PLAN DE TRATAMIENTO DE RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSIÓN IV

VIGENCIA: 2025

GOBERNACIÓN DEL MAGDALENA

EL RETÉN, MAGDALENA 2025

Contenido

INTRODUCCIÓN

La E.S.E Hospital Local El Retén, en cumplimiento de los lineamientos legales para la protección de la información que ella reposa, actualiza el Plan Tratamiento De Riesgo De La Seguridad Y Privacidad De La Información, con el fin de prever los riesgos que se puedan presentar con la divulgación de información confidencial.

Este plan tiene como objetivo la planificación del tratamiento que se le dará a la información en nuestra institución en la vigencia 2025, acatando todos los lineamientos vigentes de la legislación colombiana.

Es compromiso de nuestra institución velar por la seguridad y la privacidad de la información que en ella se maneje, por ello adoptaremos buenas prácticas de confidencialidad, mecanismos y herramientas que nos permitan cumplir a cabalidad con este plan.

MISIÓN

Somos una Empresa Social Del Estado que ofrece servicios de atención en salud garantizando a todas las personas el acceso a los servicios de prevención, promoción, protección y recuperación de la salud con eficiencia, calidad, seguridad y oportunidad, contamos con un capital humano calificado, formado en valores, y atención humanizada, siendo responsables con el medio ambiente y la optimización de recursos, comprometidos con la mejora continuo para la prestación eficiente de un servició orientado a haciala satisfacción del usuario y sus familia

VISIÓN

En el 2025 seremos reconocida como una Empresa Social Del Estado que ofrece servicios oportunos y de calidad, fundamentados en su equipo humano e infraestructura tecnológica, La ESE Hospital Local De Reten fijará como propósito fortalecer los servicios habilitados con reconocimiento servicios prestados con responsabilidad Social, humanizados, gestión administrativa y financiera sostenible, y preservación del ambiente en beneficio de nuestros usuarios y sus familias.

VALORES Y PRINCIPIOS INSTITUCIONALES

ORIENTACION AL USUARIO: El hospital actuará en todo momento en función de satisfacer las necesidades y expectativas del usuario en materia de servicios de salud, impulsando una atención y trato personalizados.

DILENGENCIA: Los funcionarios cumplirán con los deberes, funciones y responsabilidades asignadas a su cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos.

EFICACIA: La actuación de los funcionarios del Hospital se orientará hacia la adopción de decisiones que garanticen el mejor resultado, concreción de logros que afecten los servicios de salud que se prestan al usuario.

EFICIENCIA: Los funcionarios del Hospital actuaran responsablemente con el uso de los recursos para lograr los mejores

resultados, reconociendo que los recursos son limitados, y eligiendo entre alternativas que pueden suministrar el mayor beneficio.

INNOVACIÓN: El Hospital y los funcionarios de este, deberán tener orientación a fomentar y crear nuevas ideas imprimiendo creatividad e imaginación lo que nos permitirá mejorar y fortalecer nuestra competitividad y liderazgo.

HONESTIDAD: Nos comprometemos en actuar y desarrollar nuestra misión en un ambiente de transparencia, de cara a la verdad y en cumplimento a la ley.

RESPETO: Propiciamos el respeto a la persona, reconocimiento y compromiso al valor de la diversidad de ideas y puntos de vista de los colaboradores, de los usuarios y sus familias. Tenemos especial preocupación por aquellos que se encuentran en estado devulnerabilidad.

TRABAJO EN EQUIPO: Fomentamos la colaboración al interior del hospital, con la red asistencial y la comunidad respetando y valorando nuestras diferencias, fortaleciendo las relaciones interpersonales y priorizando el éxito del equipo por encima del éxito individual.

DILENGENCIA: Los funcionarios cumplirán con los deberes, funciones y responsabilidades asignadas a su cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos.

EFICACIA: La actuación de los funcionarios del Hospital se orientará hacia la adopción de decisiones que garanticen el mejor resultado, concreción de logros que afecten los servicios de salud que se prestan al usuario.

EFICIENCIA: Los funcionarios del Hospital actuaran responsablemente con el uso de los recursos para lograr los mejores resultados, reconociendo que los recursos son limitados, y eligiendo entre alternativas que pueden suministrar el mayor beneficio.

INNOVACIÓN: El Hospital y los funcionarios de este, deberán tener orientación a fomentar y crear nuevas ideas imprimiendo creatividad e

imaginación lo que nos permitirá mejorar y fortalecer nuestra competitividad y liderazgo.

HONESTIDAD: Nos comprometemos en actuar y desarrollar nuestra misión en un ambiente de transparencia, de cara a la verdad y en cumplimento a la ley.

RESPETO: Propiciamos el respeto a la persona, reconocimiento y compromiso al valor de la diversidad de ideas y puntos de vista de los colaboradores, de los usuarios y sus familias. Tenemos especial preocupación por aquellos que se encuentran en estado devulnerabilidad.

TRABAJO EN EQUIPO: Fomentamos la colaboración al interior del hospital, con la red asistencial y la comunidad respetando y valorando nuestras diferencias, fortaleciendo las relaciones interpersonales y priorizando el éxito del equipo por encima del éxito individual.

COMPROMISO: Trabajamos comprometidos más allá de nuestro simple deber, generando siempre nuestro mayor esfuerzo consecuentes a la capacidad de la entidad. ÉTICA: Los funcionarios del Hospital sostendrán una conducta transparente, honesta y preocupada por la dignidad de todas las personas con las que se interactúa.

