# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## GESTIÓN DE LA INFORMACIÓN

## 2026

## 1. INTRODUCCIÓN

La información que genera constantemente el Hospital San Rafael de Yolombó es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales. La seguridad y privacidad de la información se convierten en atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo en la prestación de servicios de salud.

Como institución prestadora de servicios de salud, el Hospital maneja información altamente sensible, especialmente datos relacionados con la salud de los pacientes contenidos en historias clínicas, resultados de laboratorio, imágenes diagnósticas, prescripciones médicas y demás documentación clínica. Esta información está protegida por múltiples marcos normativos que incluyen la Ley 1581 de 2012 sobre protección de datos personales, la Resolución 1995 de 1999 sobre historia clínica, la Resolución 866 de 2021 sobre historia clínica electrónica, entre otras.

El Hospital San Rafael adopta la metodología 'Guía de Riesgos' del Departamento Administrativo de la Función Pública como herramienta para hacer una gestión integral y transversal de los riesgos a los que se encuentren expuestos los diferentes procesos, con especial énfasis en aquellos que tengan impacto sobre la seguridad y privacidad de la información en el contexto del gobierno digital.

## 2. OBJETIVOS

### 2.1. Objetivo General

Definir las directrices y acciones para abordar el tratamiento de los riesgos de seguridad y privacidad de la información que puedan comprometer el logro de los objetivos de la E.S.E. San Rafael Yolombó, con especial énfasis en la protección de datos sensibles de salud y la continuidad de los servicios críticos de atención, aprovechando la infraestructura tecnológica basada en el aplicativo web de la Intranet, Microsoft 365 y otros aplicativos contratado para la gestión de la información.

### 2.2. Objetivos Específicos

Promover entre el grupo de servidores de la E.S.E. el enfoque y pensamiento basado en riesgos en la gestión de los riesgos relacionados con seguridad y privacidad de la información, favoreciendo la capacidad de diálogo e interacción entre los procesos involucrados en su gestión.

1. Contribuir a la generación de mecanismos de seguimiento, reporte y control que promuevan la generación de datos y su traducción en información para la toma de decisiones.
2. Asegurar un tratamiento permanente y continuo de los riesgos de seguridad y privacidad de la información, que permita la toma de acciones y el mantenimiento de una gestión preventiva.
3. Vincular la identificación y análisis de riesgos de la Entidad hacia los temas de seguridad y privacidad de la información con las directrices metodológicas de la Guía de Administración de Riesgos y Diseño de Controles de Función Pública.
4. Garantizar la confidencialidad, integridad y disponibilidad de los datos sensibles de salud en cumplimiento de la Ley 1581 de 2012, la Resolución 1995 de 1999, la Resolución 866 de 2021 y normativa sectorial específica.
5. Asegurar la disponibilidad continua de los sistemas críticos de información en salud que soportan la atención de pacientes, especialmente en servicios de urgencias y hospitalización.
6. Implementar controles específicos para la protección, trazabilidad y conservación de la historia clínica conforme a la normativa vigente.
7. Establecer capacidades de detección, respuesta y recuperación ante incidentes de seguridad que puedan comprometer datos de pacientes o la continuidad del servicio.
8. Mantener el cumplimiento de las obligaciones ante autoridades de control (SIC, Supersalud, MinTIC) en materia de protección de datos y seguridad de la información.
9. Aprovechar las capacidades de seguridad y colaboración de Microsoft 365 para fortalecer la protección de la información institucional.

## 3. MARCO LEGAL Y NORMATIVO

### 3.1. Protección de Datos Personales

- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Establece los principios, derechos, obligaciones y procedimientos para el tratamiento de datos personales.
- Decreto 1377 de 2013: Reglamenta aspectos específicos de la Ley 1581, incluyendo el tratamiento de datos sensibles (datos de salud), autorización, aviso de privacidad, y transferencia internacional de datos.
- Circular Externa 000006 de 2014 (SIC): Instrucciones para el tratamiento de datos de salud por parte de prestadores de servicios de salud.

