Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Enero 2023

2023 - 2024

Contenido

1. INTRODUCCIÓN

El presente documento define las medidas de seguridad identificadas para desarrollar e implementar el plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital en la FLA EICE.

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos, evitando aquellas situaciones que impidan el logro de los objetivos de la empresa.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes y se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados.

Las anteriores medidas se definieron teniendo en cuenta la información del análisis de riesgos, el cual brindó información acerca de las necesidades del Proceso TIC en cuanto a la seguridad de la información y proporcionó las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

2. DEFINICIONES

- ✓ **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

- ✓ **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- ✓ **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

- ✓ **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- ✓ **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

- ✓ **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

3. OBJETIVOS

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital y de esta manera alcanzar los objetivos, la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

- Gestionar riesgos de Seguridad y Privacidad de la información y Seguridad Digital de la Operación, de acuerdo con los contextos establecidos en la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información y Seguridad Digital.

4. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información y Seguridad Digital, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

5. METODOLOGÍA

5.1. DESARROLLO METODOLÓGICO

- **Fase 1: Análisis de la información**

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas).
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

- **Fase 2: Desarrollo y análisis de los controles**

En esta fase se realizarán las actividades que permitan la estructuración de las acciones a tomar.
- Determinar el nombre de la acción.
- Definir los responsables de cada acción.
- Definir las actividades a realizar para el desarrollo de la acción.
- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados
- Análisis de la aplicabilidad

- **Fase 3: Ciclo de vida del tratamiento de riesgos**

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos (PHVA).

5.2. PLAN DE ACCIÓN

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE	EVIDENCIA	FECHAS	
					INICIO	FIN
Gestión de Riesgos	Identificación de riesgos de seguridad y privacidad de la información	Identificación, análisis y evaluación de riesgos de seguridad de la información y seguridad digital	Director TI Oficial de Seguridad y Privacidad de la Información	Matriz de riesgos	Ene	Dic
	Seguimiento a las acciones y controles	Seguimiento al estado de los planes de tratamiento de riesgos identificados y verificación de evidencias	Asesor oficina de riesgos	Matriz de riesgos	Ene	Dic

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE	EVIDENCIA	FECHAS	
					INICIO	FIN
	Mejoramiento	Identificación de oportunidades de mejora si aplican	Asesor oficina de riesgos Director TI Oficial de Seguridad y Privacidad de la Información	Matriz de riesgos	Ene	Dic
	Auditorías	Revisión o seguimientos de la gestión del riesgo	Oficina de Control Interno	Plan de auditoría a los procesos	Ene	Dic

6. RECURSOS

En el marco de la gestión de riesgos de seguridad y Privacidad de la información y Seguridad Digital, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Metología institucional definida por la Oficina de Riesgos de la FLA EICE, en cumplimiento de la Política de Gestión de Riesgos.
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

7. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de lainformación identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

8. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realiza con los indicadores de gestión que están definidos en el Proceso de Tecnología los cuales se encuentran cargados en el Sistema de Información y orienta principalmente la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información.

Créditos

Ministerio de Tecnologías de la Información y las Comunicaciones

Bibliografía

Información tomada del plan de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones