


PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



HOMERIS

E.S.E. Hospital Mental
Universitario de Risaralda

VIGENCIA AÑO 2019

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
		PÁGINA	2 de 15
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		COPIA CONTROLADA	

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN


Zacarías Mosquera Lara
Gerente

EQUIPO DE TRABAJO

Nydia Lucero Ospina López
Subdirectora Administrativa y Financiera


Andrés Del Río Restrepo
Profesional Universitario Sistemas

Jhoan Sebastián Cuervo Burbano
Profesional Universitario Sistemas

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
		PÁGINA	3 de 15
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		COPIA CONTROLADA	

Contenido

Introducción.....	4
Objetivos	4
Objetivo General	4
Objetivo Especifico.....	4
Alcance	5
Responsable(s)	5
Marco Conceptual (Definiciones Relevantes)	6
Marco Normativo	11
Diseño del Plan	13
Política de Seguridad Informática	13
Referencias	15

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	4 de 15
COPIA CONTROLADA			

Introducción

Este documento pretende adoptar mejoras prácticas, en materia de diagnóstico, planificación, implementación, gestión y mejoramiento continuo, para el Modelo de Seguridad y Privacidad de la Información (MSPI), en la E.S.E. Hospital Mental Universitario de Risaralda. Para ello, se tomarán como referencia los lineamientos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), y el Departamento de Administrativo de la Función Pública en el Modelo Integrado de Planeación y Gestión (MIPG).

El Modelo de Seguridad y Privacidad de la Información busca aumentar la confianza que proporciona la institución a sus clientes internos, externos y partes interesadas, a través de la garantía a la privacidad, continuidad, integralidad y disponibilidad de los datos.


Objetivos

Objetivo General

Generar un documento institucional basado en los lineamientos de buenas prácticas en Seguridad y Privacidad de la Información.

Objetivo Especifico

- Promover el uso de mejores prácticas de seguridad de la información en la E.S.E.
- Optimizar la gestión de la seguridad de la información al interior del Hospital.
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales.
- Optimizar la labor de acceso a la información pública.

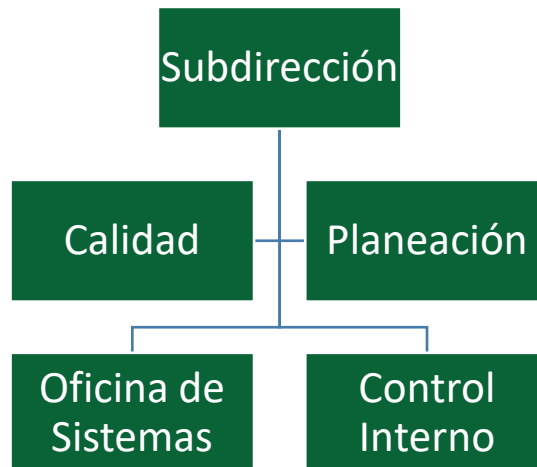
	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSION	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	5 de 15
COPIA CONTROLADA			

Alcance


El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la E.S.E. Hospital Mental Universitario de Risaralda que manejen, procesen o interactúen con información institucional.

Responsable(s)

De acuerdo con la estructura organizacional de los procesos, los responsables de la realización del plan es la siguiente:




- Subdirectora Administrativa.
- Profesional Universitario de Planeación.
- Profesional Universitario de Calidad.
- Ingenieros de Sistemas.
- Control Interno.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSION	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	6 de 15
COPIA CONTROLADA			


Marco Conceptual (Definiciones Relevantes)

- **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

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	7 de 15
COPIA CONTROLADA			


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

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	8 de 15
COPIA CONTROLADA			


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

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	9 de 15
COPIA CONTROLADA			


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, 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

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	10 de 15
COPIA CONTROLADA			

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,


	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	11 de 15
COPIA CONTROLADA			

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:** Calidad 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.

Marco Normativo

- **Ley 57 de 1985** - Publicidad de los actos y documentos oficiales.
- **Decreto Ley 2150 de 1995** - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
- **Ley 527 de 1999** - Ley de Comercio Electrónico.
- **Ley 594 de 2000** - Ley General de Archivos.
- **Decreto 1747 de 2000** - Entidades de certificación, los certificados y las firmas digitales.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	12 de 15
COPIA CONTROLADA			

- **Ley 962 de 2005** - Racionalización de trámites y procedimientos administrativos procedimientos administrativos.
- **Ley 1266 de 2008** - Disposiciones generales de habeas data y se regula el manejo de la información.
- **Ley 1437 de 2011** - Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Decreto 2364 de 2012** - Firma electrónica.
- **Decreto 019 de 2012** - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- **Ley Estatutaria 1581 de 2012** - Protección de datos personales.
- **Ley estatutaria 1618 de 2013** - Ejercicio pleno de las personas con discapacidad.
- **Ley 1712 de 2014** - Ley de Transparencia y acceso a la información pública.
- **Decreto Reglamentario Único 1081 de 2015** - Reglamento sobre la gestión de la información pública.
- **Acuerdo 03 de 2015 del Archivo General de la Nación** - Lineamientos generales sobre la gestión de documentos electrónicos.
- **Anexo 1 - Resolución 3564 de 2015** - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
- **Título 9 - 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.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSION	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	13 de 15
COPIA CONTROLADA			

Diseño del Plan


Política de Seguridad Informática

HOMERIS define su política del riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión en los procesos, así como los del Modelo Estándar de Control Interno, en lo referente a las líneas de defensa, los lineamientos de la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas*, del Departamento Administrativo de la Función Pública (de ahora en adelante DAFP o Función Pública), la cual articula los riesgos de gestión, corrupción y de seguridad digital y la estructura del Sistema Integrado de Gestión – SGI en el módulo de riesgos.

Dado lo anterior, la política de Administración de Riesgos de HOMERIS es la siguiente:

La E.S.E. Hospital Mental Universitario de Risaralda adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores públicos de la entidad se comprometen a:

- 1) Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
- 2) Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- 3) Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para tal efecto.
- 4) Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
- 5) Reportar los eventos de riesgo que se materialicen, utilizando los

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
		PÁGINA	14 de 15
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	COPIA CONTROLADA	


procedimientos e instrumentos establecidos para tal efecto.

- 6) Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
- 7) Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad, para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado, la Alta Dirección asignará los recursos humanos, presupuestales y tecnológicos necesarios, que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política¹.

El siguiente plan está diseñado para cumplir la fase de determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. Para realizar este paso los responsables del plan deben efectuar la recolección de la información con la ayuda de la guía de autoevaluación, guía de encuesta y guía metodológica de las pruebas de efectividad del Modelo de Seguridad y Privacidad de la Información (MSPI).

¹ Tomado del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2019 de HOMERIS.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA NIT: 891.412.134-1	CÓDIGO	100-OT-29
		VERSIÓN	1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	15 de 15
COPIA CONTROLADA			

Referencias

Ministerio de las TIC. *Modelo de seguridad*. Obtenido de:
<http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

Ministerio de las TIC. *Modelo de Seguridad y Privacidad de la Información*. Obtenido de:
https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Escuela Tecnológica Instituto Técnico Central. *Seguridad de la Información*. Obtenido de: <http://www.itc.edu.co/es/nosotros/seguridad-informacion>