POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La E.S.E. Hospital Regional Sur Oriental considera la información que gestiona, recolecta y custodia, como un activo valioso para el logro de sus metas y objetivos, reconociendo la importancia de proteger esta información de una amplia variedad de amenazas, diseña la política de seguridad y privacidad de la información, con sus respectivos lineamientos, la cual constituye una parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno en Línea (GEL) y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

1 OBJETIVO:

Brindar las directrices y lineamientos necesarios que deben seguir los funcionarios, contratistas y terceros que cumplan funciones en nombre de La E.S.E. Hospital Regional Sur Oriental, con el fin de fortalecer la Seguridad de la Información y garantizar la disponibilidad, integridad y confidencialidad de la información.

2 ALCANCE

La Política de Seguridad de la Información aplica a toda La E.S.E. Hospital Regional Sur Oriental., sus funcionarios, contratistas, que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la Institución.

3 DEFINICIONES

MSPI: Modelo de Seguridad y Privacidad de la Información**.**
SGSI: Sistema de Gestión de Seguridad de la Información.
Activo de Información: Todo lo que tiene valor para la Organización ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
Amenaza: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
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, (Nota: Control es también utilizado como sinónimo de salvaguarda).
Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.
Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.
Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.
Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.
Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de La E.S.E. Hospital Regional Sur Oriental con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La E.S.E. Hospital Regional Sur Oriental, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.

- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de La E.S.E. Hospital Regional Sur Oriental
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del La E.S.E. Hospital Regional Sur Oriental y la ciudadanía en general. Nivel de cumplimiento Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de La E.S.E. Hospital Regional Sur Oriental:

- La E.S.E. Hospital Regional Sur Oriental ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- La E.S.E. Hospital Regional Sur Oriental protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- La E.S.E. Hospital Regional Sur Oriental protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La E.S.E. Hospital Regional Sur Oriental protegerá su información de las amenazas originadas por parte del personal. • NOMBRE DE LA ENTIDAD protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La E.S.E. Hospital Regional Sur Oriental controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La E.S.E. Hospital Regional Sur Oriental implementará control de acceso a la información, sistemas y recursos de red.
- La E.S.E. Hospital Regional Sur Oriental garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La E.S.E. Hospital Regional Sur Oriental garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- La E.S.E. Hospital Regional Sur Oriental garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- La E.S.E. Hospital Regional Sur Oriental garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5 ROLES Y RESPONSABILIDADES

La política de seguridad de la información es de aplicación obligatoria para todo el talento humano de la entidad.

Gerente:

- Aprobar las políticas de seguridad de la información.
- Validar el proceso de gestión de Seguridad de la Información.
- Sancionar las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales, que se generen como resultado de los reportes o propuestas del Comité Institucional de Gestión y Desempeño.
- Facilitar los recursos requeridos para su ejecución.

Comité Institucional de Gestión y Desempeño: El Comité tendrá las siguientes funciones y responsabilidades en temas de Seguridad de la Información:

- Revisar y proponer al Gerente, para su aprobación, la Política de Seguridad de la Información.
- Supervisar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información.
- Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para implementar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas.
- Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones.
- Reportar a la Gerencia, respecto a oportunidades de mejora en materia de Seguridad de la Información, así como los incidentes relevantes y su solución.

Encargado de Seguridad de la Información Institucional. Es un servidor público nombrado por el Gerente como su asesor en materia de seguridad de la información. El Encargado de Seguridad de la Información tendrá las siguientes funciones y responsabilidades:

- Organizar las actividades del Comité Institucional de Gestión y Desempeño en materia de seguridad de la información.
- Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la entidad y el control de su implementación; y velar por su correcta aplicación.

- Supervisar el Monitoreo del avance general de la implementación de las estrategias de control y tratamiento de riesgos.
- Gestionar la coordinación con otras áreas de la entidad para apoyar los objetivos de seguridad.
- Hacer el enlace con los responsables de seguridad de otras entidades públicas y especialistas externos, con el fin de mantenerse actualizado acerca de las tendencias, normas y métodos de la seguridad de la Información.