa, debe asegurar que todos los funcionarios que tengan definidas responsabilidades en la Seguridad de la Información sean competentes para desempeñar sus funciones y que cuenten con los programas de capacitación y entrenamiento requeridos para ello.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

De igual forma, todos los funcionarios y, cuando sea relevante, los terceros tendrán un proceso formal de concientización, mediante el cual se capacitará sobre las políticas de seguridad de la Institución y los riesgos conocidos a los que se puede ver expuesta, en caso que estas no se cumplan.

Los programas de concientización, educación y entrenamiento se encuentran diseñados de manera apropiada y relevante para los roles, responsabilidades y habilidades de las personas que deben asistir a ellos.

## 6.8 PROCESO DISCIPLINARIO

En el caso de identificarse un incidente de seguridad, éste será registrado en la herramienta de gestión designada, y se hará la investigación respectiva para determinar las causas y responsables, posteriormente la E.S.E. Hospital San Vicente de Paul de Paipa, tomará las acciones pertinentes para que el funcionario y/o tercero vinculado con el incidente, mediante un proceso disciplinario formal de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la organización.

## 6.9 DEVOLUCIÓN DE ACTIVOS.

Todo funcionario al momento de su retiro o cambio de funciones en la institución debe hacer entrega del equipo que se le había asignado, adjuntado un inventario con toda la información contenida en él.

## 6.10 SEGURIDAD FÍSICA Y DEL ENTORNO

La E.S.E. Hospital San Vicente de Paul de Paipa, será el responsable de definir el perímetro de la seguridad física de acuerdo a la clasificación de los activos de la información, controlando el acceso a la información a través de controles (Ejemplo: acceso a áreas, registro de entrada de equipos, autenticación), los cuales disminuyen la posibilidad de riesgo de divulgación o pérdida de información.

- **Controles de Acceso Físico**

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran área de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

- **Protección y ubicación de los equipos**

Los equipos que hacen parte de la Infraestructura tecnológica de la E.S.E. Hospital San Vicente de Paul de Paipa tales como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica E.S.E. Hospital San Vicente de Paul de Paipa no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

Cualquier traslado de equipos de cómputo se realizará con la coordinación del área de Sistemas previa verificación de las condiciones técnicas y de seguridad.

Toda persona que note algún problema de funcionamiento o ataque de virus en una estación de trabajo debe reportarlo de inmediato al personal de soporte técnico.

La E.S.E. Hospital San Vicente de Paul de Paipa debe proveer suministros y equipamiento de soporte como electricidad, planta eléctrica y un sistema de

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

alimentación no interrumpida (UPS) que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de cualquiera de estos elementos, evitando así la pérdida o corrupción de información. Estos suministros deben ser monitoreados, revisados y medidos permanentemente para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños.

De igual manera, la E.S.E. Hospital San Vicente de Paul de Paipa, debe establecer un programa de planeación y ejecución de mantenimientos preventivos anuales (como mínimo), a la infraestructura tecnológica.

Ningún empleado, contratista o tercero podrá desarmar o destapar equipos.

- **Gestión de contraseñas**

Las contraseñas o claves de acceso a los activos de información son personales e intransferibles.

Toda acción realizada con el usuario y contraseñas asignadas es responsabilidad del usuario a quien se le haya asignado.

Las contraseñas no deben ser divulgadas o compartidas entre usuarios. Cualquier daño o alteración de la información es responsabilidad del usuario que la realizó.

No se debe prestar el usuario asignado ni la contraseña, ya que, en caso de haber alguna violación de seguridad, la responsabilidad recae sobre la persona a cargo de dicho usuario.

- **Seguridad de los equipos y medios de información fuera de las instalaciones**

Independientemente del propietario, todos los funcionarios son responsables de velar por la seguridad de los equipos de la E.S.E. Hospital San Vicente de Paul de Paipa que se encuentren fuera de las instalaciones de la organización.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.

Los equipos de la E.S.E. Hospital San Vicente de Paul de Paipa, deberán contar con un seguro que los proteja de robo.

En caso de pérdida o robo de un equipo de la E.S.E. Hospital San Vicente de Paul de Paipa, se deberá informar inmediatamente al Líder del Proceso para que se inicie el trámite interno y se deberá poner la denuncia ante la autoridad competente.

