e

Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información

Empresa De Servicios Públicos De Chía Emserchia E.S.P.

Área de Sistemas de información

2026

Contenido

1. OBJETIVO

Brindar a la Empresa de Servicios Públicos de Chía Emserchia E.S.P. una herramienta que proporcione las pautas necesarias para el adecuado tratamiento de los riesgos a los que está expuesta la entidad, que permitan una adecuada toma de decisiones para disminuir la probabilidad de materialización de amenaza o para reducir la vulnerabilidad del sistema o el posible impacto en la Entidad.

1.1. OBJETIVOS ESPECÍFICOS

- Proteger los activos de información de acuerdo con su clasificación y criterios de confidencialidad, Integridad y Disponibilidad.
- Garantizar el manejo correcto de los riesgos para disminuir su probabilidad e impacto.
- Generar conciencia institucional de la importancia del tratamiento de riesgos.
- Preparar al personal de la entidad ante posibles amenazas externas.

2. ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la Empresa de Servicios Públicos de Chía Emserchia E.S.P., a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las estrategias para la identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

3. MARCO CONTEXTUAL

3.1. FACTORES EXTERNOS E INTERNOS DE RIESGO

Los factores de riesgo son aquellos que afectan a la entidad en mayor o menor grado de impacto.

Tabla 1. CONTEXTO FACTORES EXTERNOS E INTERNOS DE RIESGO	
FACTORES EXTERNOS	**FACTORES INTERNOS**
Económicos: disponibilidad de capital, emisión de deuda o no pago de la misma, liquidez, mercados financieros, desempleo, competencia.	**Procesos:** Eventos Relacionados con errores en la actividades que deben realizar los servidores de la organización.

Medioambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	**Talento Humano:** Incluye SST , Se analiza posible dolo e intención frente a la corrupción.
Políticos: cambios de gobierno, legislación, políticas públicas, regulación.	**Infraestructura:** Eventos relacionados con la infraestructura fisica de la entidad.
Sociales: demografía, responsabilidad social, terrorismo.	**Tecnología:** Eventos relacionados con la infraestructura tecnológica de la entidad
Tecnológicos: interrupciones, comercio electrónico, datos externos, tecnología emergente.	

3.2. RIESGOS

3.2.1. CLASES DE RIESGOS

En el desarrollo de las actividades de la entidad, esta se enfrenta a diversos riegos que pueden afectar de diferentes maneras el correcto funcionamiento y seguridad de los datos. Para conocer el contexto, Emserchia E.S.P. ha definido aquellos riesgos a los cuales se enfrenta para poder generar las diferentes estrategias y mitigar los efectos negativos de estos.

Tabla 2. CLASES DE RIESGO	
CLASE	**DESCRIPCIÓN**
ESTRATEGICO	Se asocia con la forma en que se administra la Entidad. Se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
IMAGEN	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
OPERATIVOS	Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.
FINANCIEROS	Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

DE CUMPLIMIENTO	Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
DE TECNOLOGÍA	Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
DE CORRUPCIÓN	Están relacionados con el uso indebido del poder, de los recursos o de la información, para la obtención de un beneficio particular.
AMBIENTALES	Estan relacionados con las Perdidas por contaminación de recursos naturales; Perdidas generadas por situaciones de emergencia ambiental, pagos de sanciones de la autoridad ambiental o resarcimiento de daños a partes interesadas afectadas; Perdidas por fallas en la continuidad de la operación generadas por dificultad para el acceso a los componentes del ecosistema (Agua, Aire, Suelo, Fauna, Flora, Personas)
POLITICO	Esta relacionado con Pérdidas por decisiones políticas que afectan a la organización.
COMERCIAL	Esta relacionado con las Pérdida de clientes o mercados; Pérdidas económicas por pérdida de clientes; Perdidas por reclamaciones y atención de garantías
DE ORDEN PUBLICO	Estan Relacionados con la Pérdida derivada del conflicto armado; Pérdidas por afectación de la seguridad
DEL RECURSO HUMANO	Pérdida por indisponibilidad del recurso humano con el conocimiento y la competencia requerida para cumplir con los resultados previstos
FENOMENOS NATURALES	Pérdidas por manifestaciones de la naturaleza que puedan afectar los recursos de la organización y la continuidad del negocio

3.2.2. CLASIFICACIÓN DEL RIESGO

De acuerdo con las clases de riesgo, se ha establecido un valor para la probabilidad de la ocurrencia del riesgo teniendo en cuenta la descripción y frecuencia, de la siguiente manera:

