PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

E.S.E CENTRO DE SALUD SANTA BÁRBARA

CLAUDIA NAYIBE CACERES BAEZ
GERENTE

VIGENCIA FISCAL 2024

CONTENIDO

INTRODUCCIÓN

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad del negocio. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en la Ese Centro de Salud Santa Bárbara.

Se realiza la identificación, el análisis, la evaluación de los riesgos, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo a través de él plan de tratamiento de riesgos. La necesidad de crear un plan de seguridad y tratamiento de riesgos enfocados a la información, es de vital importancia, hoy día uno de los activos más importantes en toda institución es la información, y es por ello que se deben tener barreras de seguridad y controles en la administración y tratamiento de la misma.

1. OBJETIVOS

1.1 Objetivo General

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la Ese Centro de Salud Santa Bárbara.

1.2 Objetivos Específicos

- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.
- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos a proteger en la Institución.
- Identificar las principales amenazas que afectan a los activos.

2. ALCANCE

El plan de tratamiento de riesgo y seguridad de la información, aplica a todos los procesos que se desarrollan, procesen e interactúen en la E.S.E.

3. TERMINOS Y DEFINICIONES

Los términos y definiciones aplicables para la identificación de riesgos de Seguridad de la Información se basan en la Norma NTC-ISO/IEC 27000, Norma NTC-ISO/IEC 27005, Norma NTC-ISO/IEC 31000, Guía GTC 137 (ISO Guía 73:2009 - Vocabulario de Gestión de Riesgos), GTC ISO 27035:

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Activo: Cualquier cosa que tiene valor para la organización. La norma ISO/IEC 27000, define los siguientes tipos de activos:
- información;
- software, como programas informáticos;
- físico, como computadores;
- servicios;
- personas, y sus calificaciones, habilidades y experiencia; e
- intangibles, como reputación e imagen.

Activo de información: Conocimiento o información que tiene valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo con base en su probabilidad e impacto de ocurrencia.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones.

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. Control es también utilizado como sinónimo de salvaguarda o contramedida. También se puede definir como una medida que modifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma técnica NTCISO/IEC 27001:2013.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona/entidad autorizada. La información debe estar en el momento y en el formato que se requiera, al igual que los recursos necesarios para su uso. La no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante los usuarios de la E.S.E.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de Seguridad de la Información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de incidentes de Seguridad de la Información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros, como pérdida de reputación o implicaciones legales.

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Incidente de seguridad de la información: Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La información de la E.S.E. debe ser con calidad, clara y completa, y solo podrá ser modificada por el personal expresamente autorizado para ello. La falta de integridad de la información puede exponer a la Entidad a toma de decisiones incorrectas, lo cual puede tener impacto reputacional, financiero y/o legal.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de Seguridad de la Información inaceptables e implantar los controles necesarios para proteger la información.

Probabilidad: Medida para estimar la ocurrencia del riesgo.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado.

Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados.

Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de

seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación.

Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

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

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información

Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Riesgo inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Selección de controles: Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizacional, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer la política y los objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. MARCO NORMATIVO

Marco Normativo	Año	Descripción
Políticas técnicas de seguridad de la información Función Pública	2020	La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades
Decreto 103 de 2015,	2019	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1494 de 2015	2019	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014;	2018	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto 2573 de 2014	2018	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 1377 de 2013	2018	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2609 de 2012.	2017	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Ley estatutaria 1581 de 2012,	2017	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley 1474 de 2011	2017	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011	2017	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Ley 1273 de 2009,	2016	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 527 de 1999	2015	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Constitución Política de Colombia1991 - Artículo 15	2015	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
Ley 23 de 1982	2015	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
Norma técnica colombiana NTC - ISO/IEC 27001	2013	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.

5. TRATAMIENTO DE RIESGOS

5.1 Definición de Riesgos

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la “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”. De igual manera, el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información de la ESE Santa Bárbara.

De acuerdo a lo anterior, la política de tratamiento de datos personales Institucional y nacional la ESE Santa Bárbara busca diseñar una metodología enfocada en la identificación, gestión y tratamiento de los riesgos de seguridad y privacidad de la información.

5.2 Identificación del riesgo

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía

hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

5.3 Factores de riesgo

Para la vigencia 2024 se priorizan los siguientes factores de riesgo digital en nuestro plan de tratamiento de riesgos:

- Nivel de conocimiento del personal en amenazas digitales, políticas y controles de seguridad
- Disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura
- Identificación y protección de los datos de carácter personal
- Adecuada clasificación de la información bajo custodia de la Entidad de acuerdo con el marco legal vigente
- Entorno global digital inseguro
- Segregación apropiada de roles y privilegios en todos los sistemas de información

5.4 Valoración del riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos con el fin de obtener información para establecer su nivel y las posibles acciones a implementar.

Dicho análisis incluye las fuentes, así como los factores que generan las consecuencias y aumentan la probabilidad de que ocurran. En la etapa de análisis se identifican los controles existentes ya sean administrativos, técnicos y/o procedimientos implementados en la entidad.

NIVELES DE PROBABILIDAD		DESCRIPCIÓN
5	MUY ALTA	Riesgo cuya materialización es recurrente (Casi seguro).
4	ALTA	Riesgo que puede materializarse de manera habitual (Probable).
3	MODERADA	Riesgo que se presenta de forma casual o accidental (Posible).
2	BAJA	Riesgo que puede presentarse de manera eventual (Raro).
1	MUY BAJA	Riesgo cuya probabilidad de materializarse es mínima (Improbable).

5.5. Impacto.

La valoración del impacto que puede ocasionar a la E.S.E. la materialización de los Riesgos de Seguridad y Privacidad de la Información, se representa con la descripción de los siguientes niveles:

Muy Bajo: Afecta a una actividad del proceso.

Bajo: Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso

Moderado: Afecta un conjunto de datos personales o el proceso.

Alto: Afecta varios conjuntos de datos personales o procesos de la organización.

Muy Alto: Afecta toda la organización.

Multas por incumplimiento de la Legislación. Suspensión de las actividades misionales de la organización.

Esta valoración se realiza sobre los principios de la Seguridad de la Información:

Confidencialidad: Mide el impacto que tendría para la pérdida de confidencialidad sobre los activos de información, es decir, que sean conocidos por personas no autorizadas.

Integridad: Mide el impacto que tendría la pérdida de integridad, es decir, si la exactitud y estado completo de los activos de información o sus métodos de procesamiento fueran alterados.

Disponibilidad: Mide el impacto que tendría la pérdida de disponibilidad, es decir, si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran.

5.6 Estrategia de tratamiento de riesgo

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones:

• **Transferir:** Son procedimientos que permiten eliminar el riesgo por medio de la transferencia.

• **Mitigar:** Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.

• **Evitar:** Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.

• **Aceptar:** consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

La estrategia de control de riesgos para la vigencia 2024, contempla cuatro ejes que son: conocimiento, continuidad, control de acceso y controles tecnológico.

Estrategias de control de riesgos 2024	
Conocimiento	Habeas Data- Ley de protección de datos personales
	Transparencia y acceso a la información
	Amanezas Informáticas
	Políticas de seguridad de la información
Continuidad	Servicios esenciales
	Anticipación de eventos de riesgos
Control de Acceso	Inventario de activos de información
	Confidencialidad de la información
Controles tecnológicos	Seguridad de la información en la nube
	Detección de eventos
	Copias de respaldos de la información
	Uso de contraseñas con niveles bajos de seguridad.