### 3.2. Historia Clínica y Datos de Salud

- Ley 23 de 1981: Normas de ética médica. Establece el secreto profesional médico y la reserva de la historia clínica.
- Resolución 1995 de 1999: Normas para el manejo de la historia clínica. Define contenido, conservación, confidencialidad y acceso.
- Resolución 866 de 2021: Adopción del Manual de Gestión de Historia Clínica Electrónica. Establece requisitos técnicos, funcionales y de seguridad para sistemas de HCE.
- Ley 1751 de 2015: Derecho fundamental a la salud. Art. 10 sobre derecho a la información en salud.
- ISO/IEC 27001:2022: Estándar internacional para sistemas de gestión de seguridad de la información.

### 3.3. Seguridad de la Información y Gobierno Digital

- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.
- Decreto 1008 de 2018: Lineamientos de la Política de Gobierno Digital.
- Modelo de Seguridad y Privacidad de la Información (MSPI): Marco de referencia para entidades públicas emitido por MinTIC.
- Guía de Administración de Riesgos y Diseño de Controles (Función Pública): Metodología adoptada por el Hospital para la gestión de riesgos.

### 3.4. Gestión Documental

- Ley 594 de 2000: Ley General de Archivos.
- Acuerdo AGN 060 de 2001: Pautas para la administración de comunicaciones oficiales.
- Acuerdo AGN 004 de 2019: Criterios de conservación de documentos electrónicos.

### 3.5. Otras Normas Aplicables

- Ley 1712 de 2014: Transparencia y acceso a la información pública.
- Decreto 780 de 2016: Decreto Único Reglamentario del Sector Salud.
- Resolución 2654 de 2019: Sistema de Información para la Calidad.

## 4. ALCANCE

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica para todos los procesos institucionales del Hospital San Rafael de Yolombó contemplados en el

mapa de procesos, con especial énfasis en aquellos que involucran el tratamiento de información en medios digitales.

### 4.1. Información Incluida en el Alcance

Este plan cubre específicamente:

- **Datos de Salud de Pacientes**

  - Historia clínica (física y electrónica).
  - Resultados de laboratorio clínico.
  - Imágenes diagnósticas (radiografías, ecografías, y tomografías).
  - Órdenes médicas y prescripciones.
  - Consentimientos informados.
  - Registros de procedimientos quirúrgicos.
  - Registros de atención en urgencias, hospitalización y consulta externa.

- **Datos Administrativos**

  - Información de recursos humanos (datos personales de empleados, nómina, salud ocupacional).
  - Información financiera y contable.
  - Contratos con proveedores y terceros.
  - Correspondencia oficial.
  - Auditorías de calidad.

- **Datos de Facturación y Aseguramiento**

  - RIPS (Registro Individual de Prestación de Servicios).
  - Información de afiliación a EPS.
  - Facturación de servicios.
  - Autorizaciones de servicios.

### 4.2. Sistemas de Información Cubiertos

- Sistema de Historia Clínica Electrónica (HCE) – XENCO Advance.
- Sistema de generación y envío de RIPS.
- Sistema de agendamiento de citas – COCO.
- Aplicativo web de gestión - Intranet.

- Microsoft 365 (correo institucional, OneDrive, Teams, etc)
- Sistemas de información de laboratorio clínico – LabSense.

### 4.3. Procesos Críticos de Salud

- Urgencias (disponibilidad 24/7).
- Hospitalización.
- Consulta externa.
- Cirugía.
- Laboratorio clínico.
- Farmacia.
- Radiología e imágenes diagnósticas.
- Gestión de la información y la comunicación.

## 5. MATRIZ ESTRATÉGICA DE RIESGOS Y TRATAMIENTO 2026.

| Riesgo Identificado | Nivel de Riesgo | Acción de Tratamiento | Control Implementado |
|---|---|---|---|
| Ataque de Ransomware: Secuestro de datos del hospital. | Muy Alto | Mitigar | Backup "Inmutable" en la nube y actualización de Firewall perimetral. |
| Acceso No Autorizado: Personal consultando historias clínicas sin permiso. | Alto | Prevenir | Implementación de Doble Factor de Autenticación (2FA) y auditorías de Log. |
| Pérdida de Información por Desastre: Incendio o inundación en servidores. | Medio | Transferir | Contratación de Seguro de Ciberriesgos y migración a Nube Híbrida. |
| Fuga de Información (Insider Threat): Empleado compartiendo datos. | Alto | Reducir | Acuerdos de confidencialidad firmados y control de puertos USB (DLP). |

## 6. CONTEXTO ORGANIZACIONAL Y TECNOLÓGICO

### 6.1. Infraestructura Tecnológica Actual

El Hospital cuenta con los siguientes recursos tecnológicos que son base para la implementación de este plan:

### 6.2. Microsoft 365

Todas las áreas y procesos cuentan con cuentas institucionales de Microsoft 365, lo que proporciona:

- Correo electrónico institucional con protección avanzada contra phishing y malware.
- OneDrive for Business: almacenamiento seguro en la nube con capacidad de respaldo automático.
- Microsoft Teams: para comunicaciones seguras y agendamiento de reunión vituales así como su grabación.
- Office Online: para trabajo colaborativo en documentos.
- Herramientas de seguridad integradas: autenticación multifactor (MFA) y prevención de pérdida de datos (DLP).

### 6.3. Aplicativo Web Intranet

El Hospital cuenta con un aplicativo web para gestión de procesos administrativos que incluye funcionalidades como:

- Gestión de Asistencia digital a eventos y capacitaciones.
- Reporte del flujo de facturación y los soportes documentales.
- Portal de autogestión para empleados.
- Solicitud de compra de activos.
- Inventario de activos y soporte de mantenimientos preventivos.
- Tableros médicos para el control asistencial.
- Solicitud de la alimentación de internos y pacientes.
- Gestión del inventario de gases medicinales.
- Gestión vehicular.
- Gestión de pedidos y compras de medicamentos.

### 6.4. Sistema de Historia Clínica

Sistema especializado para la gestión de la historia clínica, consultas, evoluciones, órdenes médicas y demás registros clínicos.

### 6.5. Otros Sistemas

- Sistema de facturación y RIPS.
- Sistema de agendamiento COCO.
- Sistemas de laboratorio clínico LabSense.

## 7. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

El Hospital ha identificado los siguientes tipos de riesgos específicos relacionados con la seguridad y privacidad de la información en el contexto de la prestación de servicios de salud:

### 7.1. Riesgos de Confidencialidad

- Acceso no autorizado a historias clínicas por personal no facultado.
- Divulgación indebida de diagnósticos o condiciones de salud de pacientes.
- Uso indebido de datos de salud por parte del personal médico o administrativo.
- Filtración de información a terceros no autorizados (aseguradoras, empleadores, medios).
- Vulneración del secreto profesional médico.
- Pérdida o robo de dispositivos con información sensible sin cifrado.
- Acceso indebido a información almacenada en OneDrive o la intranet.

### 7.2. Riesgos de Disponibilidad

- Caída del sistema de historia clínica electrónica en horario de atención.
- Indisponibilidad de resultados de laboratorio para toma de decisiones clínicas críticas.
- Pérdida de acceso a sistemas de prescripción electrónica.
- Fallas en comunicaciones con entidades externas (EPS, otras IPS).
- Ataques de denegación de servicio (DoS) a sistemas críticos como la intranet.
- Ransomware que cifra información crítica e impide acceso.
- Desastres naturales o fallas de infraestructura que afecten disponibilidad.

### 7.3. Riesgos de Integridad

- Modificación no autorizada de historias clínicas.
- Alteración de órdenes médicas o prescripciones.
- Corrupción de imágenes diagnósticas.
- Pérdida de trazabilidad de cambios en registros médicos.
- Errores en la sincronización de información entre sistemas.

### 7.4. Riesgos Tecnológicos

- Ransomware dirigido específicamente a hospitales (tendencia mundial creciente).
- Obsolescencia tecnológica de sistemas críticos sin soporte del fabricante.
- Falta de respaldos adecuados o respaldos no probados.
- Vulnerabilidades en sistemas legacy de salud sin parches disponibles.
- Fallas en la infraestructura de Microsoft 365 (poco probable).
- Incompatibilidad entre sistemas que impida intercambio de información.

