EMPRESA SOCIAL DEL ESTADO
HOSPITAL MENTAL UNIVERSITARIO
DE RISARALDA
NIT 891.412.134-1

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

E.S.E HOSPITAL MENTAL DE RISARALDA

ZACARIAS MOSQUERA LARA

GERENTE

Kilómetro 4 Vía a Cerritos – Av. 30 de Agosto # 87 – 76
pereira.mental@risaralda.gov.co Teléfonos 3373444- 3370406

VIGENCIA AÑO 2018

Plan de Seguridad de la Información y Sistema de Seguridad y Privacidad de la Información

Justificación

Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, dicta el cumplimiento de los requisitos y lineamientos, que tienen como objetivo, gestionar adecuadamente la seguridad de la información, la gestión de activos, la gestión de riesgos y la continuidad en la prestación de los servicios ofrecidos. Dichos requisitos y lineamientos serán aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación, por tal motivo, deberán ser conocidos y cumplidos por todo el recurso humano (servidores públicos, proveedores y terceros), que accedan a los sistemas de información e instalaciones físicas de la Institución.

El Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, se encuentran basados, en el marco de lo establecido, en la norma internacional NTC-ISO-IEC 27001:2013 y las buenas prácticas contenidas en el componente Seguridad y Privacidad de la Información, de la estrategia, este último desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia.

Política General de Seguridad de la Información

El Hospital Mental Universitario de Risaralda consciente de la importancia que la seguridad de la información tiene para el desarrollo y buen funcionamiento de sus procesos internos, ha decidido implementar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma internacional ISO 27001 de 2013 y un Modelo de Seguridad y Privacidad de la Información (MSPI), suscribiendo la presente política.

El Hospital Mental Universitario de Risaralda establece, define y revisa unos objetivos, dentro del SGSI y el MSPI, encaminados a mejorar su seguridad, entendiéndola como la preservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas que la soportan,

incrementando los niveles de confianza en los servidores públicos, pacientes y otras partes interesadas, todo lo anterior, es fortalecido mediante el cumplimiento de todos los requisitos legales, reglamentarios y contractuales, que le sean de aplicación.

El diseño, implantación y mantenimiento del SGSI y el MSPI, se apoyará en los resultados de un proceso continuo de análisis y valoración del riesgo, del que se derivan las actuaciones a desarrollar, en materia de seguridad, dentro del alcance del SGSI y el MSPI, aprobado por la Alta Dirección de El Hospital Mental Universitario de Risaralda.

La Alta Dirección de El Hospital Mental Universitario de Risaralda establecerá los criterios de evaluación del riesgo, de manera que todos aquellos escenarios, que impiden un nivel de riesgo aceptable, sean tratados adecuadamente y mitigados, adicional, la Alta Dirección desarrollará, implantará y mantendrá actualizado un Plan de Continuidad del Negocio, acorde a las necesidades del hospital y dimensionado a los riesgos que le afectan.

La Alta Dirección de El Hospital Mental Universitario de Risaralda se compromete a la implantación, mantenimiento y mejora del SGSI y el MSPI, dotándolos de aquellos medios y recursos que sean necesarios e instando a todos los servidores públicos, proveedores y partes interesadas, para que asuman este compromiso. Para ello, El Hospital Mental Universitario de Risaralda implantará las medidas requeridas para la formación y concienciación de los servidores públicos, proveedores y partes interesadas, en temas de seguridad de la información. A su vez, cuando exista una violación de las políticas de seguridad de la información, aprobadas por la Alta Dirección, El Hospital Mental Universitario de Risaralda se reserva el derecho de aplicar las medidas disciplinarias, acordes a los compromisos laborales de los servidores públicos, proveedores y partes interesadas, dentro del marco legal aplicable y dimensionadas al impacto que tengan sobre la entidad

La responsabilidad general de la seguridad de la información en El Hospital Mental Universitario de Risaralda, recaerá sobre la Alta Dirección y encargados de la seguridad de la información. Por otro lado, todos los servidores públicos, proveedores y partes interesadas, tendrán la obligación de reportar los incidentes, en materia de seguridad, haciendo uso de las directrices establecidas por El Hospital Mental Universitario de Risaralda.

Todo lo definido en la Política General de Seguridad de la Información se concretará y desarrollará, mediante las buenas prácticas, normativas internacionales y procedimientos incluidos en el Sistema de Gestión de Calidad de la Institución, las cuales se integrarán, en la medida de lo posible, con otros sistemas de gestión de

la entidad, compartiendo aquellos recursos en pro de la optimización y buscando la mejora continua de la eficacia y eficiencia de la gestión de los procesos institucionales.

La presente Política General de Seguridad de la Información, será aplicada por todos los servidores públicos, proveedores y partes interesadas del SGSI, MSPI y recursos que se encuentran incluidos en el alcance del SGSI y el MSPI. Adicional, es socializada al interior de El Hospital Mental Universitario de Risaralda y comunicada a las partes interesadas.

