	PROCESO TECNOLOGIA E INFORMACIÓN	Código:PL-ADM-010
		Versión:001
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Aprobado: 2024-01-31

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información ESE FABIO JARAMILLO LONDOÑO

TABLA DE CONTENIDO

Contenido

INTRODUCCIÓN

El Plan de Tratamientos de Riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todas las entidades en cumplimiento de sus funciones están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

OBJETIVO GENERAL

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la ESE FABIO JARAMILLO, tiene los siguientes objetivos:

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

OBJETIVOS ESPECÍFICOS

- Involucrar y comprometer a todos los funcionarios en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

ALCANCE Y RESPONSABILIDADES

Este plan, proporcionará una metodología establecida por la ESE FABIO JARAMILLO LONDOÑO, para la Administración y Gestión de los Riesgos a nivel interno; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis y valoración de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

DIRECCIONAMIENTO ESTRATEGICO

LINEA ESTRATEGICA

A la hora de garantizar la seguridad en cualquier entorno, además de tener las medidas técnicas y legales adecuadas es de vital importancia el factor humano, ya que con frecuencia los mayores problemas de seguridad se presentan por errores o descuidos en el hacer diario del personal, por motivo se debe capacitar al personal que tiene acceso a la información digital y física de la ESE FABIO JARAMILLO LONDOÑO, para minimizar y eliminar el riesgo de pérdida o daño, parcial o total de la información.

GESTION DE RIESGO EN LA SEGURIDAD INFORMATICA

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

En su forma general contiene cuatro fases:

- **ANALISIS:** Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.

- **CLASIFICACION:** Determina si los riesgos encontrados y los riesgos restantes son aceptables

- **REDUCCION:** Define e implementa las medidas de protección. Además, sensibiliza y capacita los usuarios conforme a las medidas

- **CONTROL:** Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.

Orientar el funcionamiento organizativo y funcional.

Garantizar corrección de conductas o prácticas que nos hacen vulnerables

METODOLOGIA DE EVALUACIÓN DEL RIESGO

Es el primer paso hacia la Gestión de Riesgos. Necesita definir las reglas para llevar a cabo la gestión de riesgo, ya que querrá que toda la empresa lo haga de la misma forma, el principal problema del plan de tratamiento de riesgos de seguridad de la información es que la organización lo ejecute de diferente forma en distintas partes de la organización

IDENTIFICACION DEL RIESGO

La finalidad de esta fase es descubrir, reconocer y registrar los riesgos. Este proceso incluye la identificación de las causas y el origen de los riesgos, los sucesos o situaciones que pueden tener un impacto en los objetivos de la organización

METODOS DE IDENTIFICACION DEL RIESGO PUEDEN INCLUIR

Métodos basados en evidencias como pueden ser las listas de veri ficación y las revisiones de datos históricos.

Enfoques sistemáticos de equipos, como los grupos de expertos que siguen un método con una sistemática estructurada de preguntas para identificar los riesgos

ANALISIS DEL RIESGO

Esta fase implica una comprensión del riesgo, es decir, determinar sus consecuencias y probabilidades, teniendo en cuenta la presencia y la eficacia de los controles existentes.

Los métodos que se utilizan para este análisis de riesgos pueden ser cualitativos, semicuantitativos o cuantitativos.

La apreciación cualitativa se suele expresar con niveles del tipo “alto”, “medio” y “bajo” para definir
las consecuencias, las probabilidades o el nivel
de riesgo.

Los métodos semicuantitativos utilizan escalas de valoración numérica lineales o logarítmicas principalmente.

El análisis cuantitativo trabaja con valores numéricos realistas y obtiene el mismo tipo de resultados. El problema suele ser que, en ocasiones, junto a estos valores deben tenerse en cuenta otros factores difícilmente cuantificables o simplemente que faltan datos.

EVALUACIÓN DEL RIESGO

En la fase de evaluación se toman las decisiones sobre las acciones futuras basadas en el conocimiento del riesgo que se ha obtenido durante la fase de análisis.

En la mayoría de las ocasiones, el criterio para tomar la decisión de, si se debe tratar el riesgo y cómo hacerlo, depende de los costos/beneficios de aceptar el riesgo y/o de implantar los controles pertinentes.

El criterio de “tan bajo como razonablemente sea posible” es un clásico de este enfoque de criterio

SELECCIÓN DE LAS TECNICAS DE APRECIACION DEL RIESGO

Llega el momento clave de ver que técnica/herramienta vamos a elegir.

Los principales factores a tener en cuenta son:

- La disposición de recursos adecuados en tiempo y experiencia, así como el presupuesto con el que contamos.

- La naturaleza y el grado de la incertidumbre, que depende de la calidad, cantidad e integridad de los datos e información disponible sobre los riesgos considerados.

- La complejidad de los riesgos

COMPONENTES DE LA IDENTIFICACION DEL

RIESGO CAUSAS DEL RIESGO

Son las causas, uno de los aspectos a eliminar o mitigar para que el riesgo no se materialice; esto se logra mediante la definición de controles efectivos. Para realizar el análisis de las causas existen varias técnicas que serán analizadas a continuación.

LLUVIA DE IDEAS

Usualmente se utiliza la técnica de lluvia de ideas para identificar todo aquello que puede ser considerado dentro del análisis de riesgos y para que esta sea eficaz, se debe considerar que:

- Debe haber un moderador que tome nota y que organice las exposiciones de todos los participantes, indicando el tiempo que cada cual tiene para presentar sus ideas.

- Es más importante la cantidad de ideas que la calidad de las mismas. Todas las ideas son valiosas para el proceso de recopilación de información.

- No se deben calificar las ideas como buenas o malas, son simplemente puntos de vista que capitalizados pueden brindar alternativas no consideradas.

- Es importante soportarse en las ideas de los otros. Es decir, agregar valor a las apreciaciones de otros o considerar situaciones a partir de las mismas.

- El análisis de las ideas se debe realizar al final, por el moderador, quien las organizará y las expondrá a manera de resultado.

- Todos deben participar de manera equitativa, es importante no fijar la atención en pocos participantes, ni mantenerse en la palabra sin dar la oportunidad a otro de expresar sus ideas

CONSECUENCIAS

Son los efectos que se generan o pueden generarse con la materialización del riesgo sobre los objetivos de los procesos y de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Se deben determinar las consecuencias del riesgo en escala ascendente; definiendo cual podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado

CLASIFICACION DE LOS RIESGOS

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo.