PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2020 - 2023

RED DE SALUD DEL CENTRO

Empresa Social del Estado

Nivel I

Santiago de Cali, Enero de 2020

RED DE SALUD CENTRO ESE.
Sede Administrativa - IPS Diego Lalinde - Cra. 12E # 50-18 B / Villa Colombia. Cali - Valle
PBX: 4851717 - 441 1914 fax 4411518 Ext. 16
E-mail: ese.centro@saludcentro.gov.co - atencion.usuario@saludcentro.gov.co
Nit. 805.027.261 - 3

TABLA DE CONTENIDO

INTRODUCCIÓN 3
OBJETIVO 3
ALCANCE 3
JUSTIFICACIÓN 3
CICLO DE OPERACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4
Fase previa de diagnóstico del plan de seguridad y privacidad de la información 4
FASE DE PLANEACIÓN 4
Alcance del plan de seguridad y privacidad de la información 5
Gobierno de la seguridad y privacidad de la información 5
Política general de seguridad y privacidad de la información 6
Objetivos de seguridad y privacidad de la información 7
Compromiso de la Alta Dirección 7
FASE DE IMPLEMENTACIÓN 8
FASE DE EVALUACIÓN DEL DESEMPEÑO 10
Seguimiento y Medición 10
FASE DE MEJORA DEL SGSI 11

INTRODUCCIÓN

La información es el activo más importante y relevante para las organizaciones, así como aquellos que soportan y recurso indispensable para el desarrollo y cumplimiento misional junto con los compromisos del negocio; ésta puede llegar a ser sensible o crítica y por lo tanto requiere de una evaluación para determinar su nivel de protección necesario para mitigar o evitar posibles situaciones de riesgo e impacto asociado a la pérdida de su disponibilidad, integridad o confidencialidad.

En atención a las situaciones de riesgo expuestas anteriormente, se genera entonces por parte de la gerencia de la ESE CENTRO, la iniciativa de establecer, implementar y mantener un Plan de Seguridad y Privacidad de la Información enfocado en alcanzar y mantener una cultura y conciencia en el acceso y uso adecuado de la información en la institución.

El presente documento identifica y recopila buenas prácticas para la gestión del ciclo de operación del Plan de Seguridad y Privacidad de la Información, a partir de una evaluación de diagnóstico, planeación, implementación, gestión y mejora continua del mismo.

OBJETIVO

Presentar el plan de seguridad y privacidad de la información de la ESE CENTRO y los elementos que lo conforman, como marco de referencia para el establecimiento y regulación de lineamientos y medidas que permitan el aseguramiento de la protección y uso adecuado de la información y activos de información que la soportan al interior de la Institución.

ALCANCE

El presente documento identifica e incluye las orientaciones para la gestión del ciclo de operación del Plan de Seguridad y Privacidad de la Información, el cual debe ser aplicado sobre todos los procesos de la ESE CENTRO y de cumplimiento por parte de todos los colaboradores con relación contractual.

JUSTIFICACIÓN

El presente plan de seguridad de la información se define en cumplimiento a sus propósito y obligaciones internos como sectoriales en cuanto a la contribución a la

construcción de un estado más eficiente, transparente y participativo a través de la definición del plan de seguridad y privacidad de la información, al igual que a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de Gobierno Digital.

CICLO DE OPERACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la etapa inicial de los propósitos de diseño del sistema de gestión de seguridad de la información, se identificó la necesidad de definir las 5 fases que orientarían el ejercicio para los propósitos de protección de la información de la Institución bajo un modelo sostenible:

1. FASE PREVIA DE DIAGNOSTICO
2. FASE DE PLANEACIÓN
3. FASE DE IMPLEMENTACIÓN
4. FASE DE EVALUACIÓN DEL DESEMPEÑO
5. FASE DE MEJORA

Fase previa de diagnóstico del plan de seguridad y privacidad de la información

En esta fase y mediante el uso de herramientas de diagnóstico, se desarrollan actividades de reconocimiento y valoración del estado de gestión, cumplimento de requisitos y lineamientos de seguridad de la información, y de la implementación de controles de seguridad de la información con visión de mitigar todo tipo de escenario de riesgo asociado que pudiese generar un impacto indeseado a la Institución.

El resultado de la evaluación de diagnóstico permitirá establecer el nivel de madurez del ciclo de operación del Plan de Seguridad y Privacidad de la Información en la ESE CENTRO, y el mapa de ruta para las actividades claves de las fases de diseño y establecimiento del mismo modelo.

FASE DE PLANEACIÓN

Para el desarrollo de esta fase y basado con el resultado de la evaluación de diagnóstico y el análisis de contexto de la ESE CENTRO, se identificarán los aspectos claves que definan y orienten las actividades para los propósitos de

seguridad y privacidad de la información, entre ellos, la justificación, el alcance, la política y los objetivos del Plan de Seguridad y Privacidad de la Información.

Alcance del plan de seguridad y privacidad de la información

El plan de seguridad y privacidad de la información y lineamientos asociados como directriz de la gerencia de la ESE CENTRO, será de aplicabilidad e implementación para todos los procesos y aspectos administrativos de la institución y, de cumplimiento por parte de todos aquellos colaboradores y terceros que presten sus servicios o tengan algún tipo de relación con la Institución.

El alcance del plan de seguridad y privacidad de la información permitirá a la ESE CENTRO definir los límites sobre los cuales se implementará la seguridad y privacidad de la información, por tanto, deberá tener en cuenta, los procesos que impactan directamente la consecución de los objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados e interrelaciones del plan de seguridad y privacidad de la información con otros procesos.

Gobierno de la seguridad y privacidad de la información

El modelo de gobierno de la seguridad de la información se presentará a través de una estructura de directrices y lineamientos por niveles de acuerdo con el propósito de cada uno de ellos.

La estructura de directrices y lineamientos de seguridad de la información se define de la siguiente manera:

a. Política general de seguridad de la información: Documento de alto nivel que denota compromiso de la alta dirección con respecto a seguridad de la información; define reglas de comportamiento asociado a protección de activos de información.
b. Políticas Tácticas de seguridad de la información: Son exigencias particulares de apoyo a la política estratégica, manifiestan la manera en que se va a ejecutar a conseguir tienen propósito especial, es de estricto cumplimiento, que soportan los propósitos principales de la política estratégica del SGSI.
c. Normas y estándares de seguridad de la información: Todas aquellas reglas específicas orientadas para respaldar el cumplimiento de las políticas de gestión tecnológica.

Soporte Documental: Todo documento generado para dirigir y orientar la gestión de la seguridad de la información; permitirá compartir a los servidores públicos comprender los propósitos de seguridad de la información, las directrices y lineamientos relacionados con seguridad de la información.

Toda la documentación asociada al sistema de gestión de seguridad de la información deberá ser revisada y actualizada (en la medida que aplique) bajo un estricto control de cambios para asegurar la integridad de los contenidos.

Política general de seguridad y privacidad de la información

La política de seguridad de información es la declaración general que representa la posición de la ESE CENTRO frente a la necesidad de protección de su información, al igual que de la preservación de aquellos activos de información que la soportan, por tal motivo define que:

La ESE CENTRO reconoce el valor de su información como uno de sus activos más valiosos y es consciente de la necesidad de su custodia, conservación, disponibilidad, integridad, accesibilidad y confidencialidad en los casos que corresponda, generando una cultura de protección y uso adecuado a través de la implementación y mejora continua de un sistema de gestión de seguridad de la información, con un enfoque de administración y tratamiento de riesgos asociados y el cumplimiento de todos los requisitos propios de su actividad, legales, reglamentarios y contractuales, que permitan asegurar la confianza de las partes interesadas.

Objetivos de seguridad y privacidad de la información

En beneficio del apoyo y cumplimiento de los propósitos de la política estratégica de seguridad de la información en la ESE CENTRO, se declaran los siguientes objetivos generales:

- Establecer las directrices y lineamientos relativos a seguridad de la información.
- Generar una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la información por parte de los servidores públicos.
- Implementar mecanismos de control para la protección de los datos, la información y los recursos asociados que los soportan.
- Asegurar que los riesgos asociados a seguridad de la información se mantienen en un nivel aceptable.
- Mantener un enfoque de cumplimiento estricto de los requisitos legales, normativos o contractuales aplicables y relativos al tratamiento y protección de la información.

