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

CORPORACIÓN AUTÓNOMA REGIONAL DEL ALTO MAGDALENA – CAM

Control de Versiones	Fecha
Versión 1	30 de Enero de 2020

Carrera 1 No. 60 -79 Barrio Las Mercedes
Neiva – Huila (Colombia)
Teléfono (578) 8765017
Correo: camhuila@cam.gov.co
www.cam.gov.co

INTRODUCCIÓN

El plan de tratamiento de riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio. Razón por la cual, se hace necesario identificar los riesgos existentes en la Corporación, teniendo en cuenta la sensibilización y capacitación del personal para que se sigan una serie de normas y procedimientos referentes a la seguridad de la información y recursos.

El no contar con una buena gestión de la seguridad de la información, para la CAM puede traer graves consecuencias, como pérdida, fuga, robo de información, alteración de documentos, negación de servicios etc.

1. OBJETIVOS

1.1 Objetivo General

Brindar una herramienta que proporcione los lineamientos para Identificar, Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes en la Corporación Autónoma Regional de Alto Magdalena – CAM, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios, que permitan una adecuada toma de decisiones para disminuir la probabilidad de amenazas.

1.2 Objetivos Específicos

- Proponer soluciones frente a las amenazas identificadas para minimizar los riesgos a los que está expuesta la Corporación.
- Proteger los activos de información de la Corporación de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad.
- Gestionar eventos de seguridad de la información.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

2. ALCANCE

El alcance del presente plan de tratamiento del riesgo es aplicable a todos los procesos de la Corporación Autónoma Regional del Alto Magdalena - CAM con manejo de activos de información, de acuerdo al plan de Seguridad y Privacidad de la Información.

3. RECURSOS

Humano: Director General, Gestores del Proceso, Profesionales y contratistas.

Físico: Servidores, sistemas de seguridad, PC, recursos web y equipos de comunicación.

Financieros: De acuerdo a lo estimado por la corporación.

4. RESPONSABLES

- Director General de la Corporación
- Subdirectores de las dependencias de la Corporación
- Oficina de Gestión Informática y Tecnológica

5. GESTIÓN DE RIESGOS

5.1 Importancia De La Gestión De Riesgos

La Corporación Autónoma Regional del Alto Magdalena – CAM, siguiendo los lineamientos del Gobierno Nacional que viene promoviendo actividades para que las entidades se ajusten a estándares que permitan brindar seguridad en la información cumpliendo la normatividad vigente, se establece como prioridad salvar, proteger y custodiar la información, se consideran como los riesgos más comunes

los ataques dirigidos al software empresarial, daños en los equipos (PC, servidores y dispositivos de almacenamiento), afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación y entendiendo en cuenta que el costo de recuperación es muy alto es preferible tener implementados planes de gestión y prevención de riesgos que permitan la continuidad de las actividades de la Corporación tras sufrir alguna pérdida o daño en la información de la entidad.

Por lo anterior expuesto es preciso diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

La CAM adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Gestión del Riesgo, y para ello todos los funcionarios y personal relacionado con la entidad se comprometen a:

- Conocer y cumplir las normas internas y externas relacionadas con la gestión de los riesgos.

- Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

- Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.

- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.

- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.

- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Dirección General en conjunto con la Oficina de Planeación, asignará los recursos humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de la gestión de los riesgos.

5.1.1 Escenarios que se pueden presentar

- Hurto, perdida o daño de equipos de cómputo y sistemas de información.

- Daño en las instalaciones por desastres naturales o intencionales.

- Alteración de claves y mala manipulación de la información.

- Ataques maliciosos o secuestro de información, mediante malware, virus, etc.

5.2 Definiciones Gestión Del Riesgo

• Control preventivo: Conjunto de medidas orientadas a disminuir la probabilidad de riego.

• Control correctivo: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

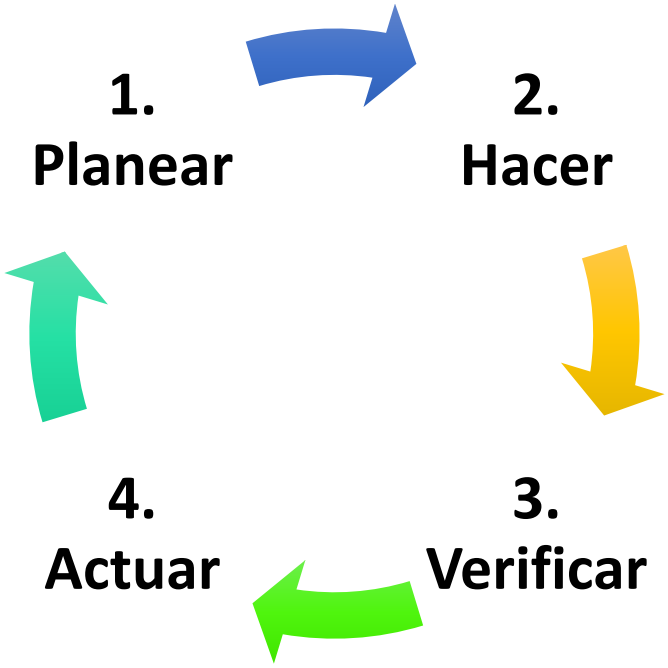
• Análisis del riesgo: Estudio para evaluar los peligros potenciales y sus posibles consecuencias, con el objeto de establecer medidas de prevención y de protección.

• Materialización del riesgo: Impacto del riesgo.

• Contexto estratégico: Identificación de los factores internos o externos a la entidad que pueden generar riesgos que afecten el cumplimiento de sus objetivos como entidad.

6. METODOLOGÍA DE IMPLEMENTACIÓN

La Corporación Autónoma Regional del Alto Magdalena - CAM se toma como modelo base la metodología PHVA (Planear, Hacer, Verificar y Actuar) emitida por MINTIC.



6.1 Propósito De La Implementación Del Plan De Tratamiento De Riesgos De Seguridad De La Información.

- Dar soporte al modelo de seguridad de la información al interior de la corporación.

- Preparación de un plan de respuesta a eventualidades.

- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

7. ACTIVIDADES

- Diseñar un plan de tratamiento de riesgos acorde con los recursos disponibles y aprobados por las directivas de la Corporación.

- Encontrar donde se ubican los riesgos y su incidencia.

- Efectuar diagnósticos en el que se identifiquen posibles vulnerabilidades.

- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información

- Realizar la Identificación de los Riesgos.

- Valorar los riesgos.

8. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las actividades indicadas arriba, se describe a continuación que se debe desarrollar y plazos para su implementación de acuerdo a lo establecido por la Corporación.

- Aspectos organizativos de la seguridad de la información

- Seguridad Ligada a los recursos humanos

- Revisión del Control de acceso

- Seguridad en la operativa

- Seguridad en las telecomunicaciones

- Gestión de Incidentes de Seguridad de la Información

- Aspectos de seguridad de la información en la gestión de continuidad de las actividades.

9. SEGUIMIENTO Y EVALUACIÓN

Al finalizar cada etapa se realizará una socialización con el Jefe de la Oficina de Planeación y la Oficina de Gestión informática y tecnológica, para presentar el informe respectivo de cada una de las actividades del avance del plan de gestión de riesgos para evaluar todos los pasos se han ido realizado.