

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

EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE MANIZALES ERUM S.A.S.

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información 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 de los objetivos trazados en el Entorno.

Lo anterior dando cumplimiento al artículo primero del Decreto 612 del 2018 cuyo tenor literal manifiesta la integración de los planes institucionales y estratégicos al Plan de Acción de la ERUM S.A.S. vigencia 2022.

DEFINICIONES

- **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 una entidad.
- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **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 institución (materializar el riesgo).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Política para la gestión del riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Manizales, Centro Administrativo Municipal CAM

Calle 19 #21 - 44 Torre A pisos 7 y 13
Tels: (+57) 6 8722053 • (+57) 6 8720538 • (+57) 6 8720630

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

OBJETIVO GENERAL

Establecer y ejecutar acciones para la aplicación de los Planes de Tratamiento del Riesgo de Seguridad con el fin de minimizar el nivel de exposición de amenazas cibernéticas preservando la confidencialidad, integridad y disponibilidad de la información en la Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S.

OBJETIVOS ESPECÍFICOS

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.
- Reducir la probabilidad materialización de un incidente de Seguridad de la Información en la infraestructura tecnológica de la ERUM S.A.S.

ALCANCE

La Gestión de Riesgos de Seguridad de la Información y sus Planes de Tratamiento aplica a todos los procesos donde se (crea, almacena y transfiere) información propiedad de la Entidad permitiendo garantizar la confidencialidad, integridad y disponibilidad de la información que emite la Empresa de Renovación y Desarrollo Urbana de Manizales.

POLÍTICA DE ADMINISTRACION DE RIESGOS

La Empresa de Renovación y Desarrollo Urbana de Manizales S.A.S. se compromete a mantener una cultura de la gestión del riesgo asociada con la responsabilidad de diseñar, adoptar y promover las políticas, planes y programas donde se regulen los riesgos de los procesos mediante mecanismos enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia dando respuesta oportuna a los riesgos de seguridad y privacidad de la Información y Seguridad Digital de manera Integral.

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 colaboradores de la ERUM S.A.S.

Para llevar a cabo el plan de manera adecuada se deben tener en cuenta las siguientes opciones:

Manizales, Centro Administrativo Municipal CAM

Calle 19 #21 - 44 Torre A pisos 7 y 13

Tels: (+57) 6 8722053 • (+57) 6 8720538 • (+57) 6 8720630

- **Evitar:** el acceso a personal no autorizado a los lugares donde se almacena la información física y digital de la entidad evitando así la pérdida de documentación se prohíbe el ingreso a un área.
- **Prevenir:** planear estrategias adecuadas a que la pérdida de información no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones y el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos de archivo de la información.
- **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 contingencia equipos de protección personal y tecnológico de acceso mantener copias de respaldo.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, teniendo en cuenta lo expuesto en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)¹, *"(...) 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 y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados"*(...).

METODOLOGÍA

La evolución de implementación del Plan de Tratamiento de Riesgos, así como la evolución en la madurez del nivel de riesgo residual, obtenido con el despliegue de las medidas puestas en producción, han permitido identificar las capacidades para anticipar los riesgos de las amenazas digitales que puedan comprometer los objetivos estratégicos y la reputación de la Entidad.

Los Planes de Tratamiento del Riesgo de Seguridad, traen consigo lograr el desarrollo de las iniciativas para la transformación digital en la ERUM S.A.S.; tales como:

- Identificación de situaciones críticas en los procesos de tratamiento de datos, que a través de la evaluación del riesgo podemos discernir la probabilidad e impacto de un evento de seguridad.
- Identificación de qué está pasando con la tecnología que soporta el respaldo de los datos.
- Identificación de qué amenazas cibernéticas son fuentes de información para poder actuar en contra de ellas, creando un plan de acción para abordar estas amenazas.



Manizales, Centro Administrativo Municipal CAM

• Calle 19 #21 - 44 Torre A pisos 7 y 13

Tels: (+57) 6 8722053 • (+57) 6 8720538 • (+57) 6 8720630

DESARROLLO DE LA METODOLOGÍA

ACTIVIDAD	OBJETIVO	TAREA
Análisis del Plan de Tratamiento	En esta etapa se analizará la información de los riesgos de seguridad con los dueños de los procesos información.	<ul style="list-style-type: none"> • Aplicar las políticas en los planes de tratamiento de riesgos. • Identificar los controles que ya existen aplicados para mitigar el riesgo. • Identificar aquellos riesgos de seguridad que por su naturaleza no se les puede aplicar un Plan de Tratamiento.
identificación de Responsabilidades	En esta fase se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa debe ser definida por el dueño del proceso y del riesgo de seguridad.	<ul style="list-style-type: none"> • Identificar las responsabilidades del gestor del riesgo en la mitigación del riesgo de seguridad. • Definir las actividades que se ejecutarán para la aplicación del Plan de Tratamiento del riesgo de seguridad.
Plan de Tratamiento como Proyecto	Esta fase determina, que para el tratamiento de un riesgo o varios riesgos es indispensable llevar a cabo la implementación de un proyecto para su mitigación.	<ul style="list-style-type: none"> • Definir las actividades que permitan el desarrollo de la acción de mitigación del riesgo en la etapa de la actividad que aplique. • Definir los responsables que

Manizales, Centro Administrativo Municipal CAM

• Calle 19 #21 - 44 Torre A pisos 7 y 13

Tels: (+57) 6 8722053 • (+57) 6 8720538 • (+57) 6 8720630

		<p>participarán en la parte del proyecto con el fin de no desviar la acción en la mitigación del riesgo.</p> <ul style="list-style-type: none"> • Establecer el objetivo de la actividad que permitirá mitigar el riesgo en la medida que avanza el proyecto. • Elaborar la justificación de la actividad que permitirá mitigar el riesgo.
<p>Análisis del Plan de Tratamiento del Riesgo de Seguridad dentro de la entidad</p>	<p>Esta fase se ejecuta una vez se determinan las medidas que se establecen en el Plan de Tratamiento.</p>	<ul style="list-style-type: none"> • Analizar los riesgos que fueron mitigados con la aplicación del control de seguridad. • Monitorear el riesgo para identificar la eficacia en la aplicabilidad del control.
<p>Ciclo de Vida del Tratamiento de Riesgos</p>	<p>En la gestión del Riesgo de Seguridad de la Información, el activo a proteger es la información. Es decir que la gestión y aplicación de los Planes de Tratamiento del Riesgo se deben ocupar de todo el ciclo de vida de la información, considerando aspectos como la creación, almacenamiento y el transporte de ésta y, así como, la destrucción de la misma.</p>	<p>la metodología usada actualmente para llevar a cabo su implementación con el apoyo de los gestores del riesgo definidos en cada uno de los procesos de la Entidad, contemplando un ciclo de PHVA.</p> <ul style="list-style-type: none"> • Planear: Dentro de esta etapa se desarrollan las actividades definidas para el tratamiento del riesgo. • Hacer: En esta etapa del ciclo de vida se

Manizales, Centro Administrativo Municipal CAM

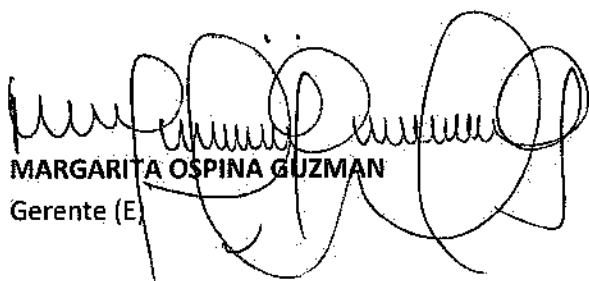
• Calle 19 #21 - 44 Torre A pisos 7 y 13

☎ Tejs: (+57) 6 8722053 • (+57) 6 8720538 • (+57) 6 8720630

		<p>desarrollan actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.</p> <ul style="list-style-type: none"> • Verificar: En esta etapa se desarrollan actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas. • Actuar: En de esta etapa se realizan mejoras en los Planes de Tratamiento, teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de éstos.
<p>Plan de Tratamiento de Riesgos de Seguridad</p>	<p>Los dueños de los procesos y/o gestores del riesgo, serán los responsables de identificar y de aplicar los planes de acción o aplicación de controles de acuerdo con la zona de exposición (baja, moderada, alta, extrema) para el tratamiento de los riesgos de seguridad de la información. Adicionalmente es responsabilidad de los dueños de proceso evaluar la efectividad de los controles implementados durante el ciclo de vida de los riesgos.</p>	<p>De acuerdo con la metodología de administración de riesgos de la Entidad, una vez se hayan evaluado los controles y el riesgo se ubica en una zona que requiera tratamiento, este se debe realizar en función de las opciones de tratamiento que se encuentran en la metodología de la ERUM S.A.S.</p>

Monitoreo y Seguimiento	El monitoreo y seguimiento del Plan de Tratamiento del Riesgo de Seguridad, permite direccionar el riesgo a una mejora continua, adoptando nuevos procedimientos o mecanismos para ser más predictivos con las nuevas amenazas	Esta actividad la realizará la persona designada para ejecutar el monitoreo y seguimiento de la aplicación de los Planes de Tratamiento del Riesgo de Seguridad.
--------------------------------	--	--

Manizales, 31 de enero de 2022


MARGARITA OSPINA GUZMAN
Gerente (E)

Manizales, Centro Administrativo Municipal CAM

• Calle 19 #21 - 44 Torre A pisos 7 y 13

Tels: (+57) 6 8722053 • (+57) 6 8720538 • (+57) 6 8720630

ernum