Empresa Social Del Estado
Hospital San Vicente De Paul Municipio De Caldas Antioquia

Plan De Seguridad y Privacidad De La Información - PESI

Contiene:
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Elaborado Por

Ruth Nacarina Garzón Urrea
Director Técnico Dirección de Gobierno Digital, Tecnologías e Información

Aprobado por

Comité Institucional de Gestión y Desempeño

Caldas Antioquia
Enero – 2025

Contenido

1. Introducción

En el entorno hospitalario, la gestión segura de la información es esencial para garantizar la **confidencialidad, integridad y disponibilidad** de los datos clínicos y administrativos.

La transformación digital en el sector salud ha incrementado la dependencia de las Tecnologías de la Información y Comunicación (TIC), lo que ha hecho necesario establecer estrategias para la protección de la información sensible de los pacientes y el cumplimiento de las normativas legales vigentes en Colombia.

En ese contexto, este **Plan de Seguridad y Privacidad de la Información** se fundamenta en el **Decreto 1072 de 2015** y el **Decreto 620 de 2020**, que establecen los lineamientos de seguridad digital para entidades públicas y privadas que manejan información personal y de salud en el país. Además, se articula con la **Ley 1581 de 2012**, la cual regula la protección de datos personales en Colombia, garantizando el derecho a la privacidad y el tratamiento adecuado de la información.

2. Objetivos

2.1 Objetivo General

Definir un Plan estratégico de Seguridad de la Información (PESI) y plan de tratamiento de riesgos de seguridad y privacidad de la Información (MSPI) liderados por la Dirección de Informática de la ESE Hospital San Vicente de Paul de Caldas Antioquia, durante la vigencia 2022, que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

2.2 Objetivos Específicos

- Proteger los datos personales y clínicos de los pacientes.
- Garantizar el cumplimiento de normativas nacionales e internacionales sobre seguridad de la información.
- Prevenir accesos no autorizados, pérdidas o alteraciones de información.
- Capacitar al personal en buenas prácticas de seguridad informática.
- Comunicar e implementar la Estrategia de Seguridad de la Información.
- Calificar el nivel de madurez en la gestión de la seguridad de la información.
- Implementar y apropiar el Modelo de Privacidad y Seguridad de la Información MPSI,

con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

- Hacer uso eficiente de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.) para garantizar la continuidad en la prestación de los servicios.
- Definir las responsabilidades relacionadas con el manejo de la seguridad.
- Establecer una metodología de gestión de seguridad de la información clara y estructurada.
- Reducir el riesgo de pérdida, robo o corrupción de información.
- Garantizar que los usuarios tengan acceso a la información a través de medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de esta.

3. Marco Legal

Norma	Descripción
Constitución Política De Colombia	Constitución Política de Colombia 1991
Ley 80 de 1983	Estatuto general de contratación de administración pública
Ordenanza Plan Departamental de Desarrollo de Antioquia 2016-2019	Plan departamental de desarrollo de Antioquia 2016-2019
Ley 594 de 2000	Ley de archivos-gestión documental
Ley 1581 de 2012	Ley de protección de datos personales
Ley 1712 de 2014	Ley de transparencia
Ley 1150 de 2007	Disposiciones generales sobre contratación con recursos públicos
Ley 1273 de 2009	Protección de la información y de los datos
Ley 1341 de 2009	Principios y conceptos sobre la sociedad de la información y las comunicaciones TIC, se crea la agencia nacional de espectro y se dictan otras disposiciones
Ley 23 de 1982	Derechos de autor
Decreto 1008 de 2018	Lineamientos generales de la estrategia de Gobierno Digital
Directiva Presidencial 04 de 2012 – cero papeles	Eficiencia administrativa y lineamientos de la política de cero papeles en la administración pública
Decreto 1078 de 2015-reglamento TIC	Reglamento del sector de las tecnologías de la información y comunicaciones
Ley 1266 de 2008	Habeas data
Ley 1928 de 2018	Convenio sobre la ciberdelincuencia

Ley 527 de 1999	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.
CONPES 3584	Política de seguridad digital
CONPES 3701	Lineamientos de política para ciberseguridad y ciberdefensa
CONPES 3854	Política Nacional de Seguridad Digital

4. Alcance

El Plan estratégico de Seguridad de la Información (PESI) y plan de tratamiento de riesgos de seguridad y privacidad de la Información (MSPI) aplica a todos los procesos, sistemas, equipos y usuarios que manejen información dentro del hospital, incluyendo personal administrativo, asistencial y proveedores externos con acceso a los sistemas hospitalarios.

