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

Yeyson Nolberto Henao
Director Técnico Dirección de Gobierno Digital, Tecnologías e Información

Aprobado por

Comité Institucional de Gestión y Desempeño

Caldas Antioquia
Enero – 2026

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:

- **Decreto 767 de 2022** (que actualiza la Política de Gobierno Digital) [
- **Decreto 338 de 2022** (Gobernanza de Seguridad Digital)
- **Decreto 620 de 2020** (Servicios Ciudadanos Digitales)
- **Resolución 2277 de 2025** (actualización del MSPI)
- **Ley 1581 de 2012** (Protección de Datos Personales)
- **Resolución 2654 de 2019** (Telesalud y Telemedicina)

Alineación Normativa

Este PESI incorpora las actualizaciones normativas vigentes desde enero de 2026, incluyendo la Resolución 2277 de 2025 del MinTIC, que actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI) con nuevos estándares ISO 20001, así como el Decreto 767 de 2022 que define la Política de Gobierno Digital y el Decreto 338 de 2022 que establece la gobernanza de seguridad digital y la gestión de incidentes cibernéticos. Esto asegura que el hospital cumple con los estándares actuales de protección de información en el sector público colombiano.

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 Gobierno Digital, Tecnologías e Información de la ESE Hospital San Vicente de Paul de Caldas Antioquia, durante la vigencia 2025-2026, que responda a las necesidades de

preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información, en cumplimiento con la normativa vigente de Gobierno Digital y Seguridad Digital establecida en el Decreto 767 de 2022 y la Resolución 2277 de 2025

2.2 Objetivos Específicos

- Proteger los datos personales y clínicos de los pacientes, especialmente en servicios de telesalud conforme a Resolución 2654 de 2019.
- 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 y en el uso seguro de Servicios Ciudadanos Digitales.
- Comunicar e implementar la Estrategia de Seguridad de la Información alineada con Decreto 338 de 2022.
- 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 (MSPI), actualizado conforme a Resolución 2277 de 2025, 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, incluyendo la conformación de un CSIRT conforme al Decreto 338 de 2022.
- Establecer una metodología de gestión de seguridad de la información clara y estructurada, basada en Gobierno Digital.
- 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
Decreto 2150 de 1995	Supresión de trámites, reforma de regulaciones y procedimientos innecesarios

Norma	Descripción
Decreto 1122 de 1999	Normas para suprimir trámites y fortalecer eficiencia pública
Ley 594 de 2000	Ley de archivos - Gestión documental
Ley 80 de 1983	Estatuto general de contratación de administración pública
Ley 527 de 1999	Acceso y uso de mensajes de datos, comercio electrónico y firmas digitales
Ley 1150 de 2007	Disposiciones generales sobre contratación con recursos públicos
Ley 1273 de 2009	Protección de la información y de los datos
Ley 1266 de 2008	Habeas data
Ley 23 de 1982	Derechos de autor
Ley 1341 de 2009	Principios y conceptos sobre la sociedad de la información y las TIC
Ley 1438 de 2011	Reforma del Sistema General de Seguridad Social en Salud
Ley 1450 de 2011	Plan Nacional de Desarrollo 2010-2014 (racionalización de trámites)
Ley 1581 de 2012	Ley de protección de datos personales
Ley 1712 de 2014	Ley de transparencia y del derecho de acceso a la información pública
Ley 1978 de 2019	Modernización del sector TIC (actualiza Ley 1341)
Ley 2052 de 2020	Racionalización y digitalización de trámites en entidades públicas
Ley 2088 de 2021	Regulación del trabajo en casa
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC (base compilatoria)
Decreto 415 de 2016	Fortalecimiento institucional en materia de TIC en Función Pública
Decreto 620 de 2020	Lineamientos para Servicios Ciudadanos Digitales (autenticación, interoperabilidad, carpeta ciudadana)
Decreto 338 de 2022	Gobernanza de Seguridad Digital (gestión de riesgos, CSIRT, infraestructuras críticas cibernéticas)
Decreto 767 de 2022	Política de Gobierno Digital y lineamientos de transformación digital del Estado
Resolución 500 de 2021 (MinTIC)	MSPI - Lineamientos generales para implementar el Modelo de Seguridad y Privacidad de la Información
Resolución 746 de 2022 (MinTIC)	Ajustes y complementos a lineamientos del MSPI
Resolución 2277 de 2025 (MinTIC)	Actualización del MSPI y nuevos lineamientos de seguridad y privacidad digital (Anexo 1)
Resolución 1519 de 2020	Lineamientos de Gobierno Digital para transparencia, datos

