ESE Hospital
San Juan de Dios
Santa Fe de Antioquia

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SANTIAGO VARELA MACIAS

GERENTE

JUAN DAVID ECHEVERRY CARGES

INGENIERO DE SISTEMAS

2026

CONTENIDO

1. INTRODUCCIÓN

Este documento busca lograr la implementación en el Hospital San Juan de Dios las mejoras prácticas dadas por el Departamento de 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.

El Modelo 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.

2. OBJETIVO GENERAL

Contar con un documento institucional que contenga los lineamientos de seguridad y privacidad de la información, alineadas con las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

3. OBJETIVOS ESPECIFICOS

1. Garantizar el cumplimiento de la **política de seguridad de la información** por parte de todos los funcionarios, contratistas, visitantes y terceros con relación al hospital.
2. Proteger la confidencialidad de la información generada, transmitida y almacenada por la institución.
3. Establecer y difundir procedimientos institucionales que aseguren un uso óptimo de las tecnologías de la información.
4. Diseñar y ejecutar programas de capacitación sobre buenas prácticas de seguridad digital para los colaboradores de la institución.
5. Mitigar riesgos asociados a ciberataques, accesos no autorizados y manipulación indebida de los datos.

4. ALCANCE

Esta normativa es aplicable en toda la E.S.E. Hospital San Juan de Dios y se deriva de las directrices generales definidas en la Política de Seguridad de la Información del Área de Tecnologías de la información. Su cumplimiento es obligatorio para todo el personal que preste servicios permanentes o eventuales, incluyendo contratistas y personal externo con acceso a los sistemas de información institucionales.

5. RESPONSABLE DEL PLAN

El liderazgo y la coordinación del **Plan de Seguridad y Privacidad de la Información** estará a cargo del **Área de Tecnologías y Sistemas de Información** del hospital, cuyos responsables deberán:

- Gestionar los recursos necesarios (humanos, tecnológicos, financieros y técnicos) para garantizar la implementación del plan.
- Monitorear el cumplimiento de las acciones planificadas.
- Coordinar con otras áreas institucionales para la ejecución de las medidas establecidas.

Además, los responsables designados deberán rendir informes periódicos sobre los avances y resultados obtenidos.

6. DEFINICIONES

Se incluyen las definiciones clave para garantizar una interpretación uniforme del plan:

- **Contraseña:** Es una clave que permite acceder a un lugar, ya sea en el mundo real o en el virtual. Las contraseñas se utilizan por varios motivos: para preservar la intimidad, para mantener un secreto, como una medida de seguridad o como una combinación de todo ello.

- **Encriptar:** Ocultar datos mediante una clave para que no puedan ser interpretados por los que no la tienen.

* **Backup:** Duplicado de un archivo informático que se guarda en previsión de la pérdida o destrucción del original': «Sería conveniente que hiciera una copia de seguridad de estos archivos» (Bustos Multimedia [Esp. 1996]). Esta es la expresión que debe usarse en español en sustitución del anglicismo back-up o Backups. Se dice también, especialmente en América, (copia de) resguardo o respaldo.

* **WinSCP:** es una aplicación de Software Libre. WinSCP es un cliente SFTP gráfico para Windows que emplea SSH. También se puede seguir usando la versión anterior del protocolo. Su función principal es facilitar la transferencia segura de archivos entre dos sistemas informáticos, el local y uno remoto que ofrezca servicios SSH.
* **ISO:** International Standard Organization.
* **MINTIC:** Ministerio de Tecnología de la Información y las Comunicaciones.
* **MOP:** Modelo de operación por procesos.
* **SPI**: Modelo de Seguridad y Privacidad de la Información.
* **SGSI:** Sistema de Gestión de Seguridad de la Información.
* **TI:** Tecnología de información.
* **TIC:** Tecnologías de la información y la comunicación.
- **Activo de Información:** Cualquier recurso que contenga datos valiosos para la organización, incluyendo sistemas, bases de datos y archivos.
- **Confidencialidad:** Propiedad que asegura que la información solo sea accesible por personas autorizadas.
- **Integridad:** Garantía de que la información es precisa y no ha sido alterada sin autorización.
- **Disponibilidad:** Aseguramiento de que los activos de información estén accesibles cuando se requieran.
- **Copia de Seguridad:** Duplicado de los datos realizado para prevenir pérdidas ante fallos o incidentes.
- **SGSI:** Sistema de Gestión de Seguridad de la Información basado en normas internacionales como **ISO/IEC 27001:2013**.

7. MARCO NORMATIVO

* Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
* Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
* Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
* Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
* Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
* Ley 594 de 2000 - Ley General de Archivos
* Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
* Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
* Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
* Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
* Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
* Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
* Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
* Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
* Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 2364 de 2012 - Firma electrónica
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.

