RADIÓLOGOS ESPECIALIZADOS DE BUCARAMANGA S.A.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FLORIDABLANCA – SANTANDER

2024

Tabla de Contenido

1. INTRODUCCIÓN 2

2. OBJETIVO 3

3. ALCANCE 3

4. DEFINICIONES 3

5. NORMATIVIDAD 5

6. ROLES Y RESPONSABILIDADES 6

6.1. Responsables de Seguridad y Privacidad de la Información. 6

6.2. Área de Tecnología 6

6.3. Usuarios (Colaboradores y Contratistas) 6

7. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 6

8. ESTRATEGIAS Y LÍNEAS DE ACCIÓN 8

8.1. Estrategia de Gestión de Riesgos de Seguridad de la Información 8

8.2. Estrategia de Protección de Datos Personales y Datos Sensibles 8

8.3. Estrategia de Control de Accesos y Gestión de Identidades 9

8.4. Estrategia de Seguridad Tecnológica y Operativa 9

8.5. Estrategia de Gestión de Incidentes de Seguridad de la Información 10

8.6. Estrategia de Continuidad del Negocio y Recuperación ante Desastres 10

8.7. Estrategia de Concientización y Capacitación en Seguridad de la Información 10

9. VIGENCIA 11

10. CONTROL DE CAMBIOS 12

1. INTRODUCCIÓN

La seguridad de la información es un componente esencial para la sostenibilidad, confiabilidad y calidad de los servicios en el sector salud. En este sentido, **Radiólogos Especializados de Bucaramanga S.A.**, reconoce que la información constituye un activo estratégico fundamental para el adecuado desarrollo de los procesos asistenciales y administrativos. En la prestación de servicios de imágenes diagnósticas, los procesos clínicos, diagnósticos y administrativos dependen de manera crítica de sistemas de información, plataformas tecnológicas especializadas y entornos digitales interconectados, lo que incrementa la exposición a riesgos de seguridad.

En este contexto, la información gestionada incluye datos personales y datos sensibles, tales como historias clínicas, imágenes diagnósticas y resultados, cuya protección resulta indispensable para preservar la seguridad del paciente, la continuidad de la atención, la confianza de los usuarios y el cumplimiento de los deberes legales.

La Seguridad de la Información se entiende como el conjunto de principios, políticas, procesos y controles orientados a proteger los activos de información, garantizando de manera permanente la confidencialidad, integridad y disponibilidad, así como la autenticidad, trazabilidad y confiabilidad. Este enfoque debe gestionarse de forma sistemática, basada en riesgos y alineada con estándares reconocidos internacionalmente, permitiendo anticipar amenazas, reducir vulnerabilidades y responder adecuadamente ante incidentes.

En este marco, la presente política se establece como el documento rector del Sistema de Gestión de Seguridad de la Información (SGSI), bajo los lineamientos de la **Norma ISO/IEC 27001**, promoviendo una cultura institucional de seguridad, privacidad y mejora continua.

2. OBJETIVO

La presente política tiene como objetivo establecer los lineamientos generales de Seguridad y Privacidad de la Información que permitan proteger de manera integral los activos de información de **Radiólogos Especializados de Bucaramanga S.A.**

A través de una gestión de riesgos, se garantiza la confidencialidad, integridad y disponibilidad de los datos, asegurando el cumplimiento de la normativa vigente de protección de datos personales y el resguardo ético de la información.

3. ALCANCE

La presente Política de Seguridad y Privacidad de la Información aplica a todos los procesos de **Radiólogos Especializados de Bucaramanga S.A.,** a la totalidad de sus activos de información y a todas las partes interesadas (colaboradores, contratistas, proveedores y terceros) garantizando una protección integral y coherente en todas sus operaciones.

4. DEFINICIONES

Para efectos de la presente Política de Seguridad y Privacidad de la Información, se adoptan las siguientes definiciones, con el fin de asegurar una interpretación uniforme y coherente de los conceptos aquí establecidos:

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, vehículos…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de información**: Cualquier información o recurso que tenga valor para la institución, incluyendo datos, bases de datos, historias clínicas, imágenes diagnósticas, software, hardware, infraestructura tecnológica, servicios y conocimiento del personal.
- **Confidencialidad:** Propiedad que garantiza que la información no sea divulgada ni puesta a disposición de personas, entidades o procesos no autorizados.
- **Integridad:** Propiedad que asegura que la información sea exacta, completa y que no haya sido alterada de manera no autorizada.

- **Disponibilidad:** Propiedad que garantiza que la información y los sistemas estén accesibles y utilizables cuando sean requeridos por usuarios autorizados, especialmente para la atención en salud.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable.
- **Dato sensible:** Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación. En el sector salud incluye, entre otros, datos relacionados con el estado de salud, historias clínicas, imágenes diagnósticas y datos biométricos.
- **Seguridad de la Información:** Conjunto de principios, políticas, procesos y controles destinados a proteger la confidencialidad, integridad y disponibilidad de la información, así como su autenticidad y trazabilidad.
- **Privacidad de la información:** Derecho de los titulares de los datos a conocer, actualizar y rectificar su información personal, así como a controlar su uso y tratamiento conforme a la normativa vigente.
- **Gestión de riesgos:** Proceso sistemático para identificar, analizar, evaluar y tratar los riesgos que puedan afectar la seguridad de la información.
- **Incidente de seguridad de la información:** Evento o conjunto de eventos que comprometen o pueden comprometer la confidencialidad, integridad o disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de políticas, procedimientos, procesos y recursos que permiten gestionar de forma sistemática la seguridad de la información, basado en un enfoque de mejora continua conforme a la Norma ISO/IEC 27001.
- **Partes interesadas:** Personas u organizaciones internas o externas que tienen relación con la institución y pueden afectar o verse afectadas por el tratamiento de la información.
- **Cookies:** Es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador.
- **Credenciales de Acceso:** Las credenciales son elementos de que dispone un usuario o sistema para comprobar su identidad y obtener el acceso a ciertos recursos.

- **Malware:** Son programas maliciosos creados para infectar y/o comprometer sistemas informáticos alterando su funcionamiento y facilitando el compromiso de los activos de información digital.
- **TI:** Tecnologías de la Información.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. NORMATIVIDAD

La presente política se fundamenta en:

- Constitución Política de Colombia – Artículo 15 (Habeas Data).
- Ley 1581 de 2012 – Protección de Datos Personales.
- Decreto 1377 de 2013 - Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.
- Decreto 1074 de 2015 - "Decreto Único Reglamentario" del Sector Comercio, Industria y Turismo que compila normas, incluyendo aspectos que reglamentan y desarrollan la aplicación de la Ley 1581 de 2012.
- Ley 23 de 1981 – Ética Médica.
- Resolución 1995 de 1999 – Historia Clínica.
- Resolución 1519 de 2020 – Seguridad y accesibilidad de la información digital.
- Circular Externa 20211700000004-5 de 2021 – Supersalud (Gestión de riesgos).
- Lineamientos de la Superintendencia Nacional de Salud.
- ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información.
- Resolución 2654 de 2019 - Define los parámetros para la Telesalud y Telemedicina.
- Resolución 866 de 2021 - Reglamenta el conjunto de datos clínicos para la interoperabilidad.

6. ROLES Y RESPONSABILIDADES

6.1. Responsables de Seguridad y Privacidad de la Información.

- Administrar el SGSI conforme a ISO 27001.
- Gestionar riesgos, controles e incidentes de seguridad.
- Coordinar auditorías internas y atención a requerimientos de entes de control.
- Liderar programas de capacitación y concientización para todo el personal.

6.2. Área de Tecnología

- Implementar controles técnicos en los sistemas de información que maneja **Radiólogos Especializados de Bucaramanga S.A.**, redes y servicios en la nube.
- Garantizar la ejecución de respaldos (backups), monitoreo y alta disponibilidad.
- Asegurar la actualización y parcheo de seguridad de los activos digitales de información.

6.3. Usuarios (Colaboradores y Contratistas)

- Usar la información solo para los fines autorizados.
- Proteger credenciales de acceso y reportar incidentes o debilidades de seguridad de forma inmediata.
- Cumplir con los acuerdos de confidencialidad y el manejo ético de la información sensible que maneja **Radiólogos Especializados de Bucaramanga S.A.**

7. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Radiólogos Especializados de Bucaramanga S.A. se compromete a proteger la seguridad y privacidad de la información que administra, procesa, almacena y transmite, reconociendo que esta constituye un activo estratégico fundamental para la prestación segura, confiable y continua de los servicios prestados.

La organización establece que la Seguridad y Privacidad de la Información es una responsabilidad institucional y transversal, aplicable a todos los procesos asistenciales, administrativos y tecnológicos, así como a todas las partes interesadas que tengan acceso a los activos de información.

En este sentido, **Radiólogos Especializados de Bucaramanga S.A**. adopta un enfoque de gestión basado en riesgos, orientado a prevenir, detectar y responder de manera oportuna a amenazas que puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, en especial aquella relacionada con datos personales y datos sensibles de los pacientes, tales como historias clínicas, imágenes diagnósticas y resultados médicos.

La presente política general se rige por los siguientes principios:

- **Confidencialidad:** Garantizar que la información solo sea accesible a personas, sistemas o procesos debidamente autorizados y bajo mecanismos de autenticación segura.
- **Integridad:** Proteger la exactitud, consistencia y completitud de la información, evitando modificaciones no autorizadas.
- **Disponibilidad:** Asegurar que la información y los sistemas estén disponibles cuando sean requeridos, especialmente para la atención oportuna en salud.
- **Legalidad y cumplimiento:** Dar estricto cumplimiento a la normativa vigente en materia de protección de datos personales, seguridad de la información y regulación del sector salud.
- **Responsabilidad y uso ético:** Promover el uso adecuado, responsable y ético de la información por parte de todos los usuarios.
- **Mejora continua:** Evaluar y fortalecer de manera permanente los controles de seguridad, a través de auditorías, gestión de incidentes y revisión del SGSI.

Radiólogos Especializados de Bucaramanga S.A. se compromete con el diseño, implementación y mejora progresiva del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001. Para ello, definirá e integrará de manera gradual las políticas, procedimientos y controles técnicos, administrativos y físicos necesarios para mitigar riesgos y proteger la información.

El incumplimiento de los lineamientos establecidos y formalizados en el marco de esta política podrá dar lugar a medidas administrativas, disciplinarias o contractuales, de acuerdo con la normativa laboral vigente y los reglamentos internos de la organización.

8. ESTRATEGIAS Y LÍNEAS DE ACCIÓN

Radiólogos Especializados de Bucaramanga S.A. priorizará y desarrolla las siguientes estrategias y líneas de acción para garantizar la implementación efectiva de la Política de Seguridad y Privacidad de la Información, asegurar la protección integral de los activos de información y fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI), bajo un enfoque de gestión de riesgos y mejora continua.

8.1. Estrategia de Gestión de Riesgos de Seguridad de la Información

Objetivo: Identificar, analizar, evaluar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Líneas de acción:

- Identificar y mantener actualizado el inventario de activos de información, incluyendo información clínica, imágenes diagnósticas, sistemas de información y plataformas tecnológicas.
- Realizar evaluaciones de riesgos de seguridad de la información conforme a ISO/IEC 27001.
- Definir e implementar planes de tratamiento del riesgo, priorizando los riesgos asociados a datos sensibles.
- Monitorear y revisar los riesgos de manera continua, especialmente frente a cambios tecnológicos o normativos.

8.2. Estrategia de Protección de Datos Personales y Datos Sensibles

Objetivo: Garantizar el tratamiento seguro, legal y ético de los datos personales y datos sensibles, en especial los relacionados con la salud.

Líneas de acción:

- Implementar controles administrativos, técnicos y físicos para la protección de datos sensibles (imágenes diagnósticas y resultados médicos)
- Asegurar el cumplimiento de los principios de protección de datos personales establecidos en la Ley 1581 de 2012.
- Gestionar autorizaciones, avisos de privacidad y políticas de tratamiento de datos personales.
- Restringir el acceso a la información sensible bajo el principio de mínimo privilegio.

8.3. Estrategia de Control de Accesos y Gestión de Identidades

Objetivo: Prevenir accesos no autorizados a los sistemas de información y activos críticos.

Líneas de acción:

- Definir perfiles de acceso según roles y responsabilidades.
- Implementar mecanismos de autenticación segura (credenciales robustas, doble factor cuando aplique).
- Gestionar el ciclo de vida de usuarios (creación, modificación y revocación de accesos).
- Revisar periódicamente los permisos de acceso a sistemas de información y plataformas.
- Registrar y monitorear los accesos a la información.

8.4. Estrategia de Seguridad Tecnológica y Operativa

Objetivo: Proteger la infraestructura tecnológica frente a amenazas internas y externas.

Líneas de acción:

- Implementar controles de seguridad en redes, servidores, estaciones de trabajo y dispositivos conectados.
- Mantener actualizados los sistemas operativos, aplicaciones y equipos mediante parches de seguridad.
- Implementar soluciones de protección contra malware y ataques cibernéticos.

- Establecer esquemas de respaldo (backups) periódicos y pruebas de restauración.
- Garantizar la disponibilidad y continuidad de los sistemas críticos para la atención en salud.

8.5. Estrategia de Gestión de Incidentes de Seguridad de la Información

Objetivo: Detectar, gestionar y responder de manera oportuna a incidentes de seguridad.

Líneas de acción:

- Definir y documentar el procedimiento de gestión de incidentes de seguridad de la información.
- Establecer canales formales de reporte de incidentes.
- Clasificar y atender los incidentes según su impacto y criticidad.
- Realizar análisis de causa raíz y acciones correctivas.
- Notificar a las autoridades competentes y a los titulares de la información cuando aplique, conforme a la normativa vigente.

8.6. Estrategia de Continuidad del Negocio y Recuperación ante Desastres

Objetivo: Garantizar la continuidad de los servicios de imágenes diagnósticas ante eventos disruptivos.

Líneas de acción:

- Identificar procesos críticos y sistemas esenciales para la atención en salud.
- Implementar planes de continuidad del negocio y recuperación ante desastres.
- Asegurar la disponibilidad de información clínica crítica en escenarios de contingencia.
- Integrar la continuidad del negocio con la gestión de riesgos institucional.

8.7. Estrategia de Concientización y Capacitación en Seguridad de la Información

Objetivo: Fortalecer la cultura organizacional en seguridad y privacidad de la información.

Líneas de acción:

- Desarrollar programas de capacitación periódica para colaboradores.

- Sensibilizar sobre el manejo seguro de la información clínica y administrativa.
- Capacitar en el reconocimiento de amenazas como phishing, malware y fraudes digitales.
- Evaluar periódicamente el nivel de conocimiento del personal.
- Promover buenas prácticas de seguridad de la información en todos los niveles de la organización.

9. VIGENCIA

La presente Política de Seguridad y Privacidad de la Información entra en vigencia a partir del nueve (9) de Abril de dos mil veinticuatro (2024); y en cuadro de control se dejará constancia de la versión vigente y fecha de modificación o actualización.

Actualizaciones de la política: **Radiólogos Especializados de Bucaramanga S.A.** podrá modificar los términos y condiciones del presente documento de políticas y procedimientos como parte de nuestro esfuerzo por cumplir con las obligaciones establecidas.

10. CONTROL DE CAMBIOS

Código	Documento	Descripción	Fecha de Aprobación	Versión
S005 - PO	Política de seguridad y privacidad de la información.	Documento original	Abril de 2024	01

Elaborado por:	Revisado por:	Aprobado por:
Deixon Ortiz Ruiz *Oficial de Protección de Datos*	**Luz Dary Diaz Villamizar** *Administradora* **José Alberto Rueda Suarez** **Ramon Rodríguez Angarita** *Área de Sistemas* **Nieto & Parra Abogados** *Área Jurídica*	**Juan Carlos Mantilla Suarez** *Representante Legal*
Fecha de Elaboración: Abril 2024	**Fecha de Revisión:** Abril 2024	**Fecha de Aprobación:** Abril 2024