

	EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.	CÓDIGO: ES-INF.PL.03
		APROBADO: 17/01/2024
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 3
		PAGINA: 1 de 10

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

2024

Se adopta mediante resolución No. 027
24 de enero de 2024

 Carrera 1 No 15 – 20 B/ Antonio Naranjo
 +57 (608) 8360012

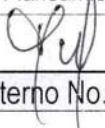
 WhatsApp: 3212500475
 contacto@empitalito.gov.co

 www.empitalito.gov.co

	EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.	CÓDIGO: ES-INF.PL.03
		APROBADO: 17/01/2024
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 3
		PAGINA: 2 de 10

TABLA DE CONTENIDO

1.	<u>INTRODUCCION</u>	3
2.	<u>JUSTIFICACIÓ</u>	3
3.	<u>OBJETIVOS</u>	3
3.1	<u>GENERAL</u>	3
3.2	<u>ESPECÍFICOS</u>	4
4.	<u>ALCANCE</u>	4
5.	<u>DEFINICIONES</u>	4
6.	<u>MARCO REFERENCIAL</u>	5
7.	<u>METODOLOGÍA</u>	6
8.	<u>RECURSOS</u>	6
9.	<u>DETALLE DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</u>	7

Elaboró: Jefersson Silva Losada	Revisó: Mónica Alexandra Lagos Serrato
Cargo: Profesional de Sistemas	Cargo: Profesional Planeamiento y Control
Firma: 	Firma: 

Aprobado Mediante Estudio de Novedad Interno No. 017 de 2024

	EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.	CÓDIGO: ES-INF.PL.03
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	APROBADO: 17/01/2024 VERSIÓN: 3 PAGINA: 3 de 10

1. INTRODUCCION

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Pérdida de la Confidencialidad, Integridad y Disponibilidad de los activos) evitando aquellas situaciones que impidan el cumplimiento de los objetivos de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

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 del mismo.

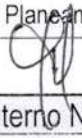
2. JUSTIFICACIÓN

El presente documento tiene como fin generar una cultura de prevención contra los riesgos a los que día a día se pudieran ver sometidos los activos de información la empresa de servicios públicos domiciliarios EMPITALITO. Basados en un enfoque de planeación de gestión del riesgo se pretende realizar una estrategia que permita diagnosticar, evaluar, implementar y desarrollar la gestión de incidentes que afectan al activo de información e implantar unas contramedidas en el sistema de gestión informático para disminuir la probabilidad de su materialización.

3. OBJETIVOS

3.1 GENERAL

Brindar a la empresa de servicio públicos domiciliarios EMPITALITO una herramienta que proporcione las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, que permitan una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza o bien reducir la vulnerabilidad del sistema o el posible impacto en la Entidad, así como permitir la recuperación del sistema o la trasferencia del problema a un tercero.

Elaboró: Jefersson Silva Losada	Revisó: Mónica Alexandra Lagos Serrato
Cargo: Profesional de Sistemas	Cargo: Profesional Planeamiento y Control
Firma: 	Firma: 

Aprobado Mediante Estudio de Novedad Interno No. 017 de 2024

	EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.	CÓDIGO: ES-INF.PL.03
		APROBADO: 17/01/2024
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 3
		PAGINA: 4 de 10

3.2. ESPECÍFICOS

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información de EMPITALITO ESP.
- Gestionar riesgos de Seguridad y Privacidad de la información, de acuerdo al contexto de EMPITALITO ESP.
- Fortalecer y apropiar conocimientos referentes a la gestión de Riesgos Seguridad y Privacidad de la información

4. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Medio y Alto acorde con los lineamientos definidos por el Ministerio de las TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

5. DEFINICIONES

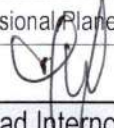
Amenaza: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo)

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 del Instituto.

Impacto: Son las consecuencias que genera un riesgo una vez se materialice.

Probabilidad: Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Riesgo: Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Elaboró: Jefersson Silva Losada	Revisó: Mónica Alexandra Lagos Serrato
Cargo: Profesional de Sistemas	Cargo: Profesional Planeamiento y Control
Firma: 	Firma: 

Aprobado Mediante Estudio de Novedad Interno No. 017 de 2024

	EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.	CÓDIGO: ES-INF.PL.03
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	APROBADO: 17/01/2024
		VERSIÓN: 3 PAGINA: 5 de 10

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información (estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información).

