E.S.E. Hospital SAN JUAN DE DIOS PAMPLONA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

CONTENIDO

INTRODUCCION

La E.S.E. Hospital San Juan de Dios de Pamplona reconoce que la información es un activo institucional crítico. En un entorno con incremento de servicios digitales, uso de herramientas colaborativas, intercambio de información con terceros y modalidades híbridas de trabajo, se hace necesario fortalecer prácticas para asegurar la confidencialidad, integridad, disponibilidad y trazabilidad.

Este Plan de Seguridad y Privacidad de la Información para la vigencia 2026 consolida lineamientos mínimos para el uso de activos, la administración de accesos, el manejo de credenciales, el uso de Internet e intranet, la protección frente a software malicioso, el respaldo y recuperación de información, y el tratamiento de datos personales y datos sensibles. Se articula con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad y con el Plan de Preservación Digital institucional.

1. OBJETIVO GENERAL

Actualizar y aplicar el Plan de Seguridad y Privacidad de la Información de la E.S.E. Hospital San Juan de Dios de Pamplona para la vigencia 2026, definiendo lineamientos y acciones que protejan los activos de información y el tratamiento de datos personales.

1.1. OBJETIVOS ESPECIFICOS

- Establecer lineamientos generales para el manejo seguro de la información y de los activos tecnológicos asociados.
- Promover prácticas de seguridad y privacidad en funcionarios, contratistas, practicantes y proveedores con acceso a información institucional.
- Fortalecer controles de acceso, uso de credenciales, respaldo, recuperación y trazabilidad sobre sistemas y repositorios institucionales.
- Alinear la gestión de seguridad y privacidad con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y con buenas prácticas de un SGSI.
- Implementar y hacer seguimiento al plan de acción 2026 con evidencias e indicadores verificables.

2. ALCANCE, EXCLUSIONES Y LIMITACIONES

2.1 Alcance

Aplica a la totalidad de dependencias, procesos, sedes y colaboradores de la E.S.E. y cubre información en cualquier soporte (digital o físico) que sea creada, almacenada, transmitida o consultada en la entidad, incluyendo equipos, redes, correo institucional, repositorios documentales, copias de respaldo y sistemas misionales y administrativos.

2.2 Exclusiones

Cualquier exclusión debe formalizarse mediante acta o memorando, indicando el responsable, la justificación, controles compensatorios y fecha de revisión.

2.3 Limitaciones

La ejecución del plan depende de disponibilidad presupuestal y capacidad operativa. En 2026 se recomienda priorizar inversiones y acciones en: (i) respaldo y recuperación, (ii) protección de endpoints, (iii) control de accesos y (iv) capacitación y concientización.

3. MARCO LEGAL Y NORMATIVO

Este plan toma como referencia normativa y técnica, entre otros, los siguientes instrumentos:

- ISO/IEC 27001:2013 - Sistema de Gestión de Seguridad de la Información (SGSI).
- NTC-ISO/IEC 27001 (equivalente nacional, según adopción vigente).
- Ley 1581 de 2012 - Protección de Datos Personales y normas complementarias.
- Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública.
- Ley 1273 de 2009 - Delitos informáticos (modifica el Código Penal).
- Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC, para entidades públicas.

4. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (CONCEPTOS BASE)

La seguridad de la información se entiende como la preservación de la confidencialidad, integridad y disponibilidad de la información; además puede involucrar autenticidad, trazabilidad, no repudio y fiabilidad.

- Integridad: salvaguardar la exactitud y el estado completo de los activos de información.
- Disponibilidad: que la información sea accesible y utilizable cuando sea requerida por una entidad autorizada.
- Confidencialidad: que la información no sea revelada a individuos, entidades o procesos no autorizados.

La privacidad de la información se relaciona con el tratamiento adecuado de datos personales y datos sensibles, garantizando que su recolección, uso, circulación y almacenamiento se realicen con finalidad legítima, acceso controlado y medidas de seguridad acordes al riesgo.

5. LINEAMIENTOS GENERALES PARA EL MANEJO DE LA INFORMACIÓN

5.1 Gestión de activos

Cada dependencia debe mantener inventario actualizado de activos tecnológicos y repositorios bajo su responsabilidad, identificando propietario funcional y administrador técnico, y reportando movimientos o cambios a Almacén y a la Oficina de Informática y Estadística.

