PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIT. 890.204.895-0

LILIAM BEATRIZ SMITH SANCHEZ MURILLO
Gerente
VIGENCIA
2026

Km 1 Vía Puerto Berrio
Tels. (7) 6260141 / 6260330
Cimitarra, Santander
Nit. 890.204.895-0

Tabla de contenido

Km 1 Vía Puerto Berrio
Tels. (7) 6260141 / 6260330
Cimitarra, Santander
Nit. 890.204.895-0

1. INTRODUCCIÓN

La ESE Hospital Integrado San Juan de Cimitarra, con este documento busca lograr la implementación y las mejoras dadas por el Departamento de Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías e Información en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información. El Modelo de Seguridad y Privacidad de la Información, pretende lograr en la institución y sus clientes internos, externos y partes interesadas confianza en el manejo de la información garantizando para cada uno la privacidad, continuidad, integralidad y disponibilidad de los datos.

2. CONTEXTO ESTRATÉGICO:

2.1. MISIÓN

Prestar los servicios de salud de primer nivel, para toda la comunidad del área de influencia, de conformidad con los lineamientos establecidos por el sistema general de seguridad Social en Salud, cumplidores de los principios de eficiencia, eficacia, oportunidad, accesibilidad y calidad, en la prestación del servicio, contando con equipos y recurso humano debidamente capacitado y con un profundo sentido humano.

2.2. VISIÓN

Para el año 2030 seremos una institución de mayor nivel con infraestructura, dotación y con tecnología de última generación. Con un servicio humanizado en la atención segura al usuario y la familia. Serán la expresión de un sano equilibrio entre el balance social y económico lo que darán la solidez estructural necesaria para adaptarse a los cambios del medio.

2.3. POLITICA DE INTEGRIDAD

La ESE Hospital Integrado San Juan de Cimitarra, Santander consolida la integridad como principal prevención de la corrupción y motor del cambio de los comportamientos de los servidores públicos. Esta política se basa en la prevención de la corrupción, herramientas de seguimiento y control, y al establecimiento y promoción de valores, incentivar a los servidores públicos a interiorizar y fortalecer prácticas y comportamientos íntegros y ejemplares.

La ESE Hospital Integrado San Juan de Cimitarra, Santander consciente de la importancia de su función y de la responsabilidad que esta implica, con el propósito de garantizar el actuar y poniendo sobre manera los valores de HONESTIDAD, RESPETO, COMPROMISO, DILIGENCIA, JUSTICIA, ETICO Y PROFESIONAL del personal que lo

conforma y de consolidar la confianza de la ciudadanía, implementa el Modelo de Integración de Planeación y Gestión orientado a promover y fortalecer la Integridad en el ejercicio de sus funciones.

3. OBJETIVOS

- Identificar y promover los valores y deberes íntegros promovidos por la ESE, que han de observar los servidores públicos en el desempeño de sus funciones.
- Establecer los criterios, conductas y controles que normen el comportamiento de los servidores públicos.
- Promover un ambiente de trabajo agradable y profesional, basado en el respeto, honestidad, compromiso, diligencia y justicia.
- Orientar la actuación de los servidores públicos.
- Consolidar la confianza de La ESE Hospital Integrado San Juan de Cimitarra, Santander, así como en el personal que la integra.

4. OBJETIVOS PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

4.1. Objetivo General

Generar un documento institucional guiado en lineamientos de buenas prácticas en seguridad y Privacidad de la información para la ESE Hospital Integrado San Juan de Cimitarra.

4.2. Objetivos de esta Gestión

- Promover el uso de mejores prácticas de seguridad de la información en la institución
- Optimizar la gestión de la seguridad de la información al interior de la entidad
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales
- Optimizar la labor de acceso a la información pública Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital, de acuerdo con los contextos establecidos en la Entidad.

5. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

6. TERMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de seguridad de la información, en beneficio de unificar criterios dentro de la ESE Hospital Integrado San Juan de Cimitarra.

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 la organización. (ISO/IEC27000).

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, 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 auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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. 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 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 a Tratamiento 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 de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus 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).

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

7. MARCO NORMATIVO

NORMA	TEMATICA
Resolución 3564 de 2015	Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
Decreto Reglamentario Único 1081 de 2015	Reglamento sobre la gestión de la información pública
Título 9 - Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
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
Ley Estatutaria 1757 de 2015	Promoción y protección del derecho a la participación democrática
Ley estatutaria 1618 de 2013	Ejercicio pleno de las personas con discapacidad
Ley 1437 de 2011:	Código de Procedimiento Administrativo y de lo Contencioso Administrativo
Acuerdo 03 de 2015 del Archivo General de la Nación	Lineamientos generales sobre la gestión de documentos electrónicos
Decreto 019 de 2012	Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública

Decreto 2364 de 2012	Firma electrónica
Ley 962 de 2005	Racionalización de trámites y procedimientos administrativos procedimientos administrativos
Decreto 1747 de 2000	Entidades de certificación, los certificados y las firmas digitales
Ley 527 de 1999	Ley de Comercio Electrónico
Decreto Ley 2150 de 1995	Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Ley Estatutaria 1581 de 2012	Protección de datos personales
Ley 1266 de 2008	Disposiciones generales de habeas data y se regula el manejo de la información

8. DESARROLLO

la ESE Hospital Integrado San Juan de Cimitarra, estructura el Plan de Seguridad y Privacidad de la Información en concordancia con los marcos legales y conceptuales del Estado relacionadas con la Seguridad y Privacidad de la Información, lo cual permite cumplir con el objetivo definido en este Plan, para esto se definen las siguientes fases:

- *Fase I Diagnostico*: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

- *Fase II Planificación (Planear)*: Hace referencia a establecer el Modelo de Seguridad y Privacidad de la Información, en esta fase se debe establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de la entidad.

- *Fase III Implementación (Hacer)*: Hace referencia a implementar u operar el MSPI, en esta fase se debe implementar y operar la política, los controles y procedimientos del MSPI.

- *Fase IV Evaluación de Desempeño (Verificar)*: Hace referencia a hacer seguimiento y revisión del MSPI, en esta fase se debe evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.

- *Fase V Mejora Continua (Actuar):* Hace referencia a mantener y mejorar el MSPI, en esta fase de debe emprender acciones correctivas y preventivas con base en los resultados de la

auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

9. DESCRIPCIÓN DEL PLAN POLITICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION

El equipo de colaboradores y la Gerencia de la ESE Hospital Integrado San Juan de Cimitarra, se comprometen a garantizar la confidencialidad, seguridad e integralidad de la información de los usuarios y su familia, clientes internos y externos en cuanto a seguridad lógica y física de los activos de la información, fomento de canales de comunicación que garanticen acceso y transparencia de la información pública a través de uso adecuado de las TICS, cumpliendo con las disposiciones generales para la protección de datos, aportando al cumplimiento de la Misión, Visión y objetivos estratégicos de la institución.

10. OBJETIVOS DE LA POLITICA DE GESTION DE CALIDAD

- Garantizar la protección de datos personales de usuarios, clientes, proveedores y trabajadores tanto en los medios físicos como electrónicos.
- Controlar el uso efectivo de equipos de cómputo que garantice la confidencialidad, seguridad e integralidad de la información de los usuarios incluyendo.
- Fortalecer el conocimiento y la adherencia en el plan de contingencia en caso de caída del sistema de información.

LILIAM B. SANCHEZ MURILLO
Gerente
ESE. Hospital Integrado San Juan de Cimitarra

Proyecto ELIANA BENAVIDES GALEANO – Control Interno