### 7.5. Riesgos Humanos

- Ataques de ingeniería social dirigidos a personal médico y administrativo (phishing).
- Errores humanos en el manejo de información sensible.
- Falta de capacitación en protección de datos de salud.
- Uso de dispositivos personales sin controles de seguridad.
- Contraseñas débiles o compartidas entre usuarios.
- Desconocimiento de políticas de seguridad.

### 7.6. Riesgos de Cumplimiento Normativo

- Incumplimiento de tiempos de conservación de historia clínica (mínimo 20 años).
- Vulneración de derechos de Habeas Data de pacientes
- Sanciones de la Superintendencia de Industria y Comercio por tratamiento indebido de datos.
- Investigaciones de ética médica por divulgación de información.
- Falta de registro de bases de datos en el RNBD.
- Ausencia de políticas de tratamiento de datos personales publicadas.

## 8. PLAN DE ACCIÓN (CICLO PHVA)

El plan de acción se estructura siguiendo el ciclo de mejora continua PHVA (Planear, Hacer, Verificar, Actuar) adoptado por la institución. A continuación, se presentan las actividades principales organizadas por fase:

### 8.1. PLANEAR

**Actividad 1: Actualización del Marco Normativo y Políticas**

Desarrollar y aprobar políticas de seguridad de la información, privacidad y protección de datos personales, política de acceso, contraseñas, uso aceptable, respaldos, dispositivos móviles y seguridad física.

Responsable: Gestión de la Información y Oficina Jurídica.

**Actividad 2: Inventario y Clasificación de Activos de Información**

Realizar inventario completo de sistemas de información, bases de datos, y clasificar la información según sensibilidad (pública, reservada, clasificada).

Responsable: Gestión de la Información.

**Actividad 3: Actualización de la Matriz de Riesgos.**

Actualizar la matriz de riesgos con escenarios específicos del sector salud, análisis de causas raíz, valoración de probabilidad e impacto.

Responsable: Gestión de la Información, Planeación y Control Interno.

**Actividad 4: Diseño "Protocolo de Respuesta Rápida de TI"**

Instalar sensores de red y reportes de usuarios a la Mesa de Ayuda.
Aislamiento de equipos afectados para evitar la propagación (segmentación de red).
Limpieza de malware y restauración de sistemas desde copias de seguridad limpias.
Retorno gradual a la operación normal priorizando Urgencias y Hospitalización.

## 8.2. HACER

### 8.2.1. Cumplimiento Normativo de Protección de Datos

**Actividad 4: Implementación de Cumplimiento Ley 1581 de 2012**

- Crear formatos de autorización para tratamiento de datos personales.
- Diseñar e implementar avisos de privacidad.
- Publicar la Política de Tratamiento de Datos Personales.
- Registrar bases de datos en el RNBD ante la SIC.
- Crear procedimiento de atención de consultas y reclamos (Habeas Data).
- Revisar contratos con terceros para incluir cláusulas de transmisión de datos.

Responsable: Oficina Jurídica y Gestión de la Información

### 8.2.2. Controles Técnicos Aprovechando Microsoft 365

**Actividad 5: Implementación de Autenticación Multifactor (MFA)**

- Configurar y habilitar MFA en todas las cuentas de Microsoft 365.

- Priorizar cuentas de administradores y personal con acceso a información crítica.
- Control del acceso a equipos de computo mediante cuenta de Institucional.

Responsable: Gestión de la Información.

**Actividad 6: Configuración de Controles de Seguridad en Microsoft 365.**

- Configurar políticas de Prevención de Pérdida de Datos (DLP).
- Configurar políticas de retención de correo y documentos.
- Configurar alertas de actividades sospechosas.
- Habilitar auditoría de actividades en OneDrive.

Responsable: Gestión de la Información.