5. Responsables

- ✓ Director Técnico Dirección de Gobierno Digital, Tecnologías e Información
- ✓ Equipo Directivo

6. Definiciones

Para garantizar una comprensión amplia y clara de los términos clave en el Plan de Seguridad y Privacidad de la Información, se presentan las siguientes definiciones:

Autenticación: Proceso de verificación de identidad que permite el acceso a sistemas informáticos mediante credenciales como usuario, contraseña o autenticación multifactor.

Autorización: Permiso otorgado a un usuario para acceder a ciertos sistemas, datos o recursos dentro del hospital, basado en su rol o función.

Ciberseguridad: Conjunto de medidas diseñadas para proteger los sistemas informáticos del hospital contra amenazas digitales, como virus, ransomware o ataques cibernéticos.

Confidencialidad: Garantía de que la información solo será accesible por personas autorizadas, evitando divulgaciones indebidas.

Control de Acceso: Mecanismo que restringe el acceso a la información hospitalaria según el perfil del usuario, evitando que personas no autorizadas accedan a datos sensibles.

Datos Personales: Información que permite identificar a una persona, como nombres, direcciones, teléfonos y documentos de identidad.

Datos Sensibles: Información que afecta la privacidad del paciente, como historiales médicos, diagnósticos, tratamientos y datos biométricos.

Disponibilidad: Garantía de que la información estará accesible y utilizable cuando sea requerida por usuarios autorizados.

Gestión de Riesgos de Información: Identificación, análisis y mitigación de vulnerabilidades que puedan afectar la seguridad de los datos en el hospital.

Historia Clínica Electrónica (HCE): Registro digital con información médica del paciente, cuyo acceso, uso y protección deben cumplir normativas de privacidad y seguridad.

Incidente de Seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de la información, como accesos no autorizados, fuga de datos o ataques cibernéticos.

Integridad: Protección de los datos contra modificaciones no autorizadas o alteraciones accidentales, asegurando su exactitud y fiabilidad.

Normativas y Regulaciones: Conjunto de leyes y estándares (Ley 1581 de 2012, Decreto 620 de 2020, ISO 27001) que establecen directrices para la protección de la información en el sector salud.

Phishing: Técnica fraudulenta utilizada por ciberdelincuentes para obtener información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos o mensajes falsificados.

Plan de Respuesta a Incidentes: Conjunto de acciones y procedimientos diseñados para detectar, responder y mitigar incidentes de seguridad en el hospital.

Privacidad de la Información: Derecho de los individuos a controlar el uso y acceso a sus datos personales, especialmente aquellos relacionados con su salud.

Respaldo de Información (Backup): Copia de seguridad de datos esenciales para garantizar su recuperación en caso de fallas, ataques o pérdidas de información.

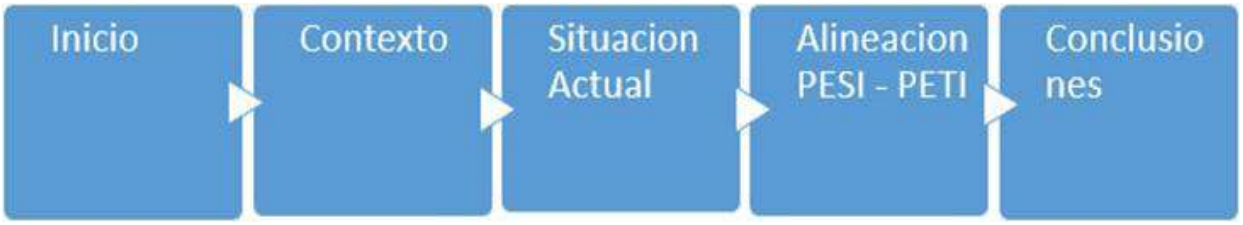
Seguridad de la Información: Conjunto de medidas y estrategias destinadas a proteger la confidencialidad, integridad y disponibilidad de los datos en el hospital.

Usuarios Autorizados: Personal del hospital que, por su rol, tiene acceso a ciertos sistemas y datos bajo condiciones de seguridad establecidas.

7. Desarrollo

7.1 Metodología

La metodología utilizada para el desarrollo del PESI se muestra a continuación:



7.2 Estructura

El éxito del Plan Estratégico de Seguridad de la Información (PESI) en el hospital depende en gran medida del compromiso y liderazgo del equipo directivo. Su rol es clave para garantizar la asignación de recursos, la implementación de políticas y la concienciación del personal sobre la importancia de la seguridad de la información. Las formas en las que equipo directivo apoyará el PESI son las siguientes:

- Definición de la Estrategia y Políticas de Seguridad apoyado la oficina de Planeación
  - ✓ Estableciendo los objetivos del PESI alineados con la misión del hospital.

- ✓ Aprobando las políticas de seguridad y privacidad de la información.
- ✓ Garantizando el cumplimiento de normativas legales (Ley 1581 de 2012, Decreto 620 de 2020, ISO 27001).

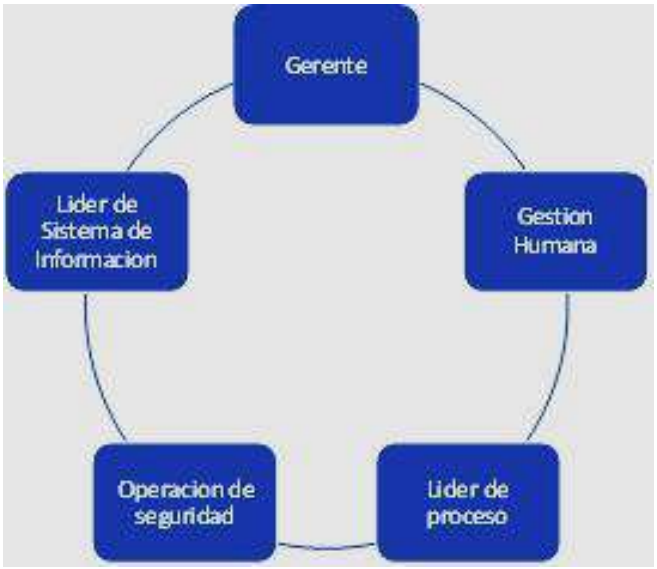
- Asignación de Recursos Humanos y Tecnológicos apoyado por la subgerencia Administrativa y Financiera
  - ✓ Destinando presupuesto para herramientas de ciberseguridad (firewalls, antivirus y análisis de vulnerabilidades).
  - ✓ Apoyando los proyectos que involucren personal especializado en seguridad informática.
  - ✓ Aprobando capacitaciones en seguridad de la información para empleados.

- Liderazgo y Cultura Organizacional en Seguridad de la Información apoyado por la Dirección de Gestión Humana y Desarrollo Organizacional
  - ✓ Promoviendo una cultura de ciberseguridad y privacidad entre todo el personal.
  - ✓ Fomentando campañas de concienciación sobre el manejo seguro de la información.
  - ✓ Aplicando con ejemplos: aplican buenas prácticas de seguridad en su propio trabajo.

- Supervisión y Seguimiento del PESI liderado por la Dirección de Gobierno Digital, Tecnología, Información
  - ✓ Realizando auditorías internas y revisando informes de seguridad periódicamente.
  - ✓ Evaluando el impacto del PESI y ajustando estrategias según resultados y nuevas amenazas.
  - ✓ Estableciendo indicadores clave (KPIs) para medir la efectividad de la seguridad de la información.