Norma	Descripción
(MinTIC)	abiertos y accesibilidad
Resolución 2710 de 2017 (MinTIC)	Lineamientos para adopción de protocolo IPv6 (actualizada por Res. 1126/2021)
Resolución 1126 de 2021 (MinTIC)	Actualización de plazos e implementación de IPv6
Resolución 2893 de 2020 (MinTIC)	Lineamientos para sedes electrónicas, ventanillas únicas y servicios ciudadanos digitales
Resolución 1117 de 2022 (MinTIC)	Lineamientos para ciudades y territorios inteligentes
Resolución 2654 de 2019 (MinSalud)	Disposiciones para telesalud y parámetros de práctica de telemedicina
Resolución 3100 de 2019 (MinSalud)	Complementaria a telesalud y habilitación de servicios de salud
Resolución 400 de 2024 (MinSalud)	Requisitos técnicos y de capacidad para infraestructura hospitalaria
Decreto 1954 de 2012	Sistema de información de pacientes con enfermedades huérfanas
CONPES 4023 de 2021	Política para reactivación y crecimiento sostenible (habilitadores digitales)

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), alineado con el Decreto 767 de 2022 y la Resolución 2277 de 2025, aplica a:

- Todos los procesos, sistemas, equipos y usuarios que manejen información dentro del hospital
- Personal administrativo, asistencial, docentes e investigadores
- Proveedores externos y contratistas con acceso a sistemas hospitalarios
- Usuarios de servicios de telesalud y telemedicina (conforme Resolución 2654 de 2019).
- Historias clínicas electrónicas y datos personales sensibles de pacientes
- Infraestructuras de TI y sistemas de información críticos para continuidad de servicios.
- Servicios Ciudadanos Digitales implementados en la institución (Decreto 620 de 2020).

5. Responsables

- ✓ Director Técnico Dirección de Gobierno Digital, Tecnologías e Información
- ✓ Equipo Directivo
- ✓ Comité de Seguridad de la Información de la E.S.E. Hospital San Vicente de Paúl de Caldas ejercerá las funciones de CSIRT institucional, garantizando la prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital, en articulación con el CSIRT-Gobierno y conforme a lo dispuesto en el Decreto 338 de 2022.
  CSIRT (Computer Security Incident Response Team).

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.

CSIRT (Computer Security Incident Response Team): Equipo multidisciplinario responsable de detectar, responder y mitigar incidentes de seguridad digital en la institución, conforme al Decreto 338 de 2022.

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.

Gobierno Digital: Política pública que busca promover el uso y aprovechamiento de las TIC para consolidar un Estado competitivo e innovador, generando valor público en un entorno de confianza digital (Decreto 767 de 2022).

Gobernanza de Seguridad Digital: Marco de responsabilidades, procesos y controles para la gestión de riesgos de seguridad digital en infraestructuras críticas cibernéticas (Decreto 338 de 2022).

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.

MSPI (Modelo de Seguridad y Privacidad de la Información): Lineamientos técnicos, administrativos y de talento humano para la implementación de seguridad digital en entidades públicas, actualizado por Resolución 2277 de 2025.

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, fundamentadas en MSPI actualizado.