Compromiso de la Alta Dirección

La gerencia de la ESE CENTRO aprueba la política general de seguridad de la información como muestra de su compromiso y apoyo a las actividades de diseño, implementación, mantenimiento y mejora continua de políticas y lineamientos consecuentemente orientados a la salvaguardar la confidencialidad, integridad y disponibilidad de la información de la Institución.

Su compromiso se demostrará a través de:

- La revisión y aprobación de políticas y lineamientos de seguridad de la información.
- La promoción de una cultura de seguridad y protección de la información.
- El apoyo para la divulgación de los propósitos y lineamientos de seguridad de la información a los servidores públicos y partes interesadas.
- La asignación de los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información.
- La realización de actividades de verificación y evaluación del desempeño del sistema de gestión de seguridad de la información de manera periódica.

FASE DE IMPLEMENTACIÓN

El Plan de Seguridad y Privacidad de la Información permitirá a la ESE CENTRO llevar a cabo la implementación de los aspectos y requisitos presentados tanto por el Plan de Seguridad y Privacidad de la Información, como los presentados por la norma ISO/IEC 27001:2013; de igual manera, la implementación de los controles de seguridad de la información, que por normativa o por resultado de la valoración de riesgos deban ser implementados.

El plan de control operacional establecerá las actividades y la programación para la implementación tanto de los requisitos, controles y buenas prácticas de seguridad y privacidad de la información en la ESE CENTRO.

Como estrategia interna para la orientación de los propósitos de seguridad y privacidad de la información, se definen e implementan políticas y directrices que guíen las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad.

Actividad	Descripción	Evidencia de Actividad
Realizar reconocimiento del contexto de la ESE CENTRO (cuestiones internas y externas) con propósito de orientar el SGSI como apoyo a la estrategia gerencial.	Definir los escenarios para los cuales el Plan de Seguridad y Privacidad de la Información será soporte a la estrategia definida por la Gerencia de la ESE CENTRO.	Documento con la identificación de las cuestiones internas y externas de la ESE CENTRO
Reconocer las partes interesadas de la ESE CENTRO e identificar sus necesidades y expectativas con respecto a seguridad de la información	Reconocer las necesidades y expectativas de seguridad de la información por cada una de las partes interesadas de la ESE CENTRO, que permitan orientar esfuerzos de cumplimiento para cada una de ellas.	Documento con la identificación de las partes interesadas, sus necesidades y expectativas pertinentes a la seguridad de información
Definir el alcance, políticas y objetivos del plan de seguridad y privacidad de la información.	Definir el alcance y los límites bajo los servicios, procesos o actividades propias de la ESE CENTRO sobre el cual se implementará el Plan de Seguridad y Privacidad de la Información.	Documento con la identificación del alcance y límites, política y objetivos del plan de seguridad y privacidad de la información

Actividad	Descripción	Evidencia de Actividad
Definir la estructura de roles y responsabilidades para la gestión de los propósitos del plan de seguridad y privacidad de la información y de las fases definidas	Definir y asignar formalmente la autoridad, roles y responsabilidades para la gestión y propósitos del modelo de seguridad y privacidad de información.	Documento con la identificación y asignación de roles y responsabilidades
Realizar la valoración y tratamiento de los riesgos de seguridad de la información.	Definir la estrategia para identificar, estimar, evaluar y tratar los riesgos asociados a la seguridad de la información en la ESE CENTRO.	Metodología para la valoración y tratamiento de los riesgos de seguridad de la información
Definir el modelo y esquema de gestión de políticas y directrices de seguridad de la información.	Documentar el esquema de políticas y lineamientos de seguridad de la información en apoyo al cumplimiento de la política general de seguridad de la información de la ESE CENTRO.	Manual de políticas y lineamientos de seguridad de la información
Ejecutar el plan de valoración y tratamiento de los riesgos de seguridad de la información	A través de la identificación del inventario de activos de información por procesos, identificar los riesgos de seguridad de la información asociados a los mismos y aplicar la mejor estrategia de tratamiento con propósito de obtener niveles de riesgo residuales aceptables.	Inventario de activos de información Mapa de riesgos de seguridad de la información
Realizar actividades de sensibilización y toma de conciencia de seguridad y privacidad de la información	Ejecución de plan de sensibilización y toma de conciencia de aspectos de seguridad de la información.	Plan de comunicación y resultados de actividades de seguimiento al cumplimiento

