Contenido

1. INTRODUCCIÓN

El presente documento establece el Plan de Gestión de Riesgos de la Información para la base de datos Oracle, el almacenamiento NAS y el aplicativo Xenco la ESE Hospital San Juan de Dios de Yarumal, su objetivo es garantizar la seguridad, integridad, disponibilidad y confidencialidad de la información médica y administrativa.

2. OBJETIVOS

2.1. Objetivo general

Establecer un plan integral de gestión de riesgos de la información para la base de datos Oracle, el almacenamiento NAS y el aplicativo Xenco, con el fin de garantizar la confidencialidad, integridad, disponibilidad y seguridad de la información médica y administrativa del hospital.

2.2. Objetivos específicos

- Identificar los activos de información críticos de la institución y su importancia en los procesos operativos y clínicos.
- Detectar amenazas y vulnerabilidades que puedan comprometer la seguridad de los activos de información.
- Diseñar e implementar estrategias de mitigación para reducir los riesgos asociados a la pérdida, alteración o divulgación no autorizada de información.
- Establecer procedimientos de respaldo y recuperación que aseguren la continuidad del servicio ante incidentes de seguridad.
- Implementar mecanismos de monitoreo y auditoría para detectar actividades sospechosas y verificar el cumplimiento de las políticas de seguridad.
- Definir un plan de respuesta ante incidentes que permita actuar de forma oportuna y eficiente ante eventos que afecten la seguridad de la información.
- Asegurar el cumplimiento del marco legal y normativo vigente, aplicable a la protección de los datos personales y la gestión de la información en el sector salud.

3. ALCANCE

El plan busca identificar, analizar, evaluar y tratar los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información, garantizando la continuidad del negocio y el cumplimiento normativo.

4. TALENTO HUMANO

Oficial de seguridad de la información y demás personal involucrado en cuanto a los riesgos de la información.

5. MATERIALES, INSUMOS Y DISPOSITIVOS

Dispositivos, políticas, manuales, inventario de activos de información.

6. ENFOQUE DIFERENCIAL

El principio de enfoque diferencial reconoce que hay poblaciones con características particulares en razón de su edad, género, raza, etnia, condición de discapacidad y víctimas de la violencia, para las cuales el Sistema General de Seguridad Social en Salud ofrecerá especiales garantías y esfuerzos encaminados a la eliminación de las situaciones de discriminación y marginación. (Artículo 3, Ley 1438 de 2011).

La ESE Hospital reconoce la existencia de grupos poblaciones que por diferentes condiciones sociales, culturales, económicas y de salud requieren una especial atención, haciendo énfasis en la igualdad de oportunidades desde la diferencia, la diversidad y la no discriminación. Para ampliar información diríjase al protocolo de atención con enfoque diferencial **PT-09-001.**

7. DEFINICIONES

- **Amenaza:** causa potencial de un incidente no deseado que puede dañar un activo.
- **Vulnerabilidad:** debilidad o hueco en un activo o control que puede ser aprovechado por una amenaza.
- **Riesgo de la Información:** la probabilidad de que una amenaza explote una vulnerabilidad, causando un impacto negativo en la institución.
- **Confidencialidad:** garantizar que solo las personas autorizadas accedan a la información.
- **Integridad:** mantener la información precisa, completa y sin modificaciones no autorizadas.
- **Disponibilidad:** asegurar que los usuarios autorizados tengan acceso a la información cuando la requieran.
- **Impacto:** el resultado de la materialización de un riesgo sobre la confidencialidad, integridad o disponibilidad de la información, generando pérdidas financieras, operativas o reputacionales.
- **Probabilidad:** la posibilidad de que una amenaza específica aproveche una vulnerabilidad existente.

8. IDENTIFICACIÓN DE ACTIVOS

8.1. Base de Datos Oracle

- Datos de pacientes (historias clínicas, diagnósticos, tratamientos).
- Información administrativa (facturación, citas, compras).
- Credenciales y roles de usuarios.

8.2. NAS (Network Attached Storage)

- Imágenes médicas (rayos X, tomografías, resonancias).
- Respaldo de documentos médicos y administrativos.
- Archivos de auditoría y logs de seguridad.

8.3. Aplicativo Xenco

- Gestión de historias clínicas.
- Administración contable, costos y facturación.
- Control de inventarios y cartera.
- Gestión de usuarios y roles administrativos.

9. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD
Ataques de ransomware	Falta de segmentación de red, Gestión de permisos débiles	Crítico	Alta
Robo de credenciales	Hardware obsoleto, falta de redundancia	Crítico	Alta
Fallas en el NAS	Hardware obsoleto, falta de redundancia	Crítico	Media
Intrusiones externas	Firewalls mal configurados	Alto	Media
Errores humanos	Capacitación deficiente	Medio	Alta
Pérdida de datos	Falta de respaldo frecuente	Crítico	Media
Vulnerabilidad en Xenco	Falta de actualizaciones y monitoreo	Alto	Media

10. ESTRATEGIAS DE MITIGACIÓN

10.1. Seguridad en la Base de Datos Oracle

- Implementación de autenticación multifactor (MFA) para accesos administrativos.
- Encriptación de datos en reposo y en tránsito con Oracle Advanced Security.
- Aplicación de parches y actualizaciones de seguridad.
- Configuración de auditoría avanzada (Oracle Audit Vault).
- Restricción de accesos mediante roles y privilegios mínimos.