Objetivo General

El objetivo principal de la seguridad de la información es mantener un ambiente razonablemente seguro, alineado a la misión del El Hospital Mental Universitario de Risaralda y que permita proteger los activos de información de la misma, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información y el aseguramiento de la continuidad del negocio.

Objetivos Específicos

- Proteger los activos de información de El Hospital Mental Universitario de Risaralda, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información institucionales.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías internas planificadas a intervalos regulares.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información.

EMPRESA SOCIAL DEL ESTADO
HOSPITAL MENTAL UNIVERSITARIO
DE RISARALDA

NIT 891.412.134-1

HOMERIS

Cronograma y seguimiento de SGSI

IdTarea	Nombre Tarea	2018							2019											
		Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
0	**DIAGNOSTICO DEL ESTADO DE IMPLEMENTACION DE ISO 27001**																			
1	**CONTEXTO DE LA ORGANIZACIÓN**																			
1.1	Comprensión De Las Necesidades Y Expectativas De Las Partes Interesadas																			
1.2	Determinación del alcance del sistema de gestión de la seguridad de la información																			
2	**LIDERAZGO**																			
2.1	Política de Seguridad de la Información																			
2.2	Roles, Responsabilidades y Autoridades de Seguridad de la Información																			

2.3	Política de Segregación de Funciones																				
2.4	Apoyo e la identificación de contenido de seguridad y protección de la información en Acuerdo de Confidencialidad y Transparencia																				
3	**PLANIFICACION**																				
3.1	Valoración de riesgos de la seguridad de la información (Modelo de Gestión de Riesgos)																				
3.2	Tratamiento de los riesgos de seguridad de la información																				
3.3	Objetivos de Seguridad de la Información y planes para su logro																				
4	**SOPORTE**																				
4.1	Toma de conciencia																				
4.2	Documentación de Sistema de Gestión de Seguridad de la																				

	Información (manuales, políticas, procedimientos, instructivos, formatos, etc																			
5	**OPERACIÓN**																			
5.1	Valoración de Riesgos de seguridad de la información																			
	Procesos tecnológico																			
	Proceso evaluación de propuestas																			
	Archivo y Gestión documental																			
	Seguridad Física y ambiental																			
	Talento Humano																			
5.2	Tratamiento de los riesgos de seguridad de la información																			
	Procesos tecnológico																			
	Proceso evaluación de propuestas																			

	Archivo y Gestión documental																			
	Seguridad Física y ambiental																			
	Talento Humano																			
6	**EVALUACION DE DESEMPEÑO**																			
6.1	Seguimiento, Medición y Evaluación de seguridad de la información																			
6.2	Auditoría Interna de seguridad de la Información																			
6.3	Revisión por la Dirección																			
7.	**CONTROLES DE SEGURIDAD DE LA INFORMACION**																			
7.1	Contacto con Autoridades y grupos de interes																			
7.2	Propuesta seguridad de la información en proyectos																			
7.3	Inventario de Activos de Información (proceso tecnológico, evaluación de propuestas, Gestión Documental																			

	Inventario Procesos tecnológico																			
	Inventario Proceso evaluación de propuestas																			
	Inventario Archivo y Gestión documental																			
	Inventario Seguridad Física y ambiental																			
	Talento Humano																			
7.4	Valoración de Riesgos de seguridad de la información (ver numerales 5.1 y 5.2)																			
7.5	Lineamientos de uso aceptable de Activos de Información																			
7.6	Política de control de acceso lógico (usuarios - contraseñas)																			
7.7	Procedimiento de custodia de contraseñas de usuarios privilegiados																			
8	**SEGURIDAD FISICA**																			

8.1	Valoración de la seguridad física y de entorno de las áreas seguras (Centro de datos ANI y de cableados en pisos)																				
8.2	Apoyo en el protocolo de seguridad de la sala de evaluación de propuestas																				
9	**SEGURIDAD DE LAS OPERACIONES**																				
9.1	Documentación de actividades de operación tecnológica (toma de respaldo y restauración de información de servidores y de información de aplicaciones, gestión de cambios TI, gestión de capacidad)																				
10	**SEGURIDAD DE LAS COMUNICACIONES**																				
10.1	Definición de políticas de acceso seguro y uso adecuado del servicio de internet																				

10.2	Política de configuración y aseguramiento de conexión inalámbrica																				
10.3	Solicitud de conexión clientes VPN																				
11	**INCIDENTES DE SEGURIDAD DE LA INFORMACION**																				
11.1	Establecimiento del modelo de gestión de incidentes de seguridad de la información																				
12	**CUMPLIMIENTO**																				
12.1	Apoyo en la identificación de la legislación aplicable a seguridad y protección de la información (normograma)																				
12.2	Control de instalación de software no autorizado																				