PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

HOMERIS
E.S.E. Hospital Mental
Universitario de Risaralda

VIGENCIA AÑO 2021

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

John Jairo Ramírez Cardona
Gerente

EQUIPO DE TRABAJO

Paula Andrea Vélez Cardona
Subdirectora Administrativa y Financiera

Jhon Jairo Naranjo Ramirez
Profesional Universitario Sistemas

Jhoan Sebastián Cuervo Burbano
Profesional Universitario Sistemas

Contenido

INTRODUCCIÓN

Este documento busca lograr la implementación de las mejoras prácticas dadas por el Departamento de Administrativo de la Función Pública con su estrategia en el Modelo Integrado de Planeación y Gestión (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 (MSPI), en la E.S.E. Hospital Mental Universitario de Risaralda.

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.

OBJETIVOS

Objetivo General

Generar un documento institucional guiado por 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 institución.
- Optimizar la gestión de la seguridad de la información al interior de le entidad.
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales.

- Optimizar la labor de acceso a la información pública.

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.

PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFROMACIÓN

La E.S.E Hospital Mental Universitario de Risaralda adopta en su modelo de procesos, el proceso de Seguridad y Privacidad de la Información en el nivel estratégico que permitirá garantizar continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la E.S.E Hospital Mental Universitario de Risaralda, por medio de la definición de políticas, programas, lineamientos, estrategias y actividades.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DEL MINISTERIO/FONDO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

La E.S.E Hospital Mental Universitario de Risaralda, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad,

autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo así por el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones -TIC, a través de políticas y programas.

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 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.
- **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 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.

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.
- 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.

DESCRIPCIÓN DEL PLAN

Política de Seguridad Informática

En la institución, todos los usuarios somos responsables de la información automatizada que manejamos y damos estricto cumplimiento a los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Alcance

Dirigida a todos los trabajadores que están involucrados con el manejo de información automatizada.

Objetivos

Con la elaboración de esta política de seguridad informática se pretende poner en conocimiento de todos los usuarios del Sistema de Información sobre:

a) La importancia de la información.

b) La importancia de la seguridad de la información.

c) El apoyo total del Proceso de Direccionamiento a esta política de seguridad de la información

d) Que la seguridad de la información se consigue entre todos y no es solo una labor del personal del proceso de Gestión de recursos de Información.

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).

PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes.

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumento de levantamiento de activos de información	Sistemas	jun-01-2021	jun-30-2021
	Levantamiento Activos de Información	Socializar la guía de activos de Información.	Sistemas	jun-01-2021	jun-30-2021
		Validar activos de información en el instrumento levantado en la vigencia anterior	Sistemas	jul-01-2021	jul-30-2021
		Identificar nuevos activos de información en cada dependencia	Sistemas	jul-15-2021	jul-30-2021
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Sistemas	ago-02-2021	ago-30-2021
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Sistemas	ago-23-2021	ago-30-2021

		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.	Sistemas	ago-20-2021	dic-29-2021
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Sistemas	mar-22-2021	ago-31-2021
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Sistemas	abr-19-2021	may-31-2021
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Sistemas	may-31-2021	sep-30-2021

		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Sistemas	may-31-2021	sep-30-2021
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Sistemas	jun-21-2021	nov-19-2021
	Publicación	Publicación Matriz de riesgos	Sistemas	jun-21-2021	nov-19-2021
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Sistemas	jun-21-2021	dic-20-2021
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Sistemas	jun-21-2021	dic-20-2021

	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Sistemas	jun-21-2021	dic-20-2021
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.	Sistemas	jun-21-2021	dic-20-2021
Gestión de Incidentes de Seguridad de la Información	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Sistemas	ene-4-2021	dic-31-2021
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información.	Sistemas	may-3-2021	may-31-2021
		Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.)	Sistemas	jun-4-2021	dic-21-2021

Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Sistemas	ene-18-2021	ene-29-2021
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Sistemas	feb-1-2021	dic-20-2021
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Sistemas	abr-22-2021	dic-20-2021

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

Ministerio de las TIC. *Plan de seguridad y privacidad de la información*. Obtenido de:

https://www.mintic.gov.co/portal/604/articles-100251_plan_seguridad_privacidad_informacion_2020_u20201228.pdf