Contenido

1. INTRODUCCIÓN 2
2. OBJETIVOS 2
   2.1. Objetivo general 2
   2.2. Objetivos específicos 2
3. ALCANCE 3
4. TALENTO HUMANO 3
5. MATERIALES, INSUMOS Y DISPOSITIVOS 3
6. ENFOQUE DIFERENCIAL 3
7. DEFINICIONES 3
8. IDENTIFICACIÓN DE LOS ACTIVOS 4
9. CLASIFICACIÓN DE LOS ACTIVOS 4
10. POLÍTICAS DE SEGURIDAD 5
   10.1. Control de Acceso 5
   10.2. Protección de Datos 5
   10.3. Respaldo y Recuperación 5
   10.4. Monitoreo y Auditoría 5
   10.5. Actualización y Parches 5
11. PLAN DE RESPUESTA ANTE INCIDENTES 6
12. MARCO LEGAL Y NORMAS 6
13. SEGUIMIENTO Y EVALUACIÓN 8
14. CONTROL DE CAMBIOS 8
15. APROBACIÓN 8

1. INTRODUCCIÓN

El presente documento establece el Plan de Gestión de Activos de Información para garantizar la seguridad, disponibilidad, integridad y confidencialidad de los datos almacenados y procesados en la infraestructura tecnológica de la ESE. Este plan se enfoca en la administración de los activos de información clave, los cuales incluyen:

- **Base de datos Oracle**: plataforma central de almacenamiento donde se resguardan los datos procesados por el sistema, asegurando integridad y disponibilidad.
- **Sistema de almacenamiento NAS (Network Attached Storage)**: solución de almacenamiento en red utilizada para respaldo y recuperación de la información crítica.
- **Aplicativo Xenco**: plataforma encargada de la recopilación y gestión de los datos clínicos y administrativos, que posteriormente se almacenan en la base de datos Oracle.

Activo: Base de Datos Oracle, Almacenamiento NAS, XENCO.

2. OBJETIVOS

2.1. Objetivo general

Establecer un plan de gestión de activos de información que garantice la seguridad, disponibilidad, integridad y confidencialidad de los datos almacenados y procesados en la infraestructura tecnológica de la ESE.

2.2. Objetivos específicos

- Identificar y clasificar los activos de información clave utilizados en la ESE.
- Establecer políticas de seguridad para el control de acceso, protección de datos, respaldo y recuperación, monitoreo y actualización de sistemas.
- Definir un plan de respuesta ante incidentes que minimice el impacto sobre los activos de información.
- Asegurar el cumplimiento del marco legal y normativo relacionado con la protección de datos y seguridad de la información.
- Implementar mecanismos de seguimiento, evaluación y mejora continua en la gestión de los activos de información.

3. ALCANCE

Establecer los límites para la identificación, inventario, clasificación y etiquetado de los activos que procesan, almacenan o transportan información crítica, garantizando que cada activo tenga un responsable asignado y un nivel de protección acorde a su importancia.

4. TALENTO HUMANO

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

5. MATERIALES, INSUMOS Y DISPOSITIVOS

Dispositivos, bases de datos, documentos, políticas de seguridad, credenciales de seguridad.

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

- **Activo de Información:** es cualquier elemento que tenga valor para la organización y que contenga, procese o transporte información. Puede ser digital (una base de datos), físico (un contrato en papel) o intangible (el conocimiento crítico de un experto).

- **Inventario de Activos:** registro documentado que contiene la lista exhaustiva de todos los activos identificados, sus características y sus responsables.

- **Etiquetado:** aplicación de marcas (marcas de agua digitales o etiquetas físicas) que indican visualmente el nivel de clasificación del activo.

- **Integridad:** garantía de que la información sea exacta, completa y no haya sido modificada o destruida sin autorización.

- **Disponibilidad:** característica de la información de ser accesible y utilizable por los usuarios autorizados cuando la requieran.

8. IDENTIFICACIÓN DE LOS ACTIVOS

ACTIVO	DESCRIPCIÓN	UBICACIÓN	RESPONSABLE
Base de datos Oracle	Almacena información crítica del negocio, paciente y operaciones de la ESE	**Servidores**	**Sistemas**
NAS	Almacenamiento compartido para respaldos, archivos y registros de sistemas	**Centro de datos**	**Sistemas**
XENCO	Aplicativo por medio del cual se captura la información	**Servidores**	**Sistemas**

9. CLASIFICACIÓN DE LOS ACTIVOS

ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	NIVEL DE RIESGO
Base datos Oracle	**Alta**	**Alta**	**Alta**	**Crítico**
NAS	**Media**	**Alta**	**Alta**	**Medio-Alto**
Xenco	**Media**	**Alta**	**Alta**	**Alto**

10. POLÍTICAS DE SEGURIDAD

10.1. Control de Acceso

- Implementación de roles y privilegios en Oracle para restringir accesos innecesarios.
- Uso de autenticación multifactor (MFA) para administradores de base de datos.
- Restricción de accesos al NAS mediante grupos de seguridad y listas de control de acceso
- Implementar roles para los usuarios de XENCO para que solo se acceda a lo que corresponde a su perfil de usuario

10.2. Protección de Datos

- Cifrado de datos en reposo y en tránsito (TDE en Oracle, cifrado SMB/NFS en NAS
- Enmascaramiento y anonimización de datos en entornos de prueba/desarrollo.

10.3. Respaldo y Recuperación

- Política de backups diarios y semanales con RMAN en Oracle y Snapshots en NAS.
- Pruebas periódicas de recuperación de datos para garantizar la efectividad de los backups.
- Tener copia o instalador de XENCO para restablecer el servicio.

10.4. Monitoreo y Auditoría

- Activación de auditoría en Oracle para registrar cambios en datos y accesos.
- Monitoreo de logs y alertas en NAS para detectar accesos no autorizados.
- Monitorear XENCO para su correcto funcionamiento.

10.5. Actualización y Parches

- Aplicación de parches de seguridad y actualizaciones en Oracle y NAS según la necesidad o disponibilidad.

- Mantener actualizado XENCO con los parches que entrega el proveedor del servicio.

11. PLAN DE RESPUESTA ANTE INCIDENTES

ESCENARIO	ACCIÓN CORRECTIVA	RESPONSABLE
Acceso no autorizado a Oracle	Bloqueo de usuario, análisis forense, refuerzo de autenticación	**Sistemas**
Corrupción de datos en Oracle	Restauración desde backup más reciente	**Sistemas**
Fallo del NAS	Restauración desde réplica o backup en sitio alterno	**Sistemas**
Ataque ransomware	Aislamiento del NAS, análisis de logs, recuperación desde Snapshots	**Sistemas**
Falla en XENCO	Reinstalar aplicativo o corregir los archivos afectados, usar servidor de respaldo	**Sistemas**

12. 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.

13. 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.

14. 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

15. 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