Actividad	Descripción	Evidencia de Actividad
Definir e implementar los controles de seguridad de la información	Implementar las estrategias de mitigación de riesgos de seguridad de la información de acuerdo con resultado de valoración de riesgos y a los requisitos del Plan de Seguridad y Privacidad de la Información.	Plan de tratamiento de riesgos

FASE DE EVALUACIÓN DEL DESEMPEÑO

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

Seguimiento y Medición

Para las actividades de seguimiento y medición, la ESE CENTRO definirá procedimientos que permitan:

- Definir y orientar actividades para la identificación de situaciones de eventos o incidentes de seguridad y privacidad de la información.
- Definir los esquemas de atención a los eventos e incidentes de seguridad de la información, en beneficio de prevenir y mitigar escenarios de impacto a la Institución.
- Emprender revisiones regulares de la eficacia del plan de seguridad y privacidad de la información (que incluyen el cumplir de la política de seguridad de la información, los objetivos, los controles) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugeridas y la retroalimentación de las partes interesadas.
- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Revisar las valoraciones de riesgos de manera regular, asegurando que los niveles de riesgos residuales son comprendidos y aceptados.
- Realizar ejercicios de auditoría interna del plan de seguridad y privacidad de la información.
- Realizar actividades de revisión del plan de seguridad y privacidad de la información por parte de la gerencia de la ESE CENTRO.

Actividad	Descripción	Evidencia de Actividad
Definir y ejecutar el plan de evaluación de desempeño del Plan de Seguridad y Privacidad de la Información.	La estrategia de evaluación de desempeño establecerá el alcance y escenarios sobre los cuales se realizará seguimientos y mediciones (ejemplo, requisitos de seguridad, estados de valoración de riesgos, implementación de planes de tratamiento, etc.), los métodos elegidos, la frecuencia y los responsables de su ejecución.	Documento con la identificación de la estrategia de evaluación de desempeño y criterios (seguimiento, medición, análisis y evaluación)
Definir y aprobar el programa de auditoría interna del Plan de Seguridad y Privacidad de la Información.	El programa de auditoría identificará la(s) auditoría(s) que serán realizadas para evaluar el Plan de Seguridad y Privacidad de la Información, al igual que el cronograma para su ejecución.	Documento con la identificación del programa de auditoría
Realizar la revisión del estado del Plan de Seguridad y Privacidad de la Información por parte de la alta dirección.	Recolectar las fuentes de información de aspectos del estado de operación del Plan de Seguridad y Privacidad de la Información para presentarlas ante la alta dirección.	Plan de revisión por la dirección Informe de resultados de la revisión por la dirección.

FASE DE MEJORA DEL SGSI

La Institución con la visión de mantenimiento y mejora de los aspectos de seguridad de la información, tomará en cuenta los resultados de la fase III “Evaluación de desempeño” la cual está basada en los resultados de las actividades de seguimiento y medición (indicadores).

La ESE CENTRO:

- Implementará las mejoras identificadas en el plan de seguridad y privacidad de la información
- Identificará e implementará acciones correctivas y preventivas que mitiguen situaciones de impacto.

- Implementará acciones de mejora basadas en las lecciones aprendidas de las experiencias de seguridad internas o de otras compañías.
- Asegurar que las mejoras cumplen con los objetivos y propósitos definidos por la ESE CENTRO.

Actividad	Descripción	Evidencia de Actividad
Identificar, definir y activar planes de mejoramiento del plan de seguridad y privacidad de la información	Los resultados y conclusiones de las actividades de evaluación de desempeño del plan de seguridad y privacidad de la información permitirán identificar los escenarios sobre los cuales se podrán adoptar acciones correctivas o mejoras.	Plan de mejoramiento del plan de seguridad y privacidad de la información