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

2019

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN LAS COMUNICACIONES

El servicio público es de todos

Función Pública

CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. VALORACION DE LOS RIESGOS 3
4. ESTRATEGIAS EN EL TRATAMIENTO DE RIESGOS 4
5. PLAN DE SEGUIMIENTO DE RIESGOS - EVALUACIÓN, SEGUIMIENTO Y MONITOREO DEL PLAN DE RIESGOS 4
6. RECURSOS 5
7. ACTIVIDADES 5
8. PLAN PARA EL TRATAMIENTO DE RIESGOS EXTREMOS. 5

1. Objetivo

Establecer el plan de tratamiento de riesgos el cual define las responsabilidades, recursos y actividades que permitan la adecuada gestión de los riesgos de Seguridad de Información en alineado con la Política general de seguridad de la información, la Política de Riesgos y la Guía para la administración del riesgo de Función Pública.

2. Alcance

El presente documento rige para los activos de información y los riesgos identificados en los procesos que seleccione la entidad como prioritarios y el tratamiento de los riesgos valorados como “Extremos” conforme se describe a continuación.

3. Valoración De Los Riesgos

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 el nivel de riesgo y las posibles acciones a implementar.

El análisis de riesgos 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. Por lo tanto, se analiza el riesgo combinando estimaciones de impacto y probabilidades en el contexto de las medidas de control existente.

La aplicación de análisis cualitativo facilita la calificación y evaluación de los riesgos al aplicar formas descriptivas para presentar la magnitud de las consecuencias potenciales (consecuencia) y la posibilidad de ocurrencia (probabilidad). La siguiente tabla describe la valoración de los riesgos definidos por el Departamento Administrativo de la Función Pública.

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi seguro					
Probable					
Posible					
Improbable					
Rara vez					

El detalle se encuentra registrado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 2018, Función Pública.

4. Estrategias En El Tratamiento De Riesgos

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.

El incumplimiento dela política de Seguridad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, en cuanto a Seguridad de la Información se refiere.

5. Plan De Seguimiento De Riesgos - Evaluación, Seguimiento Y Monitoreo Del Plan De Riesgos

El seguimiento y monitoreo al Plan de Tratamiento de Riesgos está a cargo de la Oficina de Control Interno. Esta Dirección evalúa el desarrollo y cumplimiento de las acciones contempladas para prevenir o mitigar los riesgos identificados en los procesos establecidos en el alcance. El

instrumento para hacer seguimiento y monitoreo al riesgo del proceso implicado es la auditoría. Por lo tanto, la evaluación de acuerdo con normas de auditoría interna se basa en soportes como manuales de procesos, manuales de procedimientos, formatos, registros, entre otros.

La metodología utilizada para el plan de seguimiento de riesgos debe realizarse mediante la verificación, análisis de documentos y entrevistas con funcionarios del proceso mencionado. La Dirección de Control Interno indagará por el cumplimiento de las acciones estipuladas donde se sugerirá y aplicará los correctivos y ajustes necesarios para asegurar un manejo efectivo del riesgo.

6. Recursos

- Humano: Directores y jefes de Oficina, Oficina de Asesora de planeación, Oficial de Seguridad(Contratación), Encargado de Seguridad, Técnico de seguridad informática(Contratación), Técnico documentador y pruebas(Contratación).
- Físicos: Firewall, equipos de red, equipos tipo servidor y equipos de escritorio.
- Financieros:

7. Actividades

- Realizar Diagnóstico
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
- Realizar capacitación en identificación de Activos de Información y valoración de riesgos por los líderes del Proceso
- Entrevistar los líderes del Procesos
- Realizar la identificación de Riesgos mediante etical hacking
- Valorar del riesgo y del riesgo residual
- Realizar Mapas de calor donde se ubican los riesgos
- Plantear al plan de tratamiento de riego aprobado por los lideres

8. Plan para el Tratamiento de Riesgos Extremos.

Riesgo Específico	Estrategia genérica	Control Aplicable / Descripción de la estrategia a aplicar	Efecto Potencial en la severidad del riesgo y/o efectividad del control	Responsable de la estrategia	Recursos	Plazo
Problemas operativos por interrupción del servicio	Mitigar	Definir y garantizar el procedimiento de Backup así como la definición y ejecución de procedimientos de restauración de copias de respaldo a aplicaciones y sistemas. Desarrollar y revisar periódicamente planes de continuidad de seguridad de la información para su estricto cumplimiento. Procedimiento de definición y detección de posibles incidentes de seguridad de la información para dar respuesta a eventos. Desarrollar y ejecutar periódicamente un procedimiento que permita conocer el desempeño de las aplicaciones y sistemas Dimensionar los recursos necesarios para el crecimiento y desempeño de sistemas y aplicaciones. Implementar herramientas de detección automatizada de vulnerabilidades.	Estrategia utilizada para mejorar la continuidad del servicio y prevenir la probabilidad de ocurrencia del riesgo	Oficial de Seguridad / Director Oficina de Sistemas	Procedimientos, Acuerdos contractuales	31/12/2016