Plan de tratamiento de riesgos de seguridad y privacidad de la información

2020

Este documento contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta la Corporación 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 mediante el plan de tratamiento de riesgos. El no contar con una buena gestión de la seguridad de la información, puede traer consecuencias graves, como pérdida, fuga o robo de información, alteración de documentos, negación de servicios, etc

CONTENIDO

ÍNDICE DE ILUSTRACIONES

1. OBJETIVO GENERAL

Presentar el Plan de Tratamiento para los riesgos de seguridad y privacidad de la información, identificados en los procesos incluidos en el alcance del Sistema de Gestión de la Seguridad de la Información de la Corporación para el desarrollo sostenible del área de manejo especial La Macarena, en adelante CORMACARENA.

2. OBJETIVOS ESPECÍFICOS

- Identificar los riesgos asociados a los procesos que hacen parte del alcance del SGSI
- Calcular el nivel de riesgo
- Establecer el plan de tratamiento de riesgos
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos

3. MARCO LEGAL

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1080 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Cultura
NTC / ISO 27001	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC / ISO 27005	Soporte a la norma ISO 27001 la cual proporciona directrices para la gestión de riesgos de seguridad de la información
NTC/ISO 31000	Proporciona los principios y directrices para la Gestión de Riesgos.

4. MARCO TEÓRICO

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto CORMACARENA. Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la metodología emitida por el Departamento Administrativo de la Función Pública, en su versión vigente.

A continuación, se presenta las actividades generales para la implementación del Plan:

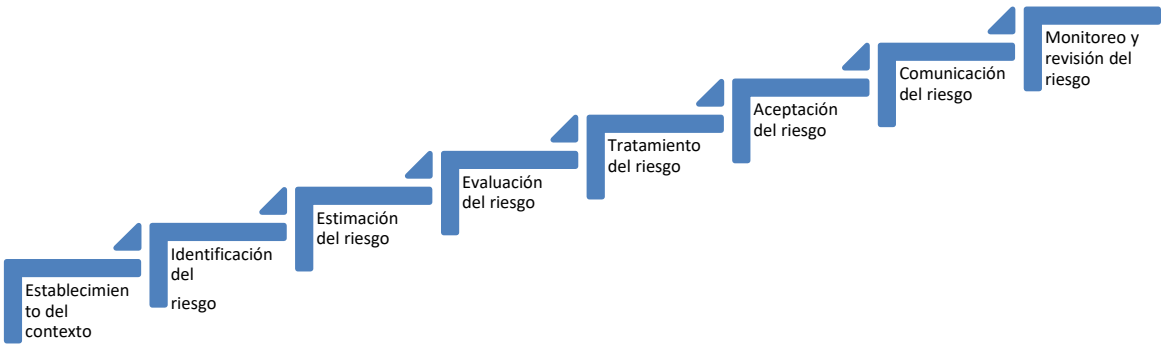

Ilustración 1. Estructura general de la metodología de riesgos

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001):

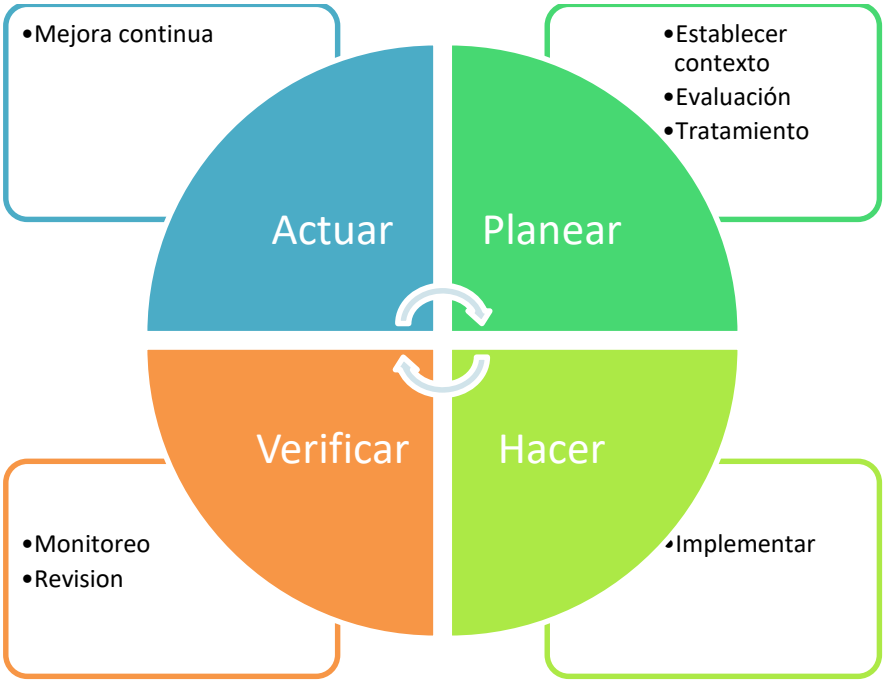

Ilustración 2. Ciclo PHVA y la gestión de riesgos

5. ACTIVIDADES

El Plan de Tratamiento de riesgos de seguridad y privacidad de la información está compuesto por las siguientes actividades:

5.1 PROGRAMACIÓN Y AGENDAMIENTO DE ENTREVISTAS

En esta fase se seleccionan los procesos incluidos en el alcance del Sistema de Gestión de la Seguridad de la Información de la CORPORACIÓN y se procede a programar y a agendar a los líderes de proceso para la identificación de riesgos.

5.2 ENTREVISTA CON LOS LÍDERES DE PROCESO

Se entrevista a cada líder de proceso, se explica la metodología y en conjunto se procede a realizar la identificación de los riesgos, los cuales se consignan en la Matriz de Riesgos.

5.3 IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS

En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

5.4 VALORACIÓN DEL RIESGO RESIDUAL

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

5.5 MAPAS DE CALOR DONDE SE UBICAN LOS RIESGOS

Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

5.6 PLAN DE TRATAMIENTO DE RIESGOS

Cada líder de proceso debe aprobar e implementar el plan de tratamiento de riesgos propuesto.

5.7 SEGUIMIENTO Y CONTROL

El seguimiento y control se realiza de acuerdo al formato PS-GSIT 1.3.74.15 Mapa de riesgos de seguridad de la información

6. CRONOGRAMA

HITOS	1	2	3	4	5	6	7	8	9	10	11	12
5.1 PROGRAMACIÓN Y AGENDAMIENTO DE ENTREVISTAS												
5.2 ENTREVISTA CON LOS LÍDERES DE PROCESO												
5.3 IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS												
5.4 VALORACIÓN DEL RIESGO RESIDUAL												
5.5 MAPAS DE CALOR DONDE SE UBICAN LOS RIESGOS												
5.6 PLAN DE TRATAMIENTO DE RIESGOS												
5.7 SEGUIMIENTO Y CONTROL												

Ilustración 3. Cronograma

7. GLOSARIO

- **Activo**: cualquier elemento que tenga valor para la organización.
- **Activo de Información:** Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.
- **Amenazas:** Cualquier evento, persona, situación o fenómeno que pueda causar daño.
- **Análisis de brechas:** es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado
- **Análisis del riesgo**: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- **Causa**: Elemento específico que origina el evento.
- **Controles**: Procesos, políticas y/o actividades que pueden modificar el riesgo.
- **Criterios de riesgos**: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- **Evaluación del Riesgo**: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.

- **Evento**: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Fuente**: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Información:** Conjunto de datos que tienen un significado.
- **Impacto:** Daño que provoca la materialización de una amenaza.
- **Identificación del riesgo**: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- **ISO:** Organización Internacional de Normalización es una organización para la creación de estándares internacionales
- **MSPI:** Modelo de seguridad y privacidad de la información
- **Riesgo aceptable**: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- **PHVA:** Planear, hacer, verificar, actuar
- **Riesgo residual**: Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- **Riesgo**: Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos
- **SGSI:** Sistema de Gestión de seguridad de la Información
- **Seguridad informática:** Se ocupa de la implementación técnica y de la operación para la protección de la información.
- **Seguridad de la información:** Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.
- **Vulnerabilidades:** Falla o debilidad en un sistema que puede ser explotada por quien la conozca.