8. DESARROLLO DEL PLAN

La E.S.E. Hospital San Juan de Dios consciente que la información es un activo valioso, definirá mecanismos que fortalezcan la capacidad del sistema para evitar las amenazas latentes en el entorno, los accesos no autorizados, la manipulación o deterioro la información almacenada en él y fomentar el adecuado manejo de la información generada en los procesos Institucionales.

La institución se compromete a establecer las acciones para hacer cumplir la Ley y los reglamentos que, para el manejo de la información administrativa y técnica del Usuario, estén vigentes:

8.1. Confidencialidad

1. Implementar mecanismos que aseguren el acceso restringido a la información sensible.
2. Establecer acuerdos de confidencialidad para todos los usuarios internos y externos con acceso a los sistemas institucionales.
3. Clasificar y etiquetar los activos de información según su nivel de sensibilidad.

8.2. Seguridad

1. Instalar sistemas de firewall para proteger los accesos a la red.
2. Implementar sistemas de monitoreo de actividad y detección de intrusiones.
3. Proteger los entornos físicos donde se resguarde información, asegurando condiciones climáticas y de seguridad.

8.3. Privacidad

1. Garantizar el cumplimiento de la **Ley 1581 de 2012** sobre protección de datos personales.
2. Diseñar procedimientos para la recolección y el manejo adecuado de datos personales.
3. Realizar auditorías periódicas para verificar el cumplimiento de las normas de privacidad.

8.4. Capacitación

1. Realizar talleres de sensibilización sobre ciberseguridad dirigidos a todos los colaboradores.
2. Actualizar a los usuarios sobre modificaciones normativas y tecnológicas.
3. Crear guías y manuales de buenas prácticas en la gestión de información.

9. SEGUIMIENTO

Para garantizar el cumplimiento de la política de seguridad del sistema de información, desde el Área de TI se implementan las siguientes medidas:

1. Capacitar periódicamente a los usuarios del sistema en la **Política de Seguridad de la Información**.
2. Notificar a los usuarios sobre modificaciones realizadas en la política de seguridad.
3. Actualizar, monitorear y reportar posibles fallos en los softwares institucionales, garantizando que las actualizaciones sean justificadas y evitando la proliferación de virus.
4. Utilizar plataformas seguras con sistemas de cortafuegos (firewall) para controlar accesos no autorizados desde Internet.
5. Definir perfiles de acceso para usuarios internos, estableciendo permisos acordes con las funciones de cada cargo.
6. Disponer de espacios adecuados para el resguardo de información en distintos medios (servidores NAS, papel, medios electrónicos o magnéticos), generando informes trimestrales sobre su uso.
7. Garantizar que las áreas de custodia de documentación en la nube cuenten con condiciones ambientales controladas (temperatura, humedad, ventilación e iluminación).
8. Implementar sistemas de almacenamiento específicos para documentos físicos, como gabinetes y estanterías, bajo la supervisión de responsables asignados.
9. Dotar a las áreas del hospital con suministros de seguridad (extintores, reguladores de corriente, etc.) para prevenir pérdidas de información por emergencias.
10. Garantizar respaldos regulares de información en servidores internos y externos.
11. Asegurar que todos los usuarios internos (contratistas, funcionarios) depuren información obsoleta para mejorar el control y archivo, bajo la orientación del Área de TI
12. Supervisar y aprobar la divulgación de información institucional bajo el control del Área de Sistemas y la alta gerencia.

9.1 NORMATIVIDAD DE CONTRASEÑAS

El objetivo de esta norma es garantizar la creación y uso de contraseñas robustas como mecanismo principal de autenticación. Las directrices son las siguientes:

1. Las contraseñas serán de uso exclusivo y personal.
2. Deben ser fáciles de recordar, pero difíciles de adivinar o descubrir mediante ataques de fuerza bruta.
3. Se prohíbe el uso de datos personales evidentes (nombre, apellidos, fechas de nacimiento, etc.) en la contraseña.
4. Longitud mínima de 8 caracteres, incluyendo al menos:
    - Una letra mayúscula.
    - Un carácter especial.
    - Números no consecutivos.
5. Las contraseñas deben cambiarse al menos tres veces al año o inmediatamente al sospechar una violación de seguridad.
6. No deben compartirse ni anotarse en lugares no seguros.
7. El Área de TI debe documentar las contraseñas de seguridad internas y protegerlas adecuadamente.