Se recomienda complementar el inventario con criticidad y clasificación de información asociada al activo (pública, interna, confidencial y sensible).

5.2 Acceso a la información

Los accesos a sistemas y repositorios deben otorgarse bajo el principio de mínimo privilegio, con autorización del responsable del proceso y revisión periódica de permisos. Se deben conservar evidencias (solicitud, aprobación, cambio aplicado) y registros de acceso cuando aplique.

Para requerimientos de acceso por terceros (externos), se debe verificar base legal, finalidad, autorización y medidas de seguridad, con acta o documento soporte.

5.3 Uso de usuarios y contraseñas

- Cada usuario debe contar con credenciales personales e intransferibles; está prohibido compartir cuentas.
- Aplicar contraseñas robustas para sistemas críticos y cuentas con privilegios; cambiar claves iniciales al primer ingreso.
- Implementar autenticación reforzada (por ejemplo, segundo factor) para correo institucional y accesos críticos cuando sea posible.
- Formalizar procedimiento de altas, bajas y cambios (ingreso, retiro y cambios de rol), con tiempos máximos de ejecución.

5.4 Uso de Internet/Intranet y redes Wi-Fi

El acceso a Internet e intranet es un activo institucional y debe usarse exclusivamente para fines laborales. En 2026 se recomienda implementar controles de navegación por categorías, monitoreo y segmentación de redes (incluyendo Wi-Fi) para reducir exposición a riesgos (phishing, descargas maliciosas, fuga de información).

- Prohibido envío, descarga o visualización de contenido ofensivo, ilegal o que afecte la imagen institucional.
- Evitar descargas de software no autorizado y uso de servicios no aprobados para compartir información institucional.
- El personal debe reportar correos o enlaces sospechosos a la Oficina de Informática y Estadística.

5.5 Uso de dispositivos de almacenamiento externo (USB)

Se permite el uso de medios externos únicamente cuando sea necesario para funciones institucionales. En 2026 se recomienda:

- Autorizar y registrar el uso de USB para dependencias que lo requieran (control de préstamo o registro).
- Escanear medios externos antes de su uso en equipos institucionales.
- Evitar transportar datos sensibles sin cifrado o sin autorización del responsable del proceso.
- Restringir el uso de medios externos de procedencia desconocida.

5.6 Seguridad de la información y confidencialidad

- Funcionarios y contratistas deben garantizar custodia, confidencialidad y uso adecuado de la información bajo su manejo.
- El software institucional está destinado exclusivamente al cumplimiento de funciones; se prohíbe su copia o uso para fines ajenos.
- En trabajo fuera de sede: no compartir pantalla con terceros, no almacenar información sensible en dispositivos personales sin autorización, y bloquear sesión al ausentarse.

5.7 Uso de impresoras y escáneres

- Promover impresión responsable (doble cara, uso de correo y medios digitales).
- No imprimir documentos personales en equipos institucionales.
- Evitar dejar documentos impresos sin supervisión; disponerlos según lineamientos de gestión documental.

5.8 Seguridad física y en el entorno

Las áreas de infraestructura tecnológica (servidores, equipos de red, UPS y cableado) deben mantenerse con acceso restringido, registro de ingreso y condiciones ambientales controladas. Se deben realizar mantenimientos preventivos y verificaciones periódicas.

5.9 Control de software malicioso y vulnerabilidades

Se implementan controles para reducir malware, ransomware y explotación de vulnerabilidades. En 2026 se prioriza:

- Protección antimalware/endpoint con actualización centralizada cuando aplique.
- Gestión de parches y actualizaciones de sistemas operativos y aplicaciones.
- Buenas prácticas frente a correos sospechosos y adjuntos (phishing).

5.10 Almacenamiento y respaldo de la información

Los sistemas misionales y administrativos deben contar con copias de seguridad, bitácoras y pruebas de restauración. En 2026 se recomienda estandarizar el esquema de respaldo (frecuencia, medios, responsables) y adoptar pruebas trimestrales documentadas.

