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

E.S.E SANTA BÁRBARA

CLAUDIA NAYIBE CACERES BAEZ
GERENTE

VIGENCIA FISCAL 2022

INTRODUCCIÓN

La norma ISO 27005:2011 es un estándar internacional diseñado para la gestión del riesgo en la seguridad de la información dentro de un sistema de gestión de seguridad de la información.

Contiene procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera. 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 el plan de tratamiento de riesgo seguridad y privacidad de la información, que permita minimizar la pérdida total o parcial de la información en la ESE Santa Bárbara.

1.2 Objetivos Específicos.

- Identificar la ubicación y propietarios de los activos de información a través del inventario del mismo.
- Categorizar y valorar los activos de información.
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.

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. 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 NTC-ISO/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.

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

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.

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.

Seguridad de la Información: Preservación de los principios de confidencialidad, la integridad y la disponibilidad de la información.

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

Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.

Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública.

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública.

Ley 57 de 1985 -Publicidad de los actos y documentos oficiales.

Ley 594 de 2000 - Ley General de Archivos.

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad.

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.

Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

Decreto 2364 de 2012 - Firma electrónica.

Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos.

Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales.

Ley 527 de 1999 - Ley de Comercio Electrónico.

Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos trámites innecesarios existentes en la Administración Pública.

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Ley Estatutaria 1581 de 2012 - Protección de datos personales.

Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.

5. DESCRIPCIÓN DEL PLAN

5.1 Definición de Riesgo.

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 Riesgos de Ciberseguridad.

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dada su naturaleza dinámica incluye también aspectos relacionados con el entorno físico. Estos riesgos tienen una relación directa con los principios de la Seguridad de la Información y se clasifican teniendo en cuenta los siguientes grupos:

- ✓ Pérdida de la Confidencialidad: Pérdida de la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.

- ✓ Pérdida de la Integridad: Pérdida de la propiedad de contar con información exacta y completa, o que pudo haber sido sin ser manipulada o alterada por personas o procesos no autorizados.

- ✓ Pérdida de la Disponibilidad: Pérdida de la cualidad o condición de la información de encontrarse a disposición de quienes requieran acceder a ella, ya sean personas, procesos o aplicaciones.

5.3 Riesgos de Seguridad y Privacidad de la Información.

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.
De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como “Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y vulnerar la seguridad”; por consiguiente, se representarían en Riesgos de Seguridad y Privacidad de la Información, como lo es el riesgo de tener un uso no adecuado de la información personal, lo que repercute en una violación de los derechos constitucionales.

6. MÉTODOLOGIA DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Para lograr determinar una metodología de identificación, análisis y valoración del riesgo en la E.S.E. se toma como base la guía para la administración del riesgo del DAFP, determinado de esta manera las clases de riesgo, administración, seguimiento y control.

6.1 identificación y clases de riesgos.

Según el DAFP El riesgo está vinculado con todo el que hacer, y no solo se debe tener en cuenta el riesgo de carácter económico, entre las clases de riesgo que pueden presentarse están:

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, de la articulación entre dependencias.

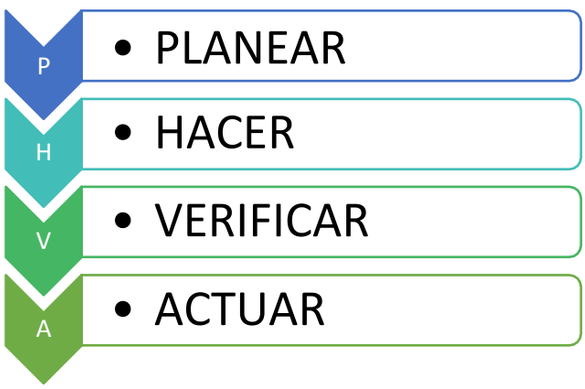
Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

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.

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.

Para llevar a cabo la implementación del plan de tratamiento de seguridad y privacidad de la información se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, que a su vez se están, basados en los lineamientos, y decretos del DAFP.

De acuerdo a lo anterior se definen las fases de implementación del plan de tratamiento de riesgos y seguridad de la información:



Para dar inicio a la etapa de diagnóstico es necesario identificar a los líderes del proceso sobre el cual se vaya a realizar el análisis de riesgos, quienes son definidos por los responsables de la información con base en la oficina o dependencia productora, quienes a su vez son los responsables del tratamiento de los riesgos de seguridad identificados.

Una vez identificados los líderes de procesos, con el acompañamiento de la oficina de sistemas realizaran la identificación de riesgos de Seguridad de la Información, los cuales contienen las siguientes secciones:

1. Información del proceso
2. Identificación del riesgo
3. Análisis del riesgo
4. Evaluación de controles
5. Plan de tratamiento de los riesgos.

Los riesgos se miden en términos de su impacto y de su probabilidad de ocurrencia de la siguiente forma:

PROBABILIDAD / IMPACTO	VALOR
MUY ALTO	5

ALTO	4
MODERADO	3
BAJO	2
MUY BAJO	1

6.2 Criterios para la valoración de riesgos.

Para la valoración de riesgos se toman como base dos variables: la probabilidad de ocurrencia del riesgo y su impacto en caso de que se materialice.

6.3 Probabilidad de ocurrencia.

Se define la probabilidad de ocurrencia para cada riesgo teniendo en cuenta los siguientes criterios de valoración:

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).

6.4 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.

Valoración de los riesgos.

Con base en la probabilidad y la valoración del impacto de cada riesgo, se establecen los niveles de riesgos (tanto los inherentes como los residuales luego de aplicar los controles identificados) teniendo una clasificación propia para la E.S.E.

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
Riesgo extremo	**>= 16**	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad, reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa o compartir y/o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	**>12 y <16**	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado o compartir y/o transferir el riesgo.

Riesgo Moderado	**>4 y < o = 11**	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor o compartir el riesgo.
Riesgo Bajo	**<= 3**	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.

7. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN.

El monitoreo anual o en el momento que se determine, debe estar a cargo de los responsables de los procesos con el apoyo del área de Control Interno y de Sistemas, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo de losriesgos de Seguridad y Privacidad de la Información.