Servicios Ciudadanos Digitales (SCD): Soluciones tecnológicas transversales que brindan al Estado capacidades para su transformación digital, incluyendo Autenticación Digital, Interoperabilidad y Carpeta Ciudadana Digital (Decreto 620 de 2020).

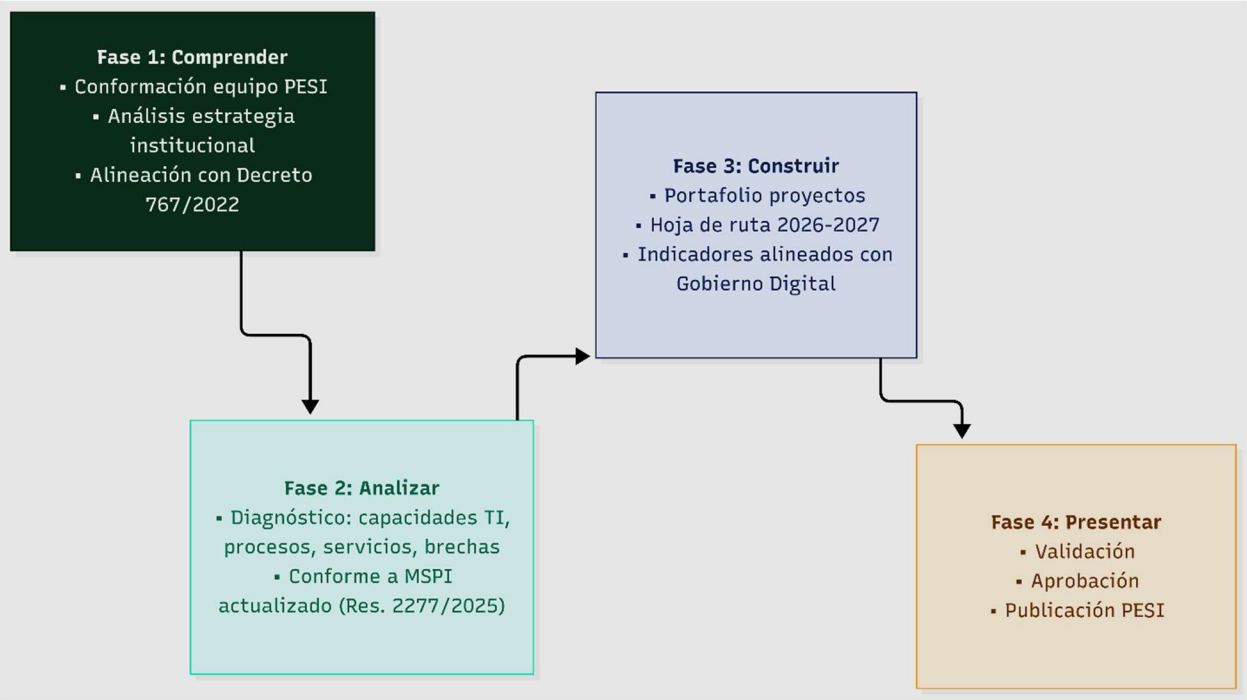
Telesalud: Provisión de servicios de salud utilizando tecnologías de información y comunicación, conforme a los parámetros de la Resolución 2654 de 2019

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 y Decreto 767 de 2022.
  - ✓ Aprobando las políticas de seguridad y privacidad de la información conforme a Resolución 2277 de 2025.
  - ✓ Garantizando el cumplimiento de normativas legales (Ley 1581 de 2012, Decreto 620 de 2020, Decreto 767 de 2022, Decreto 338 de 2022, Resolución 2277 de 2025, 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, alineadas con Gobierno Digital.
- ✓ Asignando recursos para la implementación de estrategias de respaldo de información que involucren respaldo On-Premise y en la Nube.

- **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 y Servicios Ciudadanos Digitales.
  - ✓ 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, conforme a MSPI actualizado.
  - ✓ 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.
  - ✓ Supervisando la gobernanza de seguridad digital conforme a Decreto 338/2022.

- **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), conforme a Decreto 338 de 2022.
  - ✓ 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, conforme a MSPI actualizado en Resolución 2277 de 2025.

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, Decreto 767 de 2022, Decreto 338 de 2022, Resolución 2277 de 2025, ISO 27001).
- ✓ Analizar riesgos y vulnerabilidades en los sistemas hospitalarios, incluyendo servicios de telesalud.
- ✓ Revisar la cultura organizacional en seguridad de la información.
- ✓ Definir brechas y oportunidades de mejora en protección de datos y privacidad.
- ✓ Establecer línea base MSPI conforme a Resolución 2277 de 2025.

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, considerando Resolución 2654 de 2019 para telesalud.

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

- **Análisis de Normativas y Cumplimiento**
  - ✓ Verificación del cumplimiento de regulaciones nacionales e internacionales de

protección de datos (Decreto 767 de 2022, Resolución 2277 de 2025.
- ✓ Revisión de contratos y acuerdos con terceros sobre el manejo seguro de la información.
- ✓ Análisis de políticas internas de seguridad de la información alineadas con Gobierno Digital.

- **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, conforme a Decreto 338/2022.
  - ✓ Identificación de infraestructuras críticas cibernéticas.

- **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 y Servicios Ciudadanos Digitales.

- **Informe de Diagnóstico y Recomendaciones**
  - ✓ Elaboración de un informe con los hallazgos detectados conforme a MSPI actualizado.
  - ✓ 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 doble factor de autenticación en sistemas críticos.
  - ✓ Acceso a Servicios Ciudadanos Digitales conforme a Decreto 620/2020

- **Protección de Datos Sensibles:**

- ✓ Encriptación de datos en tránsito y en reposo conforme a MSPI actualizado.
- ✓ Restricción de almacenamiento de información confidencial en dispositivos personales.
- ✓ Copias de seguridad regulares y almacenamiento en servidores seguros (En Nube y On-Premise.
- ✓ Protección especial de datos de telesalud conforme a Resolución 2654/2019.

- **Normativas y Cumplimiento:**
  - ✓ Aplicación de la Ley de Protección de Datos Personales en Salud.
  - ✓ Cumplimiento de estándares internacionales como ISO 27001 y normativas locales actualizadas (Decreto 767/2022, Resolución 2277/2025.

- **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.
  - ✓ Uso seguro de Servicios Ciudadanos Digitales.

- **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 conforme a MSPI.
- ✓ Monitoreo constante de accesos y actividades sospechosas realizado por CSIRT.
- ✓ Pruebas de penetración y evaluación de vulnerabilidades.
- ✓ Gestión de incidentes de seguridad digital conforme a Decreto 338/2022.

Capacitación y Concienciación

- ✓ Realización de talleres sobre ciberseguridad para el personal del hospital.
- ✓ Campañas de concienciación sobre buenas prácticas en el manejo de datos y Servicios Ciudadanos Digitales.
- ✓ 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 conforme a Decreto 338 de 2022:

- ✓ Identificación y reporte del incidente a las áreas responsables y CSIRT.
- ✓ 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 conforme a MSPI actualizado.
- ✓ Análisis de riesgos y actualización de estrategias alineadas con Gobierno Digital.
- ✓ Retroalimentación del personal para fortalecer medidas de seguridad.