5.11 Revisión de equipos externos y acceso remoto

El soporte remoto debe realizarse únicamente por canales autorizados. Para equipos externos con acceso a recursos institucionales, se recomienda definir condiciones mínimas: antivirus, parches al día, contraseña, bloqueo de pantalla y autorización formal.

5.12 Gestión de incidentes

Se establece un procedimiento de reporte y respuesta ante incidentes de seguridad y privacidad (por ejemplo, pérdida de equipo, phishing exitoso, fuga de información, malware). Debe definirse un canal de reporte, responsables, tiempos de contención y registro de lecciones aprendidas.

5.13 Proveedores y terceros

Los proveedores con acceso a información o infraestructura deben cumplir cláusulas de confidencialidad y seguridad, acceso por mínimo privilegio y revocación al finalizar el contrato.

6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI - MINTIC)

El MSPI del MinTIC orienta el diagnóstico, planificación, implementación, evaluación de desempeño y mejora continua de la seguridad y privacidad en entidades públicas. En 2026, este plan organiza acciones bajo dichas fases para facilitar seguimiento y auditoría.

Fases del ciclo de operación

- Diagnóstico
- Planeación
- Implementación
- Evaluación de desempeño
- Mejora continua

7. PLAN DE ACCIÓN 2026 (ACTIVIDADES, RESPONSABLES, EVIDENCIAS E INDICADORES)

El plan de acción consolida actividades mínimas para la vigencia 2026. Las fechas pueden ajustarse según priorización y recursos, manteniendo evidencia verificable.

Fase	Actividad	Responsable	Entregable	Periodo	Indicador
Diag.	Actualizar diagnóstico del estado de seguridad y privacidad	Of. Informática y Estadística	Informe diagnóstico 2026	T1	Emitido (Sí/No)
Plan.	Actualizar inventario de activos (incluye repositorios documentales)	TI + Dependencias	Inventario consolidado y aprobado	T1-T2	% dependencias reportan
Plan.	Revisión ABM (altas/bajas/cambios) y revocación de accesos de retirados	Of. Informática y Estadística	Acta/registro de revisión y bajas	Mensual	# cuentas inactivadas / # retiros
Plan.	Definir política de contraseñas y procedimiento ABM	Of. Informática y Estadística	Documento aprobado y socializado	T1	Aprobado (Sí/No)
Impl.	Reforzar autenticación para correo y accesos críticos (si aplica)	Of. Informática y Estadística	Evidencia configuración + usuarios	T2-T3	% cuentas críticas con 2FA
Impl.	Monitoreo de ancho de banda y eventos del router	Of. Informática y Estadística	Bitácora/reportes de monitoreo	Quincenal	# reportes
Impl.	Lineamientos de navegación segura y control por categorías (si aplica)	Of. Informática y Estadística	Configuración + comunicado	T2-T4	Control activo (Sí/No)
Impl.	Protección antimalware y gestión de parches en endpoints	Of. Informática y Estadística	Inventario + reporte de parches	T1-T4	% equipos al día
Impl.	Estandarizar backups (sistemas críticos y repositorios) y bitácora	Of. Informática y Estadística	Política/cronograma + bitácora	T1-T4	% backups completados
Impl.	Prueba de restauración documentada (muestra)	Of. Informática y Estadística	Acta/bitácora de restauración	Trimestral	# pruebas OK / #
Impl.	Capacitación en phishing y manejo seguro de información	TI + Talento Humano	Material + asistencia + evaluación	Semestral	# asistentes / #
Eval.	Medición de indicadores y avance del plan	Of. Informática y Estadística	Informe de desempeño	Trimestral	% actividades ejecutadas
Mej.	Revisión de incidentes y acciones correctivas	TI + Control Interno	Registro incidentes + plan mejora	Semestral	# acciones cerradas / #
Mej.	Actualización anual del plan para la vigencia siguiente	Of. Informática y Estadística	Versión 2027 propuesta	T4	Generado (Sí/No)

8. SEGUIMIENTO Y MEJORA CONTINUA

El seguimiento se recomienda con periodicidad trimestral, verificando ejecución, evidencias e indicadores. Los hallazgos deben traducirse en acciones correctivas y preventivas, y en ajustes al plan y a los procedimientos.