9.2 SISTEMA DE VERIFICACION DE CONTRASEÑAS:

* Prohibición de mecanismos para recordar contraseñas: El sistema de verificación no debe ofrecer opciones al usuario para recordar contraseñas, como preguntas de seguridad del tipo: “¿Cómo se llamaba tu primera mascota?” o similares.
* Validación de contraseñas contra listas negras: El sistema debe comparar las nuevas contraseñas de los usuarios con una lista negra de contraseñas no permitidas. Esta lista incluirá contraseñas ampliamente usadas, predecibles o comprometidas, como combinaciones de caracteres repetitivos (“12345678”), secuenciales (“1234abcd”) o palabras relacionadas con el contexto, tales como el nombre de la organización, el servicio o sus derivados. En caso de que la contraseña coincida con alguna de estas características, el sistema deberá rechazarla e instar al usuario a crear una nueva.

- Límite de intentos fallidos: El sistema debe implementar un límite al número de intentos de acceso fallidos para prevenir ataques de fuerza bruta.
- Visualización opcional de la contraseña: Aunque la contraseña se oculte por defecto, el sistema debe permitir al usuario visualizar su contenido si lo solicita, siempre que esté en un entorno confiable.
- Cifrado y canales seguros: El sistema debe emplear algoritmos de cifrado autorizados y garantizar el uso de canales protegidos al solicitar contraseñas al usuario.
- Almacenamiento seguro de contraseñas: Las contraseñas de los usuarios deben almacenarse utilizando métodos seguros, como hashing y salting, para hacerlas resistentes a ataques offline.

10. COPIAS DE SEGURIDAD

Las copias de seguridad son de gran importancia porque el activo más importante es la información, hoy en día todo depende de la información almacenada en el servidor, pero si por alguna razón como desastre natural o incendio, inundación falla de la computadora, entre otros, hay pérdida de esta información y es virtualmente imposible recuperarla sin copias de seguridad.

Todos los colaboradores de la E.S.E. Hospital San Juan de Dios tienen sus datos almacenados en nuestros archivos compartidos y es el resultado de mucho esfuerzo y trabajo que ha realizado durante un largo período de tiempo, es por eso por lo que un pequeño fallo siempre inesperado puede acabar con años de trabajo en un instante.

Esta guía intenta explicar por qué hacer copias de seguridad es una operación necesaria y muy útil y también muestra cómo crear una copia de seguridad de la información.

Objetivo: Establecer una guía práctica y realista para la ejecución de copias de seguridad, con el fin de proteger la información institucional, garantizar su disponibilidad y contar con procedimientos claros para la restauración y el adecuado tratamiento de los datos en caso de pérdida, daño, corrupción o incidente de seguridad.
Debido a las limitaciones actuales de personal especializado y a la ausencia de un proveedor externo dedicado exclusivamente a los servicios de respaldo, esta guía define un proceso básico, alcanzable y progresivo que permita al Hospital mantener un nivel razonable de protección de la

información, priorizando los sistemas críticos.

Alcance: La presente guía aplica a los servidores y sistemas de información institucionales que requieren la realización de copias de seguridad periódicas. Incluye:

- La identificación de las carpetas, bases de datos y sistemas que requieren respaldo.
- La programación y ejecución de las copias de seguridad mediante las herramientas disponibles en el hospital, actualmente Google Workspace (Drive de trabajo), respaldos manuales, y en algunos casos herramientas como Acronis cuando el servicio esté disponible.
- El almacenamiento seguro de las copias realizadas.
- Los procedimientos básicos de restauración y recuperación de información por parte del personal del área de TI.

El alcance considera las capacidades reales del Hospital San Juan de Dios, incluyendo la limitación de contar con un equipo reducido en el área de TI, lo que impide la implementación completa y diaria de un proceso formal de copias de seguridad bajo estándares internacionales. Por esta razón, el proceso se orienta a:

- Priorizar información crítica.
- Mantener al menos un nivel mínimo de protección.
- Documentar las actividades ejecutadas.
- Permitir una futura ampliación cuando se cuente con más personal o un proveedor especializado.

Generalidades: El área de TI es responsable de definir, administrar y ejecutar los mecanismos de respaldo necesarios para proteger la información institucional almacenada en los servidores y servicios digitales del Hospital San Juan de Dios. El propósito es reducir el riesgo de pérdida de información ocasionada por fallas técnicas, errores humanos o eventos externos.

Sin embargo, debido a la limitación de personal especializado y a la ausencia de una empresa dedicada exclusivamente a la administración de copias de seguridad, el proceso no puede

realizarse al 100% bajo estándares ideales. Por esta razón, se adopta un modelo de copias de seguridad progresivo y basado en prioridades, orientado a mantener la continuidad operativa de los sistemas más críticos.

Recomendaciones: El proceso de copias de seguridad requiere monitoreo constante, verificación de la ejecución de las tareas programadas, validación de la integridad de los archivos respaldados y pruebas periódicas de restauración. Sin embargo, el Hospital actualmente no cuenta con el personal especializado suficiente ni con la disponibilidad horaria necesaria para realizar este seguimiento de manera diaria y rigurosa.