10.2. Seguridad en el NAS

- Configuración de RAID para tolerancia a fallos.
- Uso de snapshots y copias de seguridad incrementales.
- Implementación de cifrado de datos en el NAS.
- Control de acceso basado en Active Directory o LDAP.
- Monitoreo de logs de acceso con alertas automáticas.

10.3. Seguridad en el Aplicativo Xenco

- Implementación de actualizaciones periódicas para evitar vulnerabilidades.
- Configuración de roles y permisos granulares.
- Monitoreo de accesos y generación de alertas en caso de actividad sospechosa.
- Respaldo automático de datos críticos.
- Autenticación multifactor (MFA) para accesos administrativos.

10.4. Respaldo y Recuperación

- Respaldo diario de la base de datos, NAS y Xenco en un servidor externo seguro.
- Pruebas periódicas de recuperación de datos.
- Uso de almacenamiento en la nube como respaldo secundario.
- Políticas de retención de datos según normativas hospitalarias.

10.5. Protección Contra Ataques y Malware

- Instalación de sistemas de detección y prevención de intrusos (IDS/IPS).
- Segmentación de red entre base de datos, NAS, Xenco y usuarios finales.
- Bloqueo de accesos desde ubicaciones no autorizadas.
- Software antimalware actualizado en servidores y estaciones de trabajo.

11. MONITOREO Y AUDITORÍA

- Implementación de SIEM (Security Information and Event Management).
- Auditoría trimestral de seguridad en base de datos, NAS y Xenco.
- Detección de accesos sospechosos con alertas en tiempo real.
- Registro de cambios y accesos en un servidor de logs centralizado.

12. Plan de Respuesta ante Incidentes

1. **Detección:** Identificación de actividad sospechosa.
2. **Contención:** Desconexión del sistema afectado.
3. **Erradicación:** Eliminación del malware o amenaza.
4. **Recuperación:** Restauración de datos y servicios.
5. **Lecciones aprendidas:** Evaluación y refuerzo de seguridad.

13. MARCO LEGAL Y NORMAS

- Ley 1581 de 2012 (Protección de Datos Personales)

- Regula el tratamiento de datos personales en Colombia.
- Define los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
- Establece la Autoridad Nacional de Protección de Datos (Superintendencia de Industria y Comercio, SIC) como ente regulador.

- Decreto 1377 de 2013

- Reglamenta la Ley 1581 y establece mecanismos para el consentimiento del titular de los datos.
- Introduce medidas para garantizar la seguridad de la información personal.

- Ley 1266 de 2008 (Habeas Data y Protección de Datos Financieros)

- Regula el manejo de información financiera, crediticia y comercial de personas naturales y jurídicas.

- Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública)

- Establece los principios y regulaciones para garantizar el acceso a la información pública.
- Exige a las entidades del Estado la gestión adecuada de sus activos de información.

- Decreto 103 de 2015

- Reglamenta la Ley 1712 y detalla la gestión documental, protección de datos y políticas de publicación de información pública.

- CONPES 3854 de 2016 - Política Nacional de Seguridad Digital

- Define estrategias para la gestión de riesgos en la seguridad de la información a nivel gubernamental y empresarial.
- Enfatiza la adopción de estándares internacionales como la **ISO/IEC 27001**.

- Ley 1273 de 2009 (Delitos Informáticos)

- Penaliza el acceso abusivo a sistemas informáticos, interceptación de datos, suplantación de identidad y otros delitos cibernéticos.

- ISO/IEC 27001:2013 (Sistema de Gestión de Seguridad de la Información - SGSI)

- Es la norma más reconocida a nivel mundial para gestionar la seguridad de la información dentro de una organización.
- Requiere la identificación y clasificación de activos de información, así como la implementación de controles para mitigar riesgos.
- Se basa en el enfoque de gestión de riesgos, lo que permite evaluar amenazas y vulnerabilidades en los activos de información.

- ISO/IEC 27002:2022 (Código de Buenas Prácticas para la Gestión de Seguridad de la Información)

- Proporciona directrices detalladas para la implementación de controles de seguridad definidos en la ISO/IEC 27001.
- Incluye controles para la protección de activos de información, control de accesos, cifrado, gestión de incidentes y continuidad del negocio.

14. Seguimiento y evaluación

- **Optimizar el rendimiento**: aplicar mejoras en consultas SQL, optimizar infraestructura y servidores
- **Seguridad**: reforzar controles de acceso, segmentación de red y autenticación multifactor.
- **Respaldo y recuperación**: ajustar frecuencias de respaldos y verificar l integridad de las copias y que se estén haciendo según el plan
- **Verificación de respaldos**: implementar un proceso de monitoreo continuo para garantizar el buen funcionamiento de los activos de información
- **Capacitación**: reforzar la formación del personal en buenas prácticas de seguridad.

15. CONTROL DE CAMBIOS

Fecha	Versión	Páginas Afectadas	Descripción del contenido
29/04/2025	01		Creación documento original
25/03/2026	02	Todo el documento	Actualización del documento

16. APROBACIÓN

Actualización	Revisó	Aprobación
Gustavo Adolfo Gómez López	Yenny Alexandra Herrera Agudelo - Ana Maria Yepes Torres	Daniel Alcides Vergara Tobón
Auxiliar de sistemas	Profesional de Calidad - Apoyo de calidad	Gerente