- Gestión de Incidentes y Respuesta a Crisis apoyado por todo el equipo directivo
  - ✓ Aprobando planes de respuesta ante incidentes de seguridad (ataques cibernéticos, fugas de datos).
  - ✓ Garantizando la comunicación efectiva en caso de una brecha de seguridad.
  - ✓ Respaldando acciones correctivas y preventivas para evitar futuros incidentes.

El respaldo del equipo directivo no solo fortalece la seguridad de la información en el hospital, sino que también protege la reputación institucional, mejora la confianza de los pacientes y garantiza la continuidad operativa sin interrupciones por incidentes digitales



7.3 Descripción del plan

Se realizará una fase de diagnóstico para la implementación del **Plan Estratégico de Seguridad de la Información (PESI)**, buscando evaluar el estado actual de la seguridad de la información en el Hospital, identificando vulnerabilidades y estableciendo una línea base para definir estrategias de mejora.

7.3.1. Objetivos de la Fase de Diagnóstico

- ✓ Identificar los activos de información críticos del hospital.
- ✓ Evaluar el cumplimiento normativo (Ley 1581 de 2012, Decreto 620 de 2020, ISO 27001).
- ✓ Analizar riesgos y vulnerabilidades en los sistemas hospitalarios.
- ✓ Revisar la cultura organizacional en seguridad de la información.
- ✓ Definir brechas y oportunidades de mejora en protección de datos y privacidad

7.3.2. Etapas del Diagnóstico

- Identificación y Clasificación de la Información
  - ✓ Listado de los datos sensibles que maneja el hospital (historias clínicas, datos administrativos, financieros).
  - ✓ Determinación de quiénes tienen acceso a esta información y en qué condiciones.
  - ✓ Clasificación de la información según su nivel de criticidad y confidencialidad.

- Evaluación de la Infraestructura Tecnológica
  - ✓ Análisis de los sistemas de información del hospital (Historia Clínica Electrónica, bases de datos, redes).
  - ✓ Revisión del uso de antivirus, firewalls, autenticación multifactor y otras medidas de seguridad.
  - ✓ Identificación de software y hardware obsoleto que pueda representar un riesgo.

- Análisis de Normativas y Cumplimiento
  - ✓ Verificación del cumplimiento de regulaciones nacionales e internacionales de protección de datos.
  - ✓ Revisión de contratos y acuerdos con terceros sobre el manejo seguro de la información.
  - ✓ Análisis de políticas internas de seguridad de la información.

- Evaluación de Riesgos y Amenazas
  - ✓ Identificación de posibles amenazas internas y externas (errores humanos, ciberataques, fallos tecnológicos).
  - ✓ Análisis de incidentes de seguridad previos y su impacto en la operatividad del hospital.
  - ✓ Priorización de riesgos según su nivel de criticidad y probabilidad de ocurrencia.

- Revisión de Cultura Organizacional y Capacitación
  - ✓ Encuestas y entrevistas con el personal para evaluar su conocimiento en seguridad de la información.
  - ✓ Revisión de capacitaciones previas en ciberseguridad y privacidad de datos.
  - ✓ Identificación de malas prácticas en el uso de la tecnología hospitalaria.

- Informe de Diagnóstico y Recomendaciones
  - ✓ Elaboración de un informe con los hallazgos detectados.
  - ✓ Definición de brechas en seguridad de la información y recomendaciones iniciales.
  - ✓ Priorización de acciones correctivas y preventivas para la siguiente fase del PESI

7.3.3. Herramientas para realizar el Diagnóstico

Políticas de Seguridad de la Información

- Acceso y Autenticación:
  - ✓ Uso de contraseñas seguras y cambio periódico obligatorio.
  - ✓ Acceso a sistemas solo para personal autorizado.

- ✓ Implementación de autenticación multifactor en sistemas críticos.

- Protección de Datos Sensibles:
  - ✓ Encriptación de datos en tránsito y en reposo.
  - ✓ Restricción de almacenamiento de información confidencial en dispositivos personales.
  - ✓ Copias de seguridad regulares y almacenamiento en servidores seguros.