VOCACION DE SERVICIO: Los funcionarios del Hospital actuaran de manera solidaria y con un accionar desinteresado inclinándose a brindar en todo instante colaboración y/o ayuda.

JUSTICIA: Todos los funcionarios actuaran con imparcialidad garantizando los derechos de las personas, con equidad, igual dad y sin discriminación.

CALIDAD: La orientación hacia la calidad nos exige procedimientos para evaluar la eficiencia, la efectividad y la seguridad de las intervenciones preventivas, de apoyo y curativas. Actuaremos aplicando nuestro recurso maximizado los beneficios de salud con el mínimo riesgo, y la máxima satisfacción del paciente con el proceso.

CONFIANZA: Entregaremos esperanza y seguridad en nuestro actuar.

PRINCIPIOS INSTITUCIONALES COMPROMISO EN EL SERVICIO: desarrollamos y mantenemos una destacada actitud de servicio frente a los usuarios y sus familiares, buscando soluciones eficaces que contribuyan a la mejora continúa reflejadas en la satisfacción de la asistencia generada por nuestro personal.

TRANSPARENCIA INSTITUCIONAL: Buscamos dar cumplimiento a nuestra misión y visión corporativa, con apego y cumplimiento a los valores éticos que, permitan generar un ambiente transparente y una relación de mutuo beneficio entre usuarios, familiares y partes interesadas.

MOVILIZADORES DE CAMBIO: Como institución sabemos que nuestras acciones no solamente pueden quedar trazadas en nuestro de trabajo cotidiano, es por ello que procuramos llevar soluciones innovadoras haciendo uso de la capacidad institucional.

COMPROMISO CON LA CALIDAD: Nos comprometemos con el logro de los mejores resultados a través de la prestación de nuestros servicios, desplegando una gestión efectiva, eficiente y oportuna de nuestros los procesos y recursos.

RESPONSABILIDAD SOCIAL: A través de nuestro servicio, nos comprometemos con el desarrollo, el bienestar y el mejoramiento de la calidad de vida de nuestros funcionarios y las partes interesadas, apoyados en acciones responsables.

ARMONÍA CON EL MEDIO AMBIENTE: Nos comprometemos en que nuestras acciones estén ligadas en respetar, preservar y conservar un medio ambiente sano y saludable.

OBJETIVOS GENERALES

Identificar los posibles riesgos que se presenten en nuestra institución con relación a la divulgación de la información de carácter confidencial

que ella reposa, y así; adoptar medidas y estrategias que nos permitan salvaguardad la seguridad de la misma.

OBJETIVOS ESPECÍFICOS

- Fortalecer a la E.S.E Hospital Local El Retén, en la identificación de riesgo de la información.
- Establecer diagnósticos sobre el riesgo de la información ajustados a la realidad de la E.S.E Hospital Local El Retén.
- Salvaguardar la información de carácter confidencial que reposa en nuestra entidad.

MARCO NORMATIVO

- Decreto Nacional 2573 de 2014
- Concordancias: Decreto 1078 del 2015
- Decreto 415 del 2016
- Decreto Numero 1083 de 2015
- Ley 1712 de 2014
- Decreto 103 de 2015 Decreto 1494 de 2015

MARCO CONCEPTUAL

Acceso A La Información Pública: 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. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la

misma(sistemas, soportes, edificios, personas. que tenga valor para laorganización. (ISO/IEC 27000).

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 ocontrole 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, art 3).

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 parallevar 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 1581de 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, art3).

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 literalh).

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 sudiscriminación, tales como aquellos que revelen el origen racial o étnico, laorientación 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 ygarantías 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 1712de 2014. (Ley 1712 de 2014, art 6)

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014. Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente. Registro Nacional de **Bases de Datos:** Directorio público de las bases de datos sujetas aTratamiento que operan en el país. (Ley 1581 de 2012, art 25).

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad dedemostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 ysus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3). **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

DESCRIPCIÓN DEL PLAN

Con el fin de implementar del Modelo de Seguridad y Privacidad de la Información en la ESE Hospital Local El Retén, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y el ciclo de operaciones que determinan los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de sus decretos. Para cada una de las fases del proceso se plantea una descripción detallada de los mismos junto a sus objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema

de gestión sostenible dentro de la entidad. Acorde a lo anterior se definenlas siguientes 5 fases:

- Diagnóstico.
- Planeación.
- Implementación.
- Evaluación.
- Mejora continua

ESTRATEGIAS PARA LA IMPLEMENTACIÓN DEL PLAN

ESTRATEGIA 1	Diligenciar una herramienta de diagnóstico que permita determinar el estado actual de la seguridad y privacidad de la información. Diligenciar una herramienta para determinar el nivel de madurez de los controles de seguridad de la información.
ESTRATEGIA 2	Efectuar pruebas de vulnerabilidad y elaborar documento con los hallazgos encontrados.
ESTRATEGIA 3	Evaluar el avance de laimplementación del ciclo de operaciones al interior de la entidad
ESTRATEGIA 4	Evaluar el nivel de cumplimiento con la legislación vigente, relacionado con protección de datos personales
ESTRATEGIA 5	Evaluar el uso frente a prácticas de Ciberseguridad.

METAS TRAZADAS POR LA INSTITUCIÓN POR LA IMPLEMENTACIÓN DEL PLAN

META 1	Identificación del uso de buenas prácticas en Ciberseguridad
META 2	Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
META 3	Identificar el avance de la implementación del ciclo de operación al interior de la entidad
META 4	Determinar el nivel de madurez de los controles de seguridad de la información.
META 4	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.