HOSPITAL DEPARTAMENTAL SAN ANTONIO DE ROLDANILLO EMPRESA SOCIAL DEL ESTADO NIT. 891900343-6

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

VIGENCIA 2025

HOSPITAL
DEPARTAMENTAL
SAN ANTONIO
ROLDANILLO - VALLE E.S.E.

TABLA DE CONTENIDO

1. INTRODUCCIÓN
2. OBJETIVOS
3. ALCANCE
4. METODOLOGÍA Y CLASIFICACIÓN DE ACTIVOS (GUÍA No. 7)
5. ANÁLISIS DE RIESGOS INHERENTES
6. PLAN DE TRATAMIENTO Y CONTROLES SELECCIONADOS (GUÍA No. 8 / ISO 27001)
7. MONITOREO Y SEGUIMIENTO
8. DECLARACIÓN DE APLICABILIDAD
9. BIBLIOGRAFIA

1. INTRODUCCIÓN

En cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la política de Gobierno Digital, el Hospital Departamental San Antonio de Roldanillo establece el presente plan.

Este documento ha sido elaborado siguiendo la metodología de gestión de riesgos establecida en la **Guía No. 7** del MSPI y la selección de controles del estándar **NTC ISO/IEC 27001:2013** referenciados en la **Guía No. 8**. Su propósito es gestionar los riesgos que amenazan la confidencialidad, integridad y disponibilidad de los activos de información críticos de la entidad, garantizando la continuidad en la prestación de los servicios de salud.

En cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la política de Gobierno Digital, el Hospital Departamental San Antonio de Roldanillo establece el presente plan.

Este documento ha sido elaborado siguiendo la metodología de gestión de riesgos establecida en la **Guía No. 7** del MSPI y la selección de controles del estándar **NTC ISO/IEC 27001:2013** referenciados en la **Guía No. 8**. Su propósito es gestionar los riesgos que amenazan la confidencialidad, integridad y disponibilidad de los activos de información críticos de la entidad, garantizando la continuidad en la prestación de los servicios de salud.

2. OBJETIVOS

- **General:** Minimizar la probabilidad e impacto de la materialización de riesgos de seguridad digital que puedan afectar la operación del Hospital y la protección de datos de los usuarios.

- **Específicos:**

    1. Identificar y proteger los activos de información críticos (Historia Clínica, SIHOS WEB, Infraestructura).
    2. Establecer controles efectivos frente a amenazas como *Ransomware*, fallas tecnológicas y accesos no autorizados.
    3. Garantizar el cumplimiento de la Ley 1581 de 2012 (Protección de Datos) y la Ley 1712 de 2014 (Transparencia).

3. ALCANCE

El presente plan cubre todos los procesos asistenciales (Urgencias, Hospitalización, Consulta Externa, Laboratorio, etc.) y administrativos que interactúan con los sistemas de información y la infraestructura tecnológica del Hospital Departamental San Antonio.

4. METODOLOGÍA Y CLASIFICACIÓN DE ACTIVOS

De acuerdo con la **Guía No. 7**, se ha realizado la valoración de los activos basándose en los tres pilares de la seguridad de la información. Un activo se considera de **Criticidad Alta** si la afectación de cualquiera de sus propiedades impacta gravemente la prestación del servicio.

Criterio	Descripción
Confidencialidad (C)	Garantía de que la información es accesible solo para autorizados.
Integridad (I)	Salvaguarda de la exactitud y totalidad de la información.
Disponibilidad (D)	Garantía de que los usuarios autorizados tengan acceso cuando lo requieran.

4.1 Inventario de Activos Críticos

Tipo de Activo	Descripción y Detalle	Propiedades Críticas	Nivel de Criticidad
Sistema de Información	**SIHOS WEB:** Gestión clínica y administrativa (Admisiones, Facturación, Historia Clínica).	C, I, D	**Extrema**
Infraestructura	**Servidores Físicos:** (HP ML 350 G9, Dell T430) Controlador de Dominio, BD y Archivos.	D, I	**Alta**

Almacenamiento	**Dispositivo NAS:** Copias de seguridad locales y servidor de archivos.	C, I	**Alta**
Red y Comunicaciones	Canales de Fibra Óptica, Firewall Perimetral, Switches y Radioenlaces (Sedes externas).	D	**Alta**
Datos Sensibles	Historias Clínicas, Bases de datos de Talento Humano y Financiera.	C, I	**Extrema**

5. ANÁLISIS DE RIESGOS INHERENTES

Se han identificado los riesgos prioritarios para la vigencia 2025, evaluando su probabilidad e impacto según la metodología institucional:

ID	Riesgo	Amenaza (Causa)	Impacto Potencial	Nivel de Riesgo
R1	**Indisponibilidad de Servicios**	Fallo en servidores, cortes de energía o caída de canales.	Interrupción en la atención de pacientes y facturación.	**Alto**

R2	**Pérdida de Información**	Ransomware (secuestro de datos) o daño físico de discos.	Pérdida de historia clínica y datos financieros.	**Extremo**
R3	**Acceso No Autorizado**	Compartir contraseñas o accesos no revocados.	Fuga de información sensible y violación de privacidad.	**Alto**
R4	**Obsolescencia Tecnológica**	Equipos sin soporte o parches de seguridad.	Vulnerabilidad a ciberataques y lentitud operativa.	**Medio**

4. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Basado en el diagnóstico tecnológico institucional, se identifican los siguientes activos críticos:

Tipo de Activo	Descripción y Detalle	Criticidad
Sistema de Información	**SIHOS WEB:** Sistema principal para la gestión clínica y administrativa (Admisiones, Facturación, Historia Clínica).	Extrema
Infraestructura Servidores	Servidores físicos (HP ML 350 G9, Dell T430) que alojan el Controlador de Dominio, Bases de Datos y Archivos.	Alta
Almacenamiento	Dispositivo NAS para copias de seguridad locales y servidor de archivos.	Alta
Red y Comunicaciones	Canales de Fibra Óptica (con redundancia), Firewall Perimetral, Switches y Radioenlaces para sedes externas (Llanitos, San Sebastián y Asunción).	Alta
Datos Sensibles	Historias Clínicas de pacientes, Bases de datos de Talento Humano y Financiera.	Extrema

5. ANÁLISIS DE RIESGOS INHERENTES

Se han identificado los siguientes riesgos prioritarios para la vigencia 2025:

Riesgo	Descripción de la Amenaza	Impacto Potencial	Nivel de Riesgo
R1. Indisponibilidad de Servicios	Fallo en servidores físicos, cortes de energía prolongados o caída de canales de internet.	Interrupción en la atención de pacientes y facturación.	**Alto**
R2. Pérdida de Información	Ataques de *Ransomware* (secuestro de datos) o daño físico de discos duros sin backup recuperable.	Pérdida de historia clínica y datos financieros.	**Extremo**
R3. Acceso No Autorizado	Usuarios compartiendo contraseñas o accesos no revocado a personal retirado.	Fuga de información sensible y violación de privacidad.	**Alto**
R4. Obsolescencia Tecnológica	Equipos de cómputo o servidores sin soporte o actualizaciones de seguridad.	Vulnerabilidad a ciberataques y lentitud operativa.	**Medio**

6. PLAN DE TRATAMIENTO Y CONTROLES SELECCIONADOS

Para el tratamiento de los riesgos, se han seleccionado los siguientes controles normativos basados en la Guía No. 8 (Anexo A de la NTC-ISO/IEC 27001:2013).

6.1 Controles Tecnológicos

Riesgo	Acción a Implementar	Control ISO 27001 (Referencia Guía 8)	Responsable	Frecuencia
R2	Ejecución de backups automáticos en NAS local y gestión nube (Off-site).	A.12.3.1 Respaldo de información: Se deben hacer copias de respaldo de la información y ponerlas a prueba regularmente.	Coord. Sistemas	Diaria / Semanal
R2, R4	Actualización de licencias, firmas del Firewall y Antivirus centralizado.	A.12.2.1 Controles contra códigos maliciosos: Implementar controles de detección, prevención y recuperación.	Coord. Sistemas	Permanente
R3	Revisión de usuarios en Directorio Activo y bloqueo inmediato de retirados.	A.9.2.1 Registro y cancelación de usuarios: Proceso formal para habilitar y revocar derechos de acceso.	Talento Humano / Sistemas	Trimestral
R1	Mantenimiento de canales	A.17.2.1 Redundancia: Instalaciones	Coord. Sistemas	Mensual

	redundantes y verificación de radioenlaces.	con redundancia suficiente para cumplir requisitos de disponibilidad.		
R3	Gestión de contraseñas seguras y no compartidas.	A.9.4.3 Sistema de gestión de contraseñas: Asegurar la calidad de las contraseñas en sistemas interactivos.	Coord. Sistemas	Permanente

6.2 Controles Administrativos

Riesgo	Acción a Implementar	Control ISO 27001 (Referencia Guía 8)	Responsable	Frecuencia
R3	Jornadas de sensibilización (phishing, seguridad).	A.7.2.2 Toma de conciencia, educación y formación: Empleados deben recibir formación regular en políticas y procedimientos.	Sistemas / Calidad	Semestral
R1, R4	Cronograma de mantenimiento preventivo (físico/lógico).	A.11.2.4 Mantenimiento de equipos: Mantener equipos correctamente para asegurar disponibilidad e integridad.	Coord. Sistemas	Cuatrimestral
General	Actualización de la Política de Seguridad.	A.5.1.1 Políticas para la seguridad de la información: Conjunto de políticas aprobada por la dirección y publicada.	Planeación / Sistemas	Anual
R3	Acuerdos de confidencialidad con terceros/proveedores.	A.13.2.4 Acuerdos de confidencialidad: Requisitos para acuerdos de no divulgación que reflejen necesidades de protección.	Jurídica / Sistemas	Por contrato

7. MONITOREO Y SEGUIMIENTO

La eficacia de los controles implementados se medirá a través de los siguientes indicadores de gestión:

1. **Efectividad de Backups (Control A.12.3.1):**
    - ***Fórmula:*** **(Backups exitosos / Backups programados) * 100.**
    - ***Meta:*** **> 98%**

2. **Disponibilidad de Servicios (Control A.17.2.1):**
    - ***Descripción:*** **Tiempo de operación de SIHOS WEB sin interrupciones no programadas.**
    - ***Meta:*** **99.5%**

3. **Gestión de Incidentes (Control A.16.1.5):**
    - ***Descripción:*** **Número de incidentes de seguridad reportados y gestionados en la mesa de ayuda.**

8. DECLARACIÓN DE APLICABILIDAD

De conformidad con la Guía No. 8, el Hospital Departamental San Antonio de Roldanillo declara que los controles listados en el numeral 6 de este documento han sido seleccionados del Anexo A de la norma ISO/IEC 27001 por ser pertinentes para mitigar los riesgos inaceptables identificados en el análisis de riesgos de la vigencia 2025. Los controles no listados se consideran no aplicables o de implementación futura según la madurez del sistema.

ELABORÓ: Coordinador de Sistemas

APROBÓ: Gerencia Hospital Departamental San Antonio de Roldanillo

BIBLIOGRAFIA

1. **Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). *Guía No. 7: Gestión de Riesgos*. Modelo de Seguridad y Privacidad de la Información. Estrategia de Gobierno en Línea.**
2. **Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). *Guía No. 8: Controles de Seguridad y Privacidad de la Información*. Modelo de Seguridad y Privacidad de la Información. Estrategia de Gobierno en Línea.**
3. **Departamento Administrativo de la Función Pública. (2018). *Guía para la administración del riesgo y el diseño de controles en entidades públicas* (Versión 4).**
4. **Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). *Anexo 4: Lineamiento para la gestión de riesgos de seguridad digital en entidades públicas*.**
5. **Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2013). *NTC-ISO/IEC 27001:2013: Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos*.**