PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CODIGO: GI PL 03	VERSIÓN: 5	FECHA DE EMISIÓN: 26/01/2022	Página 1 de 10

Cargos Involucrados:		Dueño del procedimiento:
TODO EL PERSONAL	Empresa Social del Estado HOSPITAL NUESTRA SEÑORA DEL PILAR de Medina Unidos por la Comunidad, con Humanización y Calidad.	GESTION INFORMACIÓN

	NOMBRE	CARGO	FIRMA
ELABORÓ	Sandra Yolima Rojas Reyes	Coordinadora Administrativa	
REVISÓ	Yenny Angélica Sánchez Clavijo	Jefe de Calidad	
APROBÓ	Lina Yinneth Vega Hidalgo	Gerente	

CONTROL DE CAMBIOS		
VERSION	**FECHA**	**NATURALEZA DEL CAMBIO**
1	01/01/2018	Creación del documento
2	01/01/2019	Vigencia 2019
3	25/01/2020	Vigencia 2020
4	29/01/2021	Vigencia 2021
5	26/01/2022	Vigencia 2022

Cargos Involucrados:		**Dueño del procedimiento:**
TODO EL PERSONAL	Empresa Social del Estado HOSPITAL NUESTRA SEÑORA DEL PILAR de Medina *Unidos por la Comunidad, con Humanización y Calidad.*	GESTION INFORMACIÓN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2022

CONTENIDO

1. INTRODUCCIÓN

La información es un activo de alto valor para cualquier entidad, pública o privada, es por esto que se hace necesario definir un sistema de gestión de seguridad de la información que permita garantizar la integridad, confidencialidad y disponibilidad de la información, contra las amenazas constantes y cada vez mayores.

Una vez identificado el estado actual de la entidad en materia de seguridad de la información y las necesidades de la institución en esta materia, la primera Tarea de cualquier sistema de gestión de seguridad de la información consiste en definir una política general de seguridad de la información, la cual resume el compromiso de la administración con la implementación de un sistema de gestión de seguridad de la información.

En este documento se define la política general de seguridad y privacidad de la información para el hospital nuestra señora del pilar, la cual se definió teniendo en cuenta el contexto particular de la institución y las necesidades y regulaciones en esta materia.

2. OBJETIVOS

Establecer los lineamientos que le permitan al Hospital Nuestra señora del Pilar de Medina, proteger la información y los sistemas de información ante cualquier amenaza que pueda comprometer la disponibilidad, integridad y confidencialidad de la información recolectada, procesada o almacenada por la entidad.

Fomentar en los funcionarios, usuarios y colaboradores de la entidad una cultura de seguridad de la información, que les permita tomar conciencia de sus deberes y responsabilidades frente a la gestión de seguridad de la información, así como de sus beneficios.

Minimizar los incidentes relacionados con seguridad de la información, que afecten el normal funcionamiento de la ESE Hospital Nuestra Señora del Pilar de Medina.

Desarrollar un sistema de gestión de riesgos de seguridad de la información que permita generar controles que ayuden a reducir los impactos negativos de los incidentes de seguridad.

3. ALCANCE.

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la ESE Hospital Nuestra Señora del Pilar de Medina.

4. DEFINICIONES.

Colaborador: Empleado, contratista, practicante, proveedor y en general cualquier persona que tenga acceso a información del Ministerio de Cultura y tenga un vínculo contractual con el mismo.

Criptografía: Arte o técnica de escribir con clave secreta o de un modo enigmático.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Procedimiento: Documento que describe la forma específica de llevar a cabo a una actividad o un proceso.

Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

Seguridad de la Información: Preservación de la confidencialidad, disponibilidad e integridad de la información (ISO/IEC 27000) independiente de su medio de conservación, transmisión o formato.

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).

5. MARCO NORMATIVO.

La política de seguridad de la información se encuentra regulada por las siguientes normas

Decreto 2573 de 2014 "Por el cual se establecen los lineamientos generales de la estrategia

de gobierno en línea"

Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales"

Ley 1915 de 2018 "Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos"

Norma Técnica colombiana ISO/IEC 27001 Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección del Hospital Nuestra Señora del Pilar de Medina, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión 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.

Para la E.S.E. Hospital Nuestra Señora del Pilar de Medina, 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 sistema de gestión de la seguridad de la información 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 usuarios, 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 usuarios de la E.S.E Hospital Nuestra Señora del Pilar de Medina.
- Garantizar la continuidad del negocio frente a incidentes.

A continuación, mencionamos las políticas específicas que soporten la declaración de la política general.

7. POLITICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1. Recursos tecnológicos.

El uso de los recursos tecnológicos con los que cuenta la entidad y que son asignados a funcionarios del hospital o a tercero estarán sujetos a las siguientes políticas.

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la E.S.E. Hospital Nuestra Señora de Pilar de Medina, es responsabilidad del área de tecnología, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por el hospital a través de esta área.

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, entre otros. Estos cambios pueden ser realizados únicamente por el área de TI del Hospital.

- Únicamente los funcionarios y terceros autorizados por el área de TI, previa solicitud por parte de la dependencia que lo requiera, pueden conectarse a la red inalámbrica del Hospital Nuestra señora del Pilar de Medina.

- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del Hospital, las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por el área de TI.

7.2 Seguridad del Recurso Humano.

Identificado como el eslabón más débil en la cadena de seguridad de la información se deben definir unas políticas particulares que permitan minimizar la ocurrencia de incidentes de seguridad de la información debidos a el recurso humano.

- La entidad debe asegurarse de que los funcionarios y colaboradores entienden sus responsabilidades y están capacitados para el desempeño de sus funciones.

- En los acuerdos contractuales se deben establecer las responsabilidades y obligaciones de los colaboradores para con la entidad en materia de seguridad de la información.

- Debe existir un compromiso de la dirección que exija a los colaboradores cumplir con las políticas en materia de seguridad de la información.

- Es importante desarrollar un plan de sensibilización de los funcionarios con respecto a las bondades de la implementación de un sistema de seguridad de la información, donde se muestren los lineamientos generales y los controles adoptados, pero se haga énfasis en los beneficios del SGSI y las consecuencias negativas de ignorar las responsabilidades en materia de seguridad de la información.

- Todos los funcionarios de la E.S.E. Hospital Nuestra Señora del Pilar de Medina y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

- Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos del Hospital a personas o entidades externas.

- Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos

7.3 Control de Acceso:

Se deben desarrollar políticas que permitan establecer los permisos de acceso a la información y a los sistemas encargados de su captura, procesamiento y almacenamiento, de tal forma que se establezca mantenga y actualice la información de permisos de acceso, su administración gestión y los procedimientos de otorgamiento y remoción de permisos.

7.3.A Se deben implementar mecanismos de autenticación acordes que permitan el acceso seguro a los sistemas y aplicaciones. Las credenciales de acceso son responsabilidad de los funcionarios, los cuales deben mantenerlas en secreto, deben ser de uso personal y exclusivo.

7.3.B Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información del Hospital sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

7.3.C El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información del hospital debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la Institución, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.