**Actividad 7: Gestión de Controles de Acceso y Permisos**

- Definir perfiles de usuario según función.
- Revisar y ajustar permisos de acceso en todos los sistemas.
- Implementar segregación de funciones críticas.
- Establecer procedimiento de altas, bajas y modificaciones de usuarios.
- Implementar revisión semestral de privilegios de acceso.

Responsable: Gestión de la Información y Gestión del Talento Humano.

### 8.2.3. Gestión Integral de la Historia Clínica

**Actividad 9: Gestión Integral de la Historia Clínica**

Esta actividad integral aborda todos los aspectos de la gestión de la historia clínica en cumplimiento de la Resolución 1995 de 1999, la Resolución 866 de 2021, la Ley 23 de 1981 y la Ley 1581 de 2012.

**Control de Acceso a Historia Clínica:**

- Configurar permisos granulares en HCE según rol.
- Implementar control de acceso por contexto clínico.
- Restricciones para personal administrativo (solo datos necesarios, sin información clínica sensible).
- Sistema de justificación de acceso para accesos fuera de contexto habitual.
- Procedimiento formal para acceso excepcional (auditorías médicas).

**Auditoría y Trazabilidad:**

- Registro automático de todos los accesos a HC (quién, cuándo, qué, desde dónde).
- Logs detallados de modificaciones con trazabilidad completa.
- Alertas automáticas de accesos anómalos.
- Conservar logs por mínimo 2 años.

**Integridad y Modificaciones:**

- Sistema de HC impide modificación de registros cerrados sin trazabilidad
- Firma electrónica para actos médicos según Resolución 866/2021.
- Auditoría de integridad trimestral.
- Controles que impidan eliminación de registros.

**Conservación y Archivo:**

- Conservación por mínimo 20 años desde última atención (Resolución 1995/99)
- Respaldo diario de base de datos de HCE.
- Respaldos automáticos en OneDrive para documentos complementarios.
- Respaldos fuera de sitio (nube M365 + copia local).
- Pruebas semestrales de restauración.
- Para HC físicas: sistema de préstamo y custodia.
- Plan de digitalización progresiva de HC físicas antiguas.

**Solicitudes de Pacientes (Habeas Data):**

- Procedimiento formal de solicitud de copia de HC.
- Formulario disponible en Intranet y formato físico.
- Verificación de identidad del solicitante.
- Plazo de entrega máximo 10 días hábiles (Ley 1581).
- Procedimiento para corrección o actualización de datos.
- Registro de todas las solicitudes y entregas.

**Confidencialidad y Secreto Profesional:**

- Acuerdos de confidencialidad firmados por todo el personal con acceso a HC
- Protocolo de manejo en áreas clínicas (pantallas orientadas, bloqueo automático).
- Prohibición de uso de dispositivos móviles personales para fotografiar HC.
- Política de escritorio limpio.
- Destrucción segura (trituración) de documentos con datos de pacientes.

**Indicadores de Gestión de HC:**

- Tiempo promedio atención solicitudes copia HC (meta: < 10 días hábiles)
- % éxito respaldos diarios HCE (meta: 100%)
- Número de incidentes de confidencialidad HC (meta: 0)

**Responsables:** Gestión de l a Información, Subgerencia Científica, Auditoría Médica y Archivo Clínico.

**Actividad 10: Implementación de Respaldos Robustos**

- Configurar respaldo automático en OneDrive for Business.
- Respaldo diario de BD del sistema de HCE (local + nube)
- Respaldos fuera de sitio (regla 3-2-1).
- Pruebas semestrales de restauración.

Responsable: Gestión de la Información

**Actividad 13: Plan de Respuesta a Incidentes**

- Desarrollar Plan de Respuesta a Incidentes como documento independiente.
- Definir tipos de incidentes y clasificación por severidad.
- Conformar Equipo de Respuesta a Incidentes (CSIRT).
- Documentar procedimientos: Detección, Contención, Erradicación, Recuperación.
- Habilitar canal de reporte (correo, Intranet, teléfono).
- Realizar simulacro de ransomware.

Responsable: Gestión de la Información y Oficina Jurídica

**Actividad 15: Programa de Capacitación**

- Capacitación de inducción (personal nuevo): Políticas, confidencialidad, uso de M365.
- Capacitación anual (todo el personal): ransomware, buenas prácticas.
- Capacitación por roles (médicos, administrativos, TI, directivos).
- Sensibilización continua (campañas trimestrales).
- Simulacros de phishing semestrales.

Responsable: Talento Humano y Gestión de la Información.

### 8.3. VERIFICAR

- Seguimiento con Planeación y Control Interno.
- Comité de Gobierno Digital y Comité de Seguridad de la información.
- Auditorías internas anuales.

### 8.4. ACTUAR

- Implementación de acciones de mejora.
- Acciones correctivas derivadas de incidentes.
- Actualización anual del plan.

## 9. PRIORIZACIÓN DE IMPLEMENTACIÓN

El siguiente cronograma prioriza las actividades según su criticidad y urgencia:

| Prioridad | Actividad | Tiempo |
|---|---|---|
| **CRÍTICA** | Cumplimiento normativo protección de datos | 3 meses |
| **CRÍTICA** | Implementación MFA | 1 mes |
| **CRÍTICA** | Respaldos robustos | 2 meses |
| **CRÍTICA** | Plan de respuesta a incidentes | 3 meses |
| **ALTA** | Políticas de seguridad | 3 meses |
| **ALTA** | Inventario de activos | 2 meses |
| **ALTA** | Gestión de accesos | 3 meses |
| **ALTA** | Gestión integral HC (fase 1) | 3 meses |
| **ALTA** | Gestión integral HC (fase 2) | 3 meses |
| **ALTA** | Programa capacitación | Continuo |
| **MEDIA** | Cifrado | 3 meses |
| **MEDIA** | Seguridad de red | 4 meses |
| **MEDIA** | Plan de continuidad | 6 meses |
| **MEDIA** | Seguimiento e indicadores | Continuo |

## 10. ROLES Y RESPONSABILIDADES

| Rol | Responsabilidades |
|---|---|
| **Gerente** | Aprobar políticas y planes, asignar recursos, liderar cultura de seguridad |

| Rol | Responsabilidades |
|---|---|
| **Gestión de la Información** | Responsable principal de implementación, coordinar actividades, reportar avances |
| **Oficina Jurídica** | Asesoría legal, cumplimiento normativo, contratos con terceros |
| **Planeación** | Seguimiento al plan, articulación con otros planes, seguimiento a indicadores |
| **Control Interno** | Auditoría de controles, seguimiento trimestral, recomendaciones de mejora. |
| **Talento Humano** | Coordinar capacitación, acuerdos de confidencialidad, inducción. |
| **Subgerente Científico** | Gestión de HC, validar controles clínicos, capacitación médica. |
| **Auditoría Médica** | Revisión de accesos a HC, auditoría de integridad de registros. |
| **Archivo** | Custodia de HC físicas, atención de solicitudes, conservación documental. |
| **Todo el Personal** | Cumplir políticas, reportar incidentes, participar en capacitaciones. |

## 11. INDICADORES DE GESTIÓN (DASHBOARD SEGURIDAD)

| Indicador | Fórmula | Meta 2026 |
|---|---|---|
| Eficacia de Controles | (Riesgos mitigados / Riesgos identificados) * 100 | > 90% |
| Tiempo de Respuesta | Promedio de tiempo en cerrar un incidente crítico. | < 2 horas |
| Cultura de Seguridad | % de servidores que aprobaron test de Ciberseguridad. | 100% |
| Disponibilidad Backup | % de pruebas de restauración exitosas. | 100% |

## 12. CONTROL DE CAMBIOS

| Versión | Fecha | Descripción del Cambio | Responsable |
|---|---|---|---|
| **01** | Enero 2024 | Creación del documento inicial. | Javier Adolfo Duque Lugo Ingeniero de Sistemas. |
| **02** | Enero 2025 | Actualización trabajo 2025 | Javier Adolfo Duque Lugo Ingeniero de Sistemas. |
| **03** | 29/01/2026 | Actualización trabajo 2026 | Javier Adolfo Duque Lugo Ingeniero de Sistemas. |