El retiro de equipos de cómputo, periféricos, dispositivos de almacenamientos, software e información considerada crítica propiedad E.S.E. Hospital San Vicente de Paul de Paipa, fuera de las instalaciones de la organización debe seguir los procedimientos establecidos por el área de Sistemas de la E.S.E. Hospital San Vicente de Paul de Paipa.

- **Eliminación o reutilización segura de equipos y medios**

La E.S.E. Hospital San Vicente de Paul de Paipa debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura.

Cuando un equipo sea reasignado o dado de baja, se deberá realizar el proceso de acuerdo al procedimiento establecido para tal fin.

## 7. CRONOGRAMA DE ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

| DESCRIPCION DE ESTRATEGIAS Y ACTIVIDADES |
|---|
| Realizar el mantenimiento preventivo a la totalidad de equipos de comunicación e informática |
| * Administrar sistemas SIHOS, dar soporte y realizar los ajustes requeridos en el Sistema de Información Hospitalario<br>* Genererar los informes requeridos por las diferentes áreas |
| Dar soporte en el menor tiempo posible a los usuarios en cuanto a los requeimientos por fallas en los equipos de comunicación e informática |
| Adquirir el servicio técnico, suministro de repuestos para computadores e impresoras, tintas y toner para las impresoras de la E.S.E HOSPITAL SAN VICENTE DE PAUL DE PAIPA |
| Realizar el proceo de diagnóstico para evaluar los equipos que requieren actualización o reposición y soliciutd de adquisición. |
| Realizar el proceso contractual para la adquisición de Antivirus para Servidores y equipos de computo |
| Realizar el proceso de cambio de equipos en las áreas que se requiere. |
| Adquirir Hosting, Dominio y capacidad de almacenamiento para el optimo funcionamiento de la página Web |
| Adquirir servicoos de almacenamiento en la nube para el correcto funcionamiento de los correos electrónicos |
| Actualizar la página Web de acuerdo a los líneamientos normativos |
| 1. Realizar el proceso contractual de Contratación de la Actualización del Sistema Hospitalario SIHOS |
| 1. Implementar la Actualización de los diferentes procesos del Sistema de Información Hospitalaria<br>2. Implementar los diferentes Manuales de Usuario, definiendo roles y responsabilidades.<br>3. Evaluar la efectividad y generar acciones de mejora |
| 1.Realizar el proceso de Actualización del Sistema de información Web Almera para realizar el Seguimiento a los diferentes Planes Institucionales<br>2. Administrar y mantener consolida la información generada en los diferentes procesos, en el sistema de información Almera. |
| Realizar el proceso contractual para gestionar y almacenar los laboratorios Clínicos |
| Realizar cronograma con las fechas de reporte establecidas, por los diferentes entes de control<br><br>Solicitar la información requerida al área correspondiente con dependiendo de la información a reportar con suficiente tiempo de antelación para posteriormente validarla y enviarla en la plataforma correspondiente de manera exitosa. |
| 1. Contestar las llamadas y realizar la asignación de los servicios de forma efectiva<br>2. Realizar devolución de llamadas no contestadas<br>3. Relizar Demanda Inducida |
| Actualizar e implementar el Proceso de Gestión Documental |



Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

## 8. PLAN DE SEGUIMIENTO

Se realiza seguimiento de manera anual, de tal forma que se verifique el cumplimiento de las actividades formuladas y se realicen ajustes o cambios al plan según lo amerite y de determinen las necesidades.

| | | |
|---|---|---|
| **Elaborado por:** | **Cargo:** | **Fecha: 21/01/2025** |
| Deicy Jimena Gutierrez Perez | Líder Gestión de la Información y Comunicaciones | **Firma:** |
| **Revisado Por:** | **Cargo:** | **Fecha: 21/01/2025** |
| Nelly Nayibe Dallos Lara | Líder Gestión de Calidad | **Firma:** |
| **Aprobado por:** | **Cargo:** | **Fecha: 21/01/2025** |
| Catherine Van Arcken Martínez | Gerente | **Firma:** |


Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa