E.S.E. HOSPITAL LOCAL EL RETEN

PLAN INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

VERSIÓN IV

VIGENCIA: 2025

Gobernación del Magdalena

EL RETÉN, MAGDALENA 2025

Contenido

INTRODUCCIÓN

La información que reposa en una entidad publica debe estar custodiadas con mecanismos y herramientas que garanticen la seguridad de la de la información, la ESE HOSPITAL LOCAL EL RETEN siguiendo los lineamientos de decreto 612 de 2018 actualiza el plan anual de seguridad y privacidad de la información.

Para la misma se crearán políticas que permitan la seguridad y privacidad de la información que en ella reposa, para la implementación de este plan se tendrá en cuenta las herramientas tecnológicas, ciclo de vida de la información, Ley de archivo y gestión documental.

OBJETIVOS GENERALES

- Este documento tiene como objetivo general la implementación de mejores practicas para el tratamiento de la información que repose en LA ESE HOSPITAL LOCAL EL RETÉN, de acuerdo con los lineamientos establecidos por el departamento administrativo de la función publicas

OBJETIVOS ESPECÍFICOS

- Adoptar mejores practicas para el tratamiento de la información en la E.S.E Hospital Local El Retén.

- Seguir los lineamientos ordenados por la ley para privacidad y seguridad de la información.

-

- Implementación de las tecnologías de la información y la comunicación, para la adecuada protección de la información.

- Identificación y organización de la información por siclo de vida.

MARCO CONCEPTUAL

Ley 1712 de 2014, en su artículo 4, no da la definición del Acceso a la Información Pública, describiéndolo de la siguiente manera: “Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados”

- **Activo:** se refiere a cualquier documento físico o digital que de acuerdo con el tiempo tenga validez.

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.

  También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art3)

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3) • Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras
- organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también

utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que

terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la

- pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de

riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural

  o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad

de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6) • Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

MARCO NORMATIVO

- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales • Ley 594 de 2000 - Ley General de Archivos
- Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Ley 527 de 1999 - Ley de Comercio Electrónico

DESCRIPCIÓN DEL PLAN

Para la ESE HOSPITAL LOCAL EL RETÉN, es una prioridad el adecuado trato que se le da la información que ella reposa, es por eso que mediante este plan entraremos a fortalecer la privacidad y seguridad de la información administrada, utilizando herramientas tecnológicas que nos permitan la adopción de prácticas institucionales para brindar dichas garantías.

Seguimos los lineamientos del departamento administrativo de la función pública y la aplicación del manual de procedimientos de seguridad y privacidad de la información (MPSI)

DIRECTRICES A SEGUIR PARA LA PROTECCIÓN Y PRIVACIDAD DE LA INFORMACIÓN

la gerencia de la ESE HOSPITAL LOCAL EL RETEN, junto a su equipo de colaborados, implementaremos políticas para el educado tratamiento de la información que en nuestra institución reposa y la privacidad de la misma y así salvaguardar la integridad de nuestros usuarios y sus familiares.

- CONFIDENCIALIDAD DE LA INFORMACIÓN: la información que repose en la institución solo será de conocimiento del personal del personal autorizado para ello.
- IMPLEMENTACIÓN MSPI: cumplir los lineamientos del manual de seguridad y privacidad de la información.
- REMISIÓN DE LA INFORMACIÓN: solo se remitirá la información confidencial, cuando quien la solicite tenga legitimación para que se le traslade, de acuerdo con ley de habeas data.
- GARANTÍAS: esta institución se compromete a garantizar la seguridad de la información.
- IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN: implementación de bases de datos que permitan tener la información mas segura.

METODOLOGÍA

Para garantizar la implementación de este plan se tendrán en cuenta los siguientes pasos:

1. recepción de la información.
2. aplicación de las políticas de MPSI.
3. políticas para la seguridad de la información.
4. auditorías internas.