PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EMPRESA SOCIAL DEL ESTADO HOSPITAL LA DIVINA MISERICORDIA

VIGENCIA 2023

Aprobado por: _____ GERENTE	VERSIÓN: 0.1
	Vigente desde: 19/05/2023
	Código:

INTRODUCCIÓN

La Empresa Social Del Estado Hospital La Divina Misericordia con el fin de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha decidido realizar un plan de seguridad y privacidad de la información como consecuencia de la expedición del Decreto 612 del 2018, el cual fija directrices para la integración de los planes institucionales y estratégicos del plan de acción. Además se tuvo en cuenta el ámbito de aplicación del modelo Integrado de Planeación y Gestión y las directrices del plan de acción de que trata el artículo 74 de la Ley 1474 del 2011. Es así y razón por la cual se deben implementar, publicar y sobre todo integrar los planes que para tal fin se solicitan en el mencionado Decreto.

El presente plan se realizó para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL. Comprendiendo la adaptación de la política de seguridad y privacidad de la información, conformación del Comité de Seguridad de la Información y el desarrollo de controles de la Política de Seguridad de la Información. Lo anterior enmarcado además en los esfuerzos que la E.S.E. se enfoca en impulsar las tecnologías de la información y las comunicaciones, para garantizar una entidad con mayor y mejor interacción con la ciudadanía a través del uso adecuado de los recursos a su alcance.

De allí, que en la Empresa Social Del Estado Hospital La Divina Misericordia a través de su plan de seguridad y privacidad de la información, traza actividades que permitan mantener segura la información que se genera, fluye y preserva al interior de la entidad, garantizando la incorporación del gobierno en línea como parte de la cultura organizacional y elemento de soporte en sus actividades misionales.

TABLA DE CONTENIDO

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer las medidas, actividades y controles necesarios para adelantar la gestión de la seguridad y privacidad de la información (SPI) en la Empresa Social Del Estado Hospital La Divina Misericordia para asegurar la confidencialidad, integridad y disponibilidad de la información.

1.2. OBJETIVOS ESPECÍFICOS

- Administrar los riesgos de seguridad de la información.
- Sensibilizar a los servidores públicos y contratistas de la entidad acerca del sistema de gestión de seguridad de la información y el modelo de seguridad y privacidad de la información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la entidad.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico.
- 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 de gobierno digital.
- Asignar roles y responsabilidades para garantizar la seguridad y privacidad de la información.

2. ALCANCE Y NIVEL DE CUMPLIMIENTO

La gestión de la seguridad y privacidad de la información aplica a todos los procesos institucionales de la Empresa Social Del Estado Hospital La Divina Misericordia y demás partes interesadas que comparten, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de información, ya sea interna o externa, así como las actividades pertinentes que se consideren fundamentales para determinar la estrategia de implementación de los controles de seguridad requeridos para el adecuado funcionamiento del SGSI en la entidad.

Inicia con la definición del Plan de Seguridad y Privacidad de la Información, continua con la ejecución y finaliza con el seguimiento y evaluación de la gestión realizada.

Aplica a toda información creada, procesada o utilizada sin importar el medio, formato o presentación y lugar en el cual se encuentre.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a este plan. A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad de la información de la Empresa Social Del Estado Hospital La Divina Misericordia:

- 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 Empresa Social Del Estado Hospital La Divina Misericordia, protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.

- La Empresa Social Del Estado Hospital La Divina Misericordia, protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Empresa Social Del Estado Hospital La Divina Misericordia protege su información de las amenazas originadas por parte del personal.
- La Empresa Social Del Estado Hospital La Divina Misericordia protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Empresa Social Del Estado Hospital La Divina Misericordia, controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Empresa Social Del Estado Hospital La Divina Misericordia implementa controles de acceso a la información, sistemas y recursos de red.
- La Empresa Social Del Estado Hospital La Divina Misericordia garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Empresa Social Del Estado Hospital La Divina Misericordia garantiza 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 Empresa Social Del Estado Hospital La Divina Misericordia garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- La Empresa Social Del Estado Hospital La Divina Misericordia 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.

3. DEFINICIONES

Activos de información: Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensibles o críticos para el cumplimiento de los objetivos de la entidad.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

CIGD – Sigla Comité Institucional de Gestión y Desempeño Confidencialidad: Es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

Control: Medida que modifica y mitiga el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: Acceso a la información cuando se requiere, teniendo en cuenta la privacidad.

Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Incidente de seguridad de la información: Un incidente de seguridad de la Información está indicado por un único evento o una serie de eventos de Seguridad de la Información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la entidad y de amenazar la seguridad de la información.

Integridad: Es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el organismo.

MSPI: Modelo de seguridad y privacidad de la información.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

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 (impacto). (ISO/IEC 27000).

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Información: se refiere a un conjunto independiente de recursos de Información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

4. ROLES Y RESPONSABILIDADES

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.

Las funciones del comité de Seguridad de la Información son asumidas por el Comité Institucional de gestión y desempeño. Dentro de los roles y responsabilidades del comité de seguridad de la información se resaltan:

- Garantizar la existencia de una dirección y apoyo gerencial que soporte la administración y el desarrollo de iniciativas sobre seguridad y privacidad de la información, a través de compromisos y uso adecuado de los recursos en el organismo.

- Formular y mantener una política de seguridad y privacidad de la información que aplique a toda la organización conforme con lo dispuesto por la E.S.E.
- En todo caso, dicho comité o la mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a la dirección de la Empresa Social del Estado Hospital La Divina Misericordia, para su aprobación mediante resolución o acto jurídico correspondiente.

GRUPO DE APOYO A LA SEGURIDAD.

- Desarrollar, mantener y administrar operativa y técnicamente la seguridad y privacidad de la información.
- Materializar las medidas de largo, mediano y corto plazo que permitan el desarrollo efectivo, estratégico y armónico del plan trazado.

FUNCIONARIOS PÚBLICOS, CONTRATISTAS Y PARTICULARES CON ACCESO A INFORMACIÓN DE LA EMPRESA SOCIAL DEL ESTADO HOSPITAL LA DIVINA MISERICORDIA.

- Cumplir con todas las políticas de seguridad y privacidad adoptadas por la Empresa Social Del Estado Hospital La Divina Misericordia.
- Actualizarse en los temas propios de seguridad y privacidad de activos de la información aplicados en la Empresa Social Del Estado Hospital La Divina Misericordia.
- Todos los funcionarios de la E.S.E, contratistas y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la entidad, 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 de la E.S.E. a personas o entidades externas. Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso contractual, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hará parte integral de cada uno de los contratos.

LÍDERES DE PROCESOS

El rol de los líderes de procesos en la ejecución del plan de revisión y seguimiento al SGSI, es fundamental dado que es el responsable de:

- Seguimiento a la ejecución de los planes de tratamiento de riesgos en seguridad de la información.
- Actualización de activos de información
- Revisión y cumplimiento de los procedimientos, controles y políticas del SGSI.

5. CUMPLIMIENTO

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, la Empresa Social Del Estado Hospital La Divina Misericordia, se reserva el derecho de tomar las medidas correspondientes.

6. PLAN DE IMPLEMENTACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de implementación de Seguridad y Privacidad de la Información de la Empresa Social Del Estado Hospital La Divina Misericordia tiene como propósito definir las actividades para la operación, evaluación y mejora de la Seguridad y Privacidad de la Información (SPI) con énfasis en la gestión de activos de información, riesgos, toma de conciencia, protección de datos y seguridad digital institucional. El seguimiento de la gestión del Plan SPI 2023 se presenta periódicamente al Comité Institucional de Gestión y Desempeño y se documenta según los productos definidos. A continuación, se presenta la programación de actividades que conforman el Plan de seguridad y privacidad de la información:

EJE	ACTIVIDAD	ENTREGABLE	CRONOGRAMA		RESPONSABLES
Diagnóstico MSPI	Realizar la aplicaciòn de la Matriz del MPSI	Matriz diagnóstico diligenciada	23/05/2023	14/07/2023	Gestión TICs
Política general de seguridad de la información	Diseñar y aprobar la Política de Seguridad de la información	Política de Seguridad de la Información Adoptada.	14/06/2023	20/07/2023	Alta Dirección Gestión TICs
Manual de seguridad de la información	Diseñar y aprobar el manual de Seguridad de la Información	Manual de Seguridad de la Información Adoptado.	21/07/2023	20/08/2023	Gestión Tics
Estrategia de Seguridad Digital	Diseñar y aprobar la Estrategia de Seguridad Digital	Estrategia de Seguridad Digital Adoptada	20/08/2023	02/09/2023	Gestión Tics
Gestión de activos de Información	Validar, verificar, actualizar y aprobar el inventario de activos de Información.	Matriz de activos actualizada y aprobada	23/05/2023	10/10/2023	Gestión Tics Lideres de procesos
	Verificar, actualizar y aprobar el inventario de activos críticos, infraestructuras críticas y servicios esenciales.				

Gestión de vulnerabilidades	Definir lineamientos para ejecutar las pruebas de vulnerabilidades	Documentación gestión de vulnerabilidades y resultados de pruebas de vulnerabilidades	23/05/2023	29/12/2023	Gestión Tics
	Ejecución de pruebas de seguridad (análisis de vulnerabilidades) al menos una vez al año.				
	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades				
	Realizar seguimiento al cierre de vulnerabilidad técnicas de acuerdo con su nivel de criticidad				
	Verificar la ejecución del re- test de pruebas de seguridad				
	Documentar las actualizaciones cuando ocurra un cambio importante en los activos de información producto del retest.				
Indicadores de seguridad de la información	Revisar, ajustar o formular, implementar y medir los indicadores del SGSI	Matriz con indicadores actualizados según periodicidad e informe del cumplimiento de las acciones correctivas en caso de que aplique	23/05/2023	29/12/2023	Gestión Tics

Gestión de riesgos	Realizar la identificación, análisis y evaluación de riesgos de los activos de información	Matriz con la evaluación de riesgos incluidos los riesgos de los activos de información y seguridad digital.	01/06/2023	15/11/2023	Gestión Tics Lideres de procesos
	Realizar la identificación, análisis y evaluación de riesgos de los activos críticos, infraestructura crítica y servicios esenciales (entorno digital)				
	Realizar seguimiento trimestral al Mapa o Plan de Tratamiento de Riesgos	Mapa o Plan de Tratamiento de Riesgos actualizado con soportes	23/05/2023	31/12/2023	
	Realizar valoración trimestral del riesgo residual para establecer las variaciones y/o ajustes de cada periodo cuando corresponda				
	Como parte del seguimiento se realiza la revisión y preparación de evidencias que respaldan la ejecución de las actividades de control establecidas en el Plan de Tratamiento de Riesgos				

Plan de comunicación, socialización y sensibilización	Elaborar y ejecutar el Plan de comunicación en temas relacionados con la seguridad de la información como complemento al PIC (Plan Institucional de Capacitación)	Plan de Sensibilización y toma de conciencia en temas relacionados con seguridad de la Información y Seguridad Digital	23/05/2023	29/12/2023	Alta Dirección Gestión TICs
	Desarrollar un Plan de sensibilización y toma de conciencia sobre ciberseguridad para ejercer control y protección sobre los entornos digitales				
	Realizar mínimo 2 sesiones de sensibilización en seguridad de la información en las jornadas de inducción y reinducción				

7. COMUNICACIÓN

Mediante socialización a todos los funcionarios de la Empresa Social del Estado Hospital La Divina Misericordia se dará a conocer el contenido del documento Plan de seguridad y privacidad de la información, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo a las acciones plasmadas en el plan de trabajo. Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad https://esehospitalladivinamisericordia.gov.co/ Menú “Transparencia”

8. MONITOREO

Se crearán los mecanismos y los indicadores correspondientes al Plan de seguridad y privacidad de la información con el fin de determinar el cumplimiento del mismo para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

9. NORMOGRAMA

Ley 909 de 2004: “Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones”.

Ley 1581 de 2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”.

Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

Decreto Ministerial 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Decreto Presidencial 1083 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública".

Decreto Presidencial 612 de 2018: "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".

Decreto Presidencial 767 de 2022: "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Resolución Ministerial 00500 de 2021: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital".

Original firmado

Joe Rafael Cohen Medina
Gerente