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

6. MARCO REFERENCIAL

A través de la Política de Seguridad y Privacidad de la Información, la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP, se ha comprometido con la Implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la información – MSPI alineado con el Sistema de Gestión de Seguridad de la Información SGSI, aplicando la administración y gestión de riesgos para prevenir o minimizar el impacto generado sobre los activos de la información.

Se deben tener en cuenta alguna 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 pérdida 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 contingencia, equipos de protección personal, ambiental, de acceso y 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. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos.

Elaboró: Jefersson Silva Losada	Revisó: Mónica Alexandra Lagos Serrato
Cargo: Profesional de Sistemas	Cargo: Profesional Planeamiento y Control
Firma:	Firma:

Aprobado Mediante Estudio de Novedad Interno No. 017 de 2024

	EMPRESA DE SERVICIOS PÚBLICOS		CÓDIGO: ES-INF.PL.03
	DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.		APROBADO: 17/01/2024
	PLAN DE TRATAMIENTO DE RIESGOS DE		VERSIÓN: 3
	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		PAGINA: 6 de 10

Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explícita por medio de cláusulas contractuales, derivados financieros.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento.

7. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de acuerdo al Cronograma anexo, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016).

Los controles seleccionados serán confrontados con los estándares ISO 27001:2013 y su anexo A; a fin de determinar las falencias de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP.

8. RECURSOS

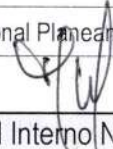
EMPITALITO ESP, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, dispone de los siguientes recursos:

Humanos: La Oficina de TIC a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.

Técnicos: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital Versión 6 noviembre de 2022 del DAFP.

Logísticos: Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.

Financieros: Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías.

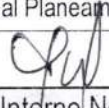
Elaboró: Jefersson Silva Losada	Revisó: Mónica Alexandra Lagos Serrato
Cargo: Profesional de Sistemas	Cargo: Profesional Planeamiento y Control
Firma: 	Firma: 

Aprobado Mediante Estudio de Novedad Interno No. 017 de 2024

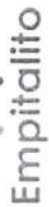
	EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.	CÓDIGO: ES-INF.PL.03
		APROBADO: 17/01/2024
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 3
		PAGINA: 7 de 10

9. DETALLE DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Según lo expuesto en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de Seguridad y Privacidad de la Información enfocado en la seguridad de la información sobre los activos de información, para lo cual se realizan un conjunto de actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados. En atención a lo anterior, a continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de Seguridad y Privacidad de la Información:

Elaboró: Jefersson Silva Losada	Revisó: Mónica Alexandra Lagos Serrato
Cargo: Profesional de Sistemas	Cargo: Profesional Planeamiento y Control
Firma: 	Firma: 

Aprobado Mediante Estudio de Novedad Interno No. 017 de 2024



DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.

APROBADO: 17/01/2024

PAGINA: 9 de 10

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaboró: Jeferson Silva Losada	Revisó: Mónica Alexandra Lagos Serrato
Cargo: Profesional de Sistemas	Cargo: Profesional Planeamiento y Control
Firma: 	Firma: 

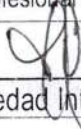
Aprobado Mediante Estudio de Novedad Interno No. 017 de 2024

	EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.	CÓDIGO: ES-INF.PL.03
		APROBADO: 17/01/2024
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 3
		PAGINA: 10 de 10

10. CONTROL DE CAMBIOS

VERSIÓN N°.	FECHA DE APROBACIÓN.	DESCRIPCIÓN DEL CAMBIO.
1	26/01/2022	Creación del plan de tratamiento de riesgos de seguridad y privacidad de la información
2	20/01/2023	Actualización del plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia 2023
3	17/01/2024	Actualización del plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia 2024

JOSE RICARDO VILLARREAL ARTUNDUAGA
GERENTE

Elaboró: Jefersson Silva Losada	Revisó: Mónica Alexandra Lagos Serrato
Cargo: Profesional de Sistemas	Cargo: Profesional Planeamiento y Control
Firma: 	Firma: 

Aprobado Mediante Estudio de Novedad Interno No. 017 de 2024