- Normativas y Cumplimiento:
  - ✓ Aplicación de la Ley de Protección de Datos Personales en Salud.
  - ✓ Cumplimiento de estándares internacionales como ISO 27001 y normativas locales.

- Uso Seguro de Equipos y Sistemas:
  - ✓ Prohibición de instalación de software sin autorización.
  - ✓ No compartir credenciales de acceso.
  - ✓ Uso responsable del correo electrónico y prevención de phishing.

- Resguardo de la Información Física:
  - ✓ Restricción de acceso a áreas donde se almacenen registros físicos.
  - ✓ Destrucción segura de documentos sensibles.

Estrategias de Protección y Monitoreo

- ✓ Implementación de firewalls y antivirus actualizados.
- ✓ Auditorías periódicas de seguridad en los sistemas hospitalarios.
- ✓ Monitoreo constante de accesos y actividades sospechosas.
- ✓ Pruebas de penetración y evaluación de vulnerabilidades.

Capacitación y Concienciación

- ✓ Realización de talleres sobre ciberseguridad para el personal del hospital.
- ✓ Campañas de concienciación sobre buenas prácticas en el manejo de datos.
- ✓ Simulaciones de ataques informáticos (phishing, malware) para entrenar al personal.

Plan de Respuesta a Incidentes: En caso de brecha de seguridad, se seguirán los siguientes pasos:

- ✓ Identificación y reporte del incidente a las áreas responsables.
- ✓ Aislamiento y mitigación del problema.

- ✓ Análisis forense para determinar la causa.
- ✓ Comunicación del incidente a las autoridades y afectados (según normativas).
- ✓ Implementación de mejoras para evitar incidentes futuros.

Evaluación y Mejora Continua

- ✓ Auditorías regulares para evaluar la efectividad del plan.
- ✓ Análisis de riesgos y actualización de estrategias.
- ✓ Retroalimentación del personal para fortalecer medidas de seguridad.

8. Bibliografía

- Fortalecimiento de la tecnología de la información. Ministerio de Tecnología de la Información. Disponible en: https://mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-657.html#:~:text=La%20iniciativa%20de%20Fortalecimiento%20de%20las%20Tecnolog%C3%ADas%20de,y%20de%20la%20informaci%C3%B3n%20sea%20coordinada%20y%20eficiente.

- El plan de seguridad de la información de la empresa: cómo crearlo https://s2grupo.es/el-plan-de-seguridad-de-la-informacion-la-empresa-como-crearlo/

9. Anexos

N/A.

10. Control de Cambios

Versión	Ítem	Descripción del Cambio	Razón del Cambio	Elaborado por	Revisado por	Aprobado por	Fecha
01		Creación del documento	Plan de Seguridad y Privacidad de la Información	Diana Isabel Posada Villada Líder de Sistemas	José David Vélez Velasquez Gerente	José David Vélez Velásquez Gerente	29 de Enero de 2021
02		Modificación documento	Plan de Seguridad y Privacidad de la Información	Diana Isabel Posada Villada Directora Gobierno Digital, Tecnología e información	José David Vélez Velásquez Gerente	José David Vélez Velásquez Gerente	Enero 2022

Versión	Ítem	Descripción del Cambio	Razón del Cambio	Elaborado por	Revisado por	Aprobado por	Fecha
03		Modificación de foco en documento para 2023 con ejecución	Plan de Seguridad y Privacidad de la Información –actualización 2023	Diana Isabel Posada Villada Directora Gobierno Digital, Tecnología e información	José David Vélez Velásquez Gerente	José David Vélez Velásquez Gerente	Enero 2023
04		Actualización del Documento	Ajustes de escenario y avances generados en 2023	Ruth Nacarina Garzón Urrea Directora Gobierno Digital, Tecnología e información	José David Vélez Velásquez Gerente	José David Vélez Velásquez Gerente	31/01/2024
05		Actualización del Documento	Se actualiza por ajuste del Plan de Seguridad y Privacidad de la Información	Director Técnico Dirección de Gobierno Digital, Tecnologías e Información	Subgerente Administrativo y Financiero	Comité Institucional de Gestión y Desempeño	22/01/2025