Empresas Públicas de La Ceja E.S.P
Tu empresa, nuestra empresa

Plan de Tratamiento de Riesgos de seguridad y Privacidad de la Información.

Nit: 811.009.329-0
Telefono: 604 553 77-88
Punto CIEM – Calle 20 # 22 – 05
Email: esplaceja@eeppdelaceja.gov.co
www.eeppdelaceja.gov.co
@eeppdelaceja

Introducción

Mediante la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información; se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos de Empresas Públicas de La Ceja E.S.P.

El presente Plan 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 la prestación esencial del servicio de la Entidad.

MARCO NORMATIVO

- 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 1008 de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

DEFINICIONES

• **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo a la Entidad 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 Entidad (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 la Entidad.

Objetivo

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, que Empresas Públicas de La Ceja E.S.P. pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

Objetivos específicos

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Gestionar riesgos de seguridad y privacidad de la información, 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.

POLÍTICA DE ADMINISTRACION DE RIESGOS

Empresas Públicas de La Ceja E.S.P, a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos de TIC, regulando los riesgos de los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y seguridad digital de manera Integral.

Nit: 811.009.329-0
Telefono: 604 553 77-88
Punto CIEM – Calle 20 # 22 – 05
Email: esplaceja@eeppdelaceja.gov.co
www.eeppdelaceja.gov.co
@eeppdelaceja

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los servidores públicos de Empresas Públicas de la Ceja E.S.P. Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- **Evitar:** es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.
- **Prevenir:** corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.
- **Reducir o mitigar:** corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo.
- **Dispersar:** es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad.
- **Compartir:** es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento, no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento.

Nit: 811.009.329-0
Telefono: 604 553 77-88
Punto CIEM – Calle 20 # 22 – 05
Email: esplaceja@eeppdelaceja.gov.co
www.eeppdelaceja.gov.co
@eeppdelaceja

DESARROLLO METODOLÓGICO

1. **Análisis de la información:** En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:
   - 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.
2. **Desarrollo de los proyectos:** En esta fase se realizarán las actividades que permitan la estructuración de las medidas.
   - Determinar el nombre de la medida.
   - Definir los responsables de cada medida.
   - Establecer el objetivo de cada medida.
   - Elaborar la justificación de la medida.
   - Definir las actividades a realizar para el desarrollo de la medida.
3. **Análisis de los proyectos**
   - Definición de los controles relacionados con cada medida.
   - Validar los riesgos mitigados por cada medida.
   - Análisis de la aplicabilidad de las medidas.
   - Priorización de las medidas.
4. **Definición del organigrama de responsabilidad**
   En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por el Ministerio teniendo en cuenta su estructura organizacional para la gestión de riesgos.
   - Identificación de las funciones del Ministerio en materia de seguridad de la información.
   - Definición del grupo de trabajo de gestión de riesgo por parte del Ministerio.
   - Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.
5. 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.

- Planear: Dentro de esta etapa se desarrollan las actividades definidas en el análisis de la información de la metodología de tratamiento de riesgos.

Nit: 811.009.329-0
Telefono: 604 553 77-88
Punto CIEM – Calle 20 # 22 – 05
Email: esplaceja@eeppdelaceja.gov.co
www.eeppdelaceja.gov.co
@eeppdelaceja

- Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en el desarrollo de los proyectos de la metodología del tratamiento de riesgos.
- Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.
- Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

OPORTUNIDAD DE MEJORA

Empresas Públicas de La Ceja E.S.P. no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

RECURSOS

La estimación y asignación de los recursos para el plan de tratamiento de riesgos de Seguridad de la información 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.

MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realizara con un indicador de gestión que está orientada principalmente en 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, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la informa.

Nit: 811.009.329-0
Telefono: 604 553 77-88
Punto CIEM – Calle 20 # 22 – 05
Email: esplaceja@eeppdelaceja.gov.co
www.eeppdelaceja.gov.co
@eeppdelaceja

Así mismo, si se llegan a presentar incidentes de seguridad se validarán los riesgos identificados para determinar si obedece a un riesgo identificado y proceder a valorar, recalificar e implementar nuevos controles.

ANEXO

- Matriz de Riesgos

SEBASTIAN ARBOLEDA CARDONA
Gerente General

YOLANDA VALLEJO TOBON
Directora Administrativa

VANESA OROZCO BENITEZ
P.U de las TIC

CONTROL DE CAMBIOS

VERSIÓN	FECHA	ELABORÓ	REVISÓ	APROBÓ	MODIFICACIONES
01					