Política de Seguridad de la Información y Respaldo de Datos (PSIR)

IPS: Radiólogos Asociados del Bajo Sinú
Versión: 1.0
Fecha de Aprobación: 20-01-2025
Responsable: Gerencia / Oficial de Seguridad de la Información

Título I: Política General de Seguridad de la Información

1. Propósito

Establecer los lineamientos y controles obligatorios para proteger los activos de información de **Radiólogos Asociados del Bajo Sinú**, garantizando los principios de **Confidencialidad, Integridad y Disponibilidad (CID)**, especialmente de la información sensible de salud de los pacientes.

2. Alcance

Esta política aplica a:

- Todos los empleados, contratistas y terceros con acceso a los sistemas de información de la IPS.
- Todos los sistemas de información críticos (PACS, RIS, RME).
- Toda la información, en formato físico o digital, que contenga datos personales o clínicos.

3. Marco Normativo y Legal

La IPS se compromete a dar estricto cumplimiento a:

- **Ley Estatutaria 1581 de 2012 (Habeas Data):** En particular, la protección de **datos sensibles** (datos de salud).
- **Resolución 839 de 2017 (MinSalud):** En cuanto a los tiempos de retención y conservación de la Historia Clínica y anexos.
- Normatividad vigente de seguridad social y salud en Colombia.

4. Directrices Clave de Seguridad

A. Control de Acceso y Autenticación

- **Principio de Mínimo Privilegio:** Los usuarios solo tendrán acceso a los datos y funciones estrictamente necesarios para el desempeño de su trabajo (ej. El personal administrativo no tendrá acceso a las imágenes DICOM si no es necesario para la facturación).
- **Contraseñas:** Todos los usuarios deben utilizar contraseñas fuertes (mínimo 10 caracteres, incluyendo mayúsculas, minúsculas, números y símbolos) y deben ser cambiadas obligatoriamente cada **90 días**.
- **Bloqueo de Sesión:** Las estaciones de trabajo y servidores deben tener un bloqueo de sesión automático si no hay actividad por un periodo máximo de **5 minutos**.

B. Protección de Datos Sensibles y Cifrado

- **Cifrado en Reposo:** Los datos almacenados en servidores críticos (PACS/RIS) deben estar protegidos mediante **cifrado a nivel de disco** o de aplicación.
- **Cifrado en Tránsito:** La transferencia de datos clínicos a terceros (ej. envío de resultados a médicos remitentes) se realizará únicamente a través de canales seguros (VPN, HTTPS o plataformas cifradas).
- **Dispositivos de Almacenamiento:** Se prohíbe el uso de dispositivos USB, discos externos o servicios de almacenamiento en la nube personales para transferir o almacenar información clínica, a menos que esté expresamente autorizado y cifrado.

C. Seguridad Física y del Entorno

- **Centros de Datos:** El acceso a los servidores (RIS/PACS) debe estar físicamente restringido mediante cerraduras de alta seguridad y monitoreo por CCTV.
- **Puestos de Trabajo:** El personal debe abstenerse de dejar impresiones de Historias Clínicas o resultados en impresoras o estaciones de trabajo desatendidas.

Título II: Política de Respaldo y Copias de Seguridad (Backup)

5. Definiciones y Regla 3-2-1

- **Activo Crítico:** Imágenes DICOM, Bases de Datos RIS/RME.
- **Regla 3-2-1:** Se mantendrán **tres (3)** copias de los datos críticos, en **dos (2)** tipos de medios diferentes, con **una (1)** copia físicamente fuera del sitio principal (*off-site*).

6. Cronograma y Tipos de Respaldo

Activo de Información	Tipo de Respaldo	Frecuencia	Retención Mínima (Normativa Colombiana)	Medio de Almacenamiento
Imágenes DICOM (PACS) y RME	Incremental / **Completo Semanal**	Diario (al final del día operativo)	**15 años** (según Res. 839 de 2017)	Disco Local (NAS) + Nube Cifrada
Bases de Datos RIS	Diferencial	Diario (varias veces al día)	2 años	Disco Local (NAS) + Nube Cifrada
Configuraciones Críticas (Firewall, Servidor)	Completo	Mensual	6 meses	Disco Externo Cifrado

7. Seguridad y Gestión de Medios de Respaldo

- **Inmutabilidad:** El sistema de almacenamiento utilizado para los *backups* críticos debe configurarse con la función de **inmutabilidad** para prevenir que el *ransomware* pueda cifrar o eliminar las copias de seguridad.
- **Cifrado *Off-site*:** La copia de seguridad enviada a la nube o al sitio remoto deberá estar siempre cifrada, siendo el administrador de TI el único custodio de la clave de cifrado.
- **Aislamiento (*Air Gap*):** El medio de respaldo *off-site* debe estar aislado de la red de producción para protegerlo contra ataques que se propaguen horizontalmente.

8. Pruebas y Procedimiento de Restauración

- **Pruebas Periódicas:** Se realizarán **pruebas de restauración (simulacros de desastre)** de manera **trimestral** para verificar que los datos DICOM y RME puedan ser recuperados de forma completa y funcional.
- **RTO (Tiempo Objetivo de Recuperación):** El sistema PACS/RIS debe estar operativo en un máximo de **4 horas** después de declarado un incidente de pérdida de datos.
- **Documentación:** El Administrador de TI mantendrá un registro detallado de las pruebas de restauración, incluyendo la validación de la integridad de los datos recuperados.

Título III: Responsabilidades y Formación

Rol	Responsabilidad Clave
Gerencia	Aprobación de recursos, compromiso y sanción del incumplimiento de la política.
Oficial de Seguridad / TI	Ejecución, monitoreo, gestión del cifrado, pruebas de restauración y respuesta a incidentes.
Jefe de Radiología	Supervisión del acceso a los RME/DICOM por parte del personal clínico.
Todo el Personal	Cumplir la política de contraseñas, reportar incidentes de seguridad y bloquear los equipos de trabajo.

Formación: Se realizará capacitación anual obligatoria para todo el personal sobre la Ley 1581 de 2012, el manejo de datos sensibles y el procedimiento de reporte de incidentes.