8. Bibliografía

Normas y Decretos

- Decreto 2150 de 1995 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=1208
- Decreto 1122 de 1999 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=31431
- Ley 1341 de 2009 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=98210
- Ley 1438 de 2011 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43101
- Ley 1450 de 2011 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43101
- Ley 1581 de 2012 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43101
- Ley 1712 de 2014 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43101
- Ley 1978 de 2019 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186766
- Ley 2052 de 2020 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=140250
- Decreto 1078 de 2015 https://normograma.mintic.gov.co/mintic/compilacion/
- Decreto 415 de 2016

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186766

- Decreto 620 de 2020 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=118337
- Decreto 338 de 2022 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866
- Decreto 767 de 2022 https://normograma.mintic.gov.co/mintic/compilacion/docs/decreto_0767_2022.htm
- Resolución 500 de 2021 https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf
- Resolución 746 de 2022 https://gobiernodigital.mintic.gov.co/692/articles-238199_recurso_1.pdf
- Resolución 2277 de 2025 (ACTUALIZACIÓN CRÍTICA) https://normograma.mintic.gov.co/mintic/compilacion/docs/resolucion_mintic_2277_2025.htm
- Resolución 1519 de 2020 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43101
- Resolución 2710 de 2017 https://gobiernodigital.mintic.gov.co/692/w3-article-272784.html
- Resolución 1126 de 2021 https://gobiernodigital.mintic.gov.co/692/w3-article-272784.html
- Resolución 2893 de 2020 https://gobiernodigital.mintic.gov.co/692/w3-article-272784.html
- Resolución 1117 de 2022 https://gobiernodigital.mintic.gov.co/692/w3-article-272784.html
- Resolución 2654 de 2019 https://www.minsalud.gov.co/normatividad_nuevo/Resolucion%202654%20de%202019.pdf
- Resolución 3100 de 2019 https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/resolucion_minsaludps_3100_2019.htm
- Resolución 400 de 2024 https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=153569
- Decreto 1954 de 2012 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43101

Documentos de Referencia MinTIC

- Guía de Construcción PETI v3.0
  https://gobiernodigital.mintic.gov.co/692/w3-article-272784.html
- Manual de Gobierno Digital
  https://gobiernodigital.mintic.gov.co/692/w3-propertyvalue-47326.html
- Marco de Referencia de Arquitectura Empresarial MRAE v3.0
  https://gobiernodigital.mintic.gov.co/692/w3-propertyvalue-47245.html

Referencias Adicionales

- CONPES 4023 de 2021 - Política para reactivación y crecimiento sostenible
  https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4023.pdf
- Gestor Normativo Función Pública (para todas las normas)
  https://www.funcionpublica.gov.co/eva/gestornormativo/normasfp.php
- Normograma MinTIC
  https://normograma.mintic.gov.co/mintic/compilacion.

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
03		Modificación de foco en documento para 2023	Plan de Seguridad y Privacidad de la Información – actualización 2023	Diana Isabel Posada Villada Directora	José David Vélez Velásquez	José David Vélez Velásquez Gerente	Enero 2023

Versión	Ítem	Descripción del Cambio	Razón del Cambio	Elaborado por	Revisado por	Aprobado por	Fecha
		con ejecución		Gobierno Digital, Tecnología e información	Gerente		
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
06		Actualización del Documento	Se actualiza por revisión general del documento y ajuste en: - Introducción Incorporación de Resolución 2277/2025, Decreto 767/2022, Decreto 338/2022, Decreto 620/2020. - Eliminación de Decreto 1008/2018. - Se complementan Objetivos Específicos - Se actualiza Marco Legal - Se complementa el alcance. - Se adiciona responsable - Se adicionan definiciones - Se ajusta ítem 7.1 Metodología (grafico). - Se amplia información ítem 8.2 Estructura.	Director Técnico Dirección de Gobierno Digital, Tecnologías e Información	Subgerente Administrativo y Financiero	Comité Institucional de Gestión y Desempeño	20/01/2026

Versión	Ítem	Descripción del Cambio	Razón del Cambio	Elaborado por	Revisado por	Aprobado por	Fecha
			- Se amplia información ítem 8.3 Descripción del Plan y de los ítems 8.3.1, 8.3.2, 8.3.3 - Se adicionan referencias bibliográficas.				