Debido a esta limitación operativa, existe el riesgo de que algunas copias automáticas no se ejecuten correctamente sin que el área de Sistemas pueda detectarlo oportunamente. Por lo tanto, se recomienda formalmente la contratación de una empresa especializada en servicios de respaldo, que asuma de manera dedicada las funciones de:

* Ejecución y validación diaria de las copias.
* Monitoreo en tiempo real de fallas o interrupciones.
* Pruebas periódicas de restauración.
* Gestión de almacenamiento en la nube o en infraestructura híbrida.
* Emisión de reportes técnicos y auditorías de backup.

Contar con un proveedor experto permitiría elevar el nivel de cumplimiento, disminuir los riesgos asociados a fallas en la copia o restauración, y garantizar la continuidad del servicio incluso cuando el equipo interno tenga cargas de trabajo adicionales, ausencias o limitaciones de tiempo.

Mientras se logra esta contratación, se recomienda:

* Mantener configuradas las tareas automáticas de backup para reducir la dependencia del monitoreo manual.
* Priorizar los respaldos de los sistemas más críticos (información clínica y administrativa esencial).
* Evitar el uso de nombres demasiado largos en los archivos, ya que pueden generar errores al momento de copiar.
* Nombrar los archivos de forma clara y estandarizada para facilitar la restauración.

* Realizar depuración periódica de las carpetas institucionales para evitar respaldar información innecesaria o personal.

11. PROGRAMACION DE ESTRATEGIAS Y ACTIVIDADES

ESTRATEGIAS	ACTIVIDADES	RESPONSABLE	PLAZOS	MEDIOS DE VERIFICACIÓN
CAPACITACIONES	Capacitación de uso y creación de contraseñas seguras para personal administrativo	Área de TI	30 mayo	Formato de lista de asistencia
	Capacitación ciberseguridad para personal administrativo	Área de TI con proveedor especializado	Cada tres meses	Formato de lista de asistencia
REVISION DE POLITICA DE ROLES Y PERMISOS	Revisión y análisis de política de Roles y permisos de TI para usuario final	Área de TI	Abril 15	Circular en intranet o página web
REVISION DE POLITICA DE CORREOS	Revisión y análisis de política de correos para migración	Área de TI	30 junio	Circular en intranet o página web

12. PRESUPUESTO

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
CAPACITACIONES	4	$ 4’500.000	$ 18.000.000
TOTAL			$ 18.000.000

13. EVALUACIÓN

INDICADOR	FÓRMULA	META	FRECUENCIA
Control de amenazas web en equipo de computo	Total = host con antivirus instalado/ cantidad de host	90%	Anual
Control de ataques cibernéticos	Total = tráfico de peticiones web / peticiones totales al servidor	80%	Trimestral

14. DOCUMENTACIÓN DE REFERENCIA

CÓDIGO	NOMBRE
DECRETO NÚMERO 1317 DE 2013	El presente **Decreto** tiene como objeto reglamentar parcialmente la **Ley** 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Artículo 2°. Tratamiento de datos en el ámbito personal o doméstico.
UNE - ISO/IEC 27002:2005	proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.
UNE - ISO/IEC 27001:2007	Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
ISO/IEC 9001:2000 Sistemas de gestión de la calidad.	La Norma ISO 9001 especifica los requisitos para un sistema de gestión de la calidad que puedan utilizarse para su aplicación interna por las organizaciones, para certificación o con fines contractuales. Se centra en la eficacia del sistema de gestión de la calidad para dar cumplimiento a los requisitos del cliente.1 ene 2005

15. ELABORACIÓN, REVISIÓN Y APROBACIÓN

15.1 CONTROL DEL CAMBIOS					
VERSIÓN	**FECHA**	**DESCRIPCIÓN**	**ELABORÓ**	**REVISÓ**	**APROBÓ**
01	Enero 2023	Elaboración del plan 2023	Juan David Echeverry – Líder de sistemas	Nallybe Durán – Subgerente de Calidad	Claudia María Calderón – Gerente
02	Enero 2024	Se actualiza de manera general el plan para vigencia 2024.	Juan David Echeverry – Líder de sistemas	David Ramírez – Profesional de Calidad	Claudia María Calderón – Gerente
03	Enero 2025	Se actualiza de manera general el plan para vigencia 2025.	Juan David Echeverry – Líder de sistemas	Jomara Úsuga – Coordinadora de calidad	Santiago Varela Macias – Gerente
04	Enero 2026	Se actualiza de manera general el plan para vigencia 2026.	Juan David Echeverry – Líder de sistemas	Jomara Usuga – Coordinadora de calidad	Santiago Varela Macias – Gerente