Tabla 3. MATRIZ DE CALIFICACIÓN DEL RIESGO			
PROBABILIDAD	**VALOR**	**FRECUENCIA DE LA ACTIVIDAD**	**PROBABILIDAD**
Muy Baja	1	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	20%
Baja	2	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%

Media	3	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	4	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy Alta	5	La actividad que conlleva el riesgo se ejecuta más de 5000 veces al año.	100%

3.2.3. IMPACTO DEL RIESGO

El impacto del riesgo es aquel que en caso de ocurrencia puede generar poca o alta afectación al desarrollo de las actividades de la entidad, de acuerdo con este impacto y a su probabilidad se tendrá el nivel del riesgo.

IMPACTO	VALOR	AFECTACIÓN ECONÓMICA	REPUTACIONAL	A LAS PERSONAS
Leve 20%	5	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización	El riesgo genera afectación leve a la salud de las personas sin incapacidad medica y/o secuelas
Menor 40%	10	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general a nivel interno, de junta directiva y accionistas y/o proveedores	El riesgo genera afectación menor a la salud de las personas con incapacidad medica menor a 8 días
Moderado 60%	20	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de objetivos.	El riesgo genera afectación moderada a la salud de las personas con incapacidad medica mayor a 8 dias y menor a 1 mes
MAYOR 80%	40	Entre 100 SMLMV y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenidos a nivel de sector administrativo,	El riesgo genera afectación mayor a la salud de las personas con incapacidad medica mayor a 1 mes y menor a 6 meses y/o

			departamental o municipal.	puede generar incapacidad laboral parcial
CATASTROFICO 100%	50	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido en el país o a nivel internacional	El riesgo genera catastrófica a la salud de las personas con incapacidad medica mayor a 6 meses, puede generar incapacidad laboral permanente o la muerte

3.2.4. EVALUACIÓN DEL RIESGO

La evaluación del riesgo es el factor más importante para analizar, ya que de este valor surge la respectiva clasificación para implementar los planes de mitigación con sus respectivas acciones, esta se calcula de la siguiente manera:

Valor Clasificación riesgo * Valor del impacto = Valor Evaluación del Riesgo

Una vez se obtenga el valor de la Evaluación del riesgo se procede a clasificarlo de acuerdo a la siguiente tabla:

Tabla 4. MATRIZ DE EVALUACIÓN DEL RIESGO

PROBABILIDAD	VALOR	NIVEL DE RIESGO				
Muy Baja -20%	1	ACEPTABLE (5)	ACEPTABLE (10)	TOLERABLE (20)	TOLERABLE (40)	GRAVE (50)
Baja - 40%	2	ACEPTABLE (10)	TOLERABLE (20)	TOLERABLE (40)	GRAVE (80)	INACEPTABLE (100)
Media - 60%	3	ACEPTABLE (15)	TOLERABLE (30)	GRAVE (60)	INACEPTABLE (120)	INACEPTABLE (150)
Alta - 80%	4	ACEPTABLE (20)	TOLERABLE (40)	GRAVE (80)	INACEPTABLE (160)	EXTREMO (200)

Muy Alta-100%	5	TOLERABLE (25)	GRAVE (50)	INACEPTABLE (100)	EXTREMO (200)	EXTREMO (250)
	VALOR	5	10	20	40	50
	IMPACTO	Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

EVALUACIÓN DEL RIESGO	
ACEPTABLE	5 A 20
TOLERABLE	25 A 40
GRAVE	50 A 80
INACEPTABLE	100 A 160
EXTREMO	200 A 250

Definiciones:

ACEPTABLE	La ubicación en esta zona de la matriz, significa que el potencial del riesgo no es capaz de afectar los resultados previstos por la Alta Dirección de la organización. Por esta razón no se requiere una atención particular para reducir su potencial
TOLERABLE	La ubicación en esta zona de la matriz significa que el potencial del riesgo es capaz de afectar parcialmente los resultados previstos por la Alta Dirección de la organización. Por esta razón se requiere una atención del riesgo en el mediano plazo para reducir su potencial.
GRAVE	La ubicación en esta zona de la matriz significa que el potencial del riesgo es capaz de afectar significativamente los resultados previstos por la Alta Dirección de la organización. Por esta razón se requiere una atención del riesgo en el corto y mediano plazo para reducir su potencial.
INACEPTABLE	La ubicación en esta zona de la matriz significa que el potencial del riesgo es capaz de afectar la estabilidad de la organización. Por esta razón se requiere una atención inmediata del riesgo para reducir su potencial en el menor tiempo posible.
EXTREMO	La ubicación en esta zona de la matriz significa que el potencial del riesgo es capaz de afectar la continuidad de la organización. Los controles deben implementarse de manera inmediata y con prioridad máxima de recursos financieros, humanos, tecnológicos y de infraestructura y hasta que no sea implementado el control la operación de la organización no puede continuar.

3.2.5. CONTROLES

Los controles son aquellos que se utilizan para disminuir la probabilidad y mitigar el impacto de los riesgos establecidos en la matriz. Estos controles ayudaran en el tratamiento del riesgo ya que hay diferentes aspectos a evaluar cómo se indican a continuación:

Tabla 5. ESCALAS DE CALIFICACIÓN ANÁLISIS DE LOS CONTROLES				
CRITERIOS DE CALIFICACIÓN	**NULO**	**MEDIO BAJO**	**MEDIO ALTO**	**ALTO**
Nivel de Documentación (DO)	0	(6-15)	(16-20)	(21-25)
Nivel de Aplicación del Control (AP)	0	(6-15)	(16-20)	(21-25)
Nivel de Efectividad (EF)	0	(6-15)	(16-20)	(21-25)
Nivel de Seguimiento, Evaluación y Mejora (EV)	0	(6-15)	(16-20)	(21-25)

Dependiendo si el control afecta la probabilidad o el impacto se desplaza en la matriz de calificación, evaluación y respuesta a los riesgos. (los controles preventivos afectan la probabilidad mientras que los correctivos afectan el impacto).

Tabla 6. VALORACIÓN DE CONTROLES		
RANGOS DE CALIFICACION DE LOS CONTROLES PUNTAJE (DO+AP+EF+RP)	**CUADRANTES A DISMINUIR EN LA PROBABILIDAD**	**CUADRANTES A DISMINUIR EN EL IMPACTO**
Entre 0 - 50	0	0
Entre 51 - 75	1	1
Entre 76 - 100	2	2

Como se indica en la tabla de acuerdo con los controles que se tenga, se establece si el control aporta a la probabilidad o al impacto y de este modo se disminuirá en la matriz bajando la categoría del riesgo.

4. METODOLOGIA

El plan de tratamiento de riesgos permitirá hacer énfasis de cómo se enfrentarán los riesgos en la entidad.

Para ello se establecen las siguientes actividades:

Actividad	Tarea	Responsable	Fecha inicio	Fecha fin
Implementación	Implementar nuevos controles establecidos en la matriz de riesgos.	Gestión de las Tics	Febrero de 2026	Febrero de 2026
Capacitación	Realizar una capacitación de acerca de ciberataques.	Gestión de las Tics	abril 2026	abril 2026
Informe	Realizar un informe de las actividades realizadas para controlar y mejorar los seguimientos.	Gestión de las Tics	Junio de 2026	Junio de 2026
Seguimiento	Realizar seguimiento de funcionamiento a los controles implementados especialmente aquellos a mitigar los riesgos.	Gestión de las Tics	Junio de 2026	Junio de 2026
Revisar y Actualizar los lineamientos de los riesgos	Revisar y actualizar la matriz de riesgos de TIC (De acuerdo al informe de hacking ético)	Gestión de las Tics y Control interno	Junio de 2026	Junio de 2026
Implementación	Implementar nuevos controles establecidos en la matriz de riesgos.	Gestión de las Tics	Julio de 2026	Julio de 2026
Seguimiento	Realizar seguimiento de funcionamiento a los controles implementados	Gestión de las Tics	Julio de 2026	Julio de 2026

	por el área de sistemas			
Capacitación	Realizar una capacitación de la policía Nacional para el manejo de los ciberataques.	Gestión de las Tics	Septiembre 2026	Septiembre 2026
Informe	Realizar un informe de las actividades realizadas para controlar y mejorar los seguimientos.	Gestión de las Tics	Noviembre de 2026	Diciembre de 2026
Seguimiento	Realizar seguimiento de funcionamiento a los controles implementados especialmente aquellos a mitigar los riesgos.	Gestión de las Tics	Noviembre de 2026	Diciembre de 2026
Revisar y Actualizar los lineamientos de los riesgos	Revisar y actualizar la matriz de riesgos de TIC (De acuerdo con el informe de hacking ético)	Gestión de las Tics y Control interno	Noviembre de 2026	Diciembre de 2026