POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

INTRODUCCION

El Hospital Regional De II Nivel de San Marcos- ESE, es una institución prestadora de servicios de salud con talento humano calificado, buscando el mejoramiento continuo de los procesos, para garantizar de esta manera servicios de calidad a la población de San Jorge, la Mojana y su área de influencia.

Por eso, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de una política de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

POLITICA DE SEGURIDAD DE LA INFORMACION

Para Hospital Regional de II Nivel de San Marcos- ESE, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- 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 Hospital Regional de II Nivel de San Marcos- ESE
- Garantizar la continuidad del negocio frente a incidentes.
- Hospital Regional de II Nivel de San Marcos- ESE 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.

El Hospital Regional de II Nivel de San Marcos- ESE, velara por la protección de la información buscando la manera de disminuir el impacto generado sobre sus activos, por consiguiente, los riesgos son identificados de manera sistemática con el objetivo de mantener un nivel mínimo de exposición que permita dar respuesta

por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

Definida la política de seguridad de la información esta será compartida, socializada, y publicada, haciendo uso de herramientas tecnológicas y canales de comunicación con los que cuenta la entidad, posterior se realizara seguimiento a la misma y teniendo en cuenta los parámetros de Gobierno Digital, se establecen las responsabilidades y el adecuado uso de la información frente a la seguridad de la política.

De esta manera se permite tener una interacción con los diferentes usuarios para trasmitir el conocimiento del impacto de la política y procesos para seguridad de la información ya que somos propenso a presentar cualquier posible falla o perdida de información. Todo esto se logra mitigar teniendo los mecanismo y herramientas necesarios para poder brindar seguridad a la información.

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.

FASES DE IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN

1. **Desarrollo de las políticas:** En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

   • Justificación de la creación de política: Debe identificarse el por qué la Entidad requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.

   • Revisión de la política: Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma.

   • Aprobación de la Política: Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de las mismas. Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas.

2. **Cumplimiento:** Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

3. **Comunicación:** Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los funcionarios contratistas y/o terceros de la entidad debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.

4. **Monitoreo:** Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos ejemplo indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

5. **Mantenimiento:** Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

6. **Retiro:** Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

ELABORACIÒN	REVISIÓN	APROBACIÓN
MIGUEL ANGEL RODRIGUEZ HERAZO Ingeniera Sistemas	**LIDIA CENAIDA PEREZ** Subgerente Administrativa y Financiera	**DUVER VARGAS ROJAS** Agente Especial Interventor
Fecha: 21/06/2021	Fecha: 21/06/2021	Fecha: 21/06/2021