PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

La Mesa, Cundinamarca enero 2025

Tabla de contenido

1. **INTRODUCCIÓN**

En el contexto actual, donde la digitalización y la gestión de datos juegan un papel fundamental en la operatividad de las organizaciones, la protección de la información se ha convertido en una prioridad esencial para garantizar la continuidad del negocio. La Empresa Regional Aguas del Tequendama S.A. E.S.P. reconoce que los riesgos asociados a la seguridad y privacidad de la información pueden tener consecuencias significativas en su eficiencia operativa, reputación y cumplimiento normativo. En este sentido, es imperativo proteger los activos informáticos, especialmente la información, que constituye el recurso más valioso para el desarrollo y cumplimiento de la misión de la empresa.

La seguridad de la información es crucial para salvaguardar los principios de confidencialidad, integridad y disponibilidad, principios que son la base de la confianza interna y externa de la organización. Dada la creciente amenaza de vulnerabilidades en un entorno tecnológico en constante evolución, se hace necesario implementar medidas de control que permitan gestionar adecuadamente los riesgos y mitigar los impactos que puedan comprometer la seguridad de los datos.

Este documento tiene como objetivo identificar, analizar y compilar los riesgos que afectan la privacidad y seguridad de la información dentro de la Empresa Regional Aguas del Tequendama S.A. E.S.P., proponiendo los lineamientos y estrategias necesarias para prevenir y mitigar dichos riesgos. Así, se busca asegurar la protección de los datos y garantizar su manejo adecuado, en consonancia con los principios de seguridad requeridos en el ámbito empresarial.

2. **OBJETIVO**

Garantizar la protección integral de los activos de información de la Empresa Regional Aguas del Tequendama S.A E.S.P. mediante la identificación, evaluación y tratamiento de los riesgos, implementando controles de seguridad efectivos que reduzcan la probabilidad de incidentes y mitiguen su impacto.

3. **OBJETIVOS ESPECÍFICOS**

- Realizar un inventario completo y actualizado de los activos de información de la organización, asegurando su clasificación según criticidad y nivel de sensibilidad.
- Analizar y documentar los riesgos de seguridad y privacidad presentes en cada proceso, estableciendo su impacto potencial en la organización.
- Diseñar y ejecutar un plan de gestión de riesgos que garantice la identificación, mitigación y monitoreo de los riesgos de seguridad y privacidad de la información.
- Aplicar controles de seguridad adecuados a cada activo de información según su nivel de criticidad y los riesgos detectados, garantizando su protección efectiva.

- Sensibilizar a todos los niveles de la organización sobre la importancia de la gestión de riesgos, asegurando el cumplimiento de las políticas establecidas.
- Implementar un programa de capacitación estructurado en gestión de riesgos, asegurando que los empleados comprendan cómo identificar, evaluar y mitigar riesgos de seguridad y privacidad.

4. **ALCANCE**

Este plan se basa en las directrices y recomendaciones de la norma ISO 27005, que proporciona un marco integral para la gestión de los riesgos asociados con la seguridad de la información. A partir de esta norma, se desarrollará una metodología detallada que orientará a la organización en la identificación, evaluación y aplicación de controles adecuados para mitigar los riesgos, con el objetivo de reducirlos a niveles aceptables, alineados con las necesidades y objetivos estratégicos de la empresa.

Se adoptará un enfoque continuo y flexible en la gestión de riesgos, lo cual permitirá anticipar amenazas potenciales y definir acciones preventivas para reducir su impacto antes de que se materialicen en incidentes. Este enfoque incluye una evaluación constante de la eficacia de las medidas implementadas, adaptándolas según la aparición de nuevas amenazas o cambios en el entorno organizacional.

El alcance del plan también abarcará la gestión de incidentes relacionados con la seguridad de la información, estableciendo procedimientos claros para su identificación, análisis, respuesta y seguimiento. Además, se implementarán medidas preventivas, detectivas y correctivas para salvaguardar los activos informáticos y asegurar la continuidad operativa, minimizando los riesgos que puedan comprometer la seguridad de la información.

Finalmente, el plan garantizará que la protección de la seguridad y privacidad de la información sea un componente central de la estrategia organizacional, apoyando la sostenibilidad y el crecimiento a largo plazo de la Empresa Regional Agua del Tequendama S.A E.S.P..

5. DEFINICIONES

- **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

- **Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

- **Amenaza informática:** la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).

- **Análisis de riesgos:** proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

- **Anonimización de datos:** eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.

- **Autenticación:** provisión de una garantía de que una característica afirmada por una entidad es correcta.

- **Autenticidad:** propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).

- **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- **Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

- **Confidencialidad**: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

- **Custodio de activo de información**: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

- **Datos abiertos:** son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

- **Datos biométricos:** parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

- **Datos personales sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

- **Dato privado:** es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

- **Dato público:** es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

- **Dato semiprivado:** es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

- **Disco duro:** disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y re-grabados como una cinta de audio.

- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **DVD:** Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

- **Evento de seguridad de la información:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

- **Gestión de claves:** son controles que realizan mediante la gestión de claves criptográficas.

- **Gestión de incidentes de seguridad de la información:** procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- **Gestión de riesgos:** actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

- **Habeas data:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

- **Impacto:** el coste para la empresa de un incidente “de la escala que sea”, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información:** La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

- **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.

- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012).

- **No repudio:** servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

- **Parte interesada (Stakeholders):** persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de continuidad del negocio:** plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos:** documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Proceso:** conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012).

- **Propietario de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

- **Responsable del tratamiento:** persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros. Decida sobre la base de datos y/o el Tratamiento de los datos.

- **Segregación de tareas:** reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

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

- **Sistema de Gestión de Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

- **Titular de la información:** es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

- **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

- **Vulnerabilidad:** debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

6. **MARCO NORMATIVO**

Guía de Gestión de riesgos. Guía No.7 (Seguridad y Privacidad de la Información) de MINTIC. “Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001 vigente e ISO 27005 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.”

7. **ROLES Y RESPONSABILIDADES**

- **Los responsables de los procesos:** Identifican, analizan, evalúan y valorar los riesgos por lo menos una vez al año, los funcionarios en el desarrollo de sus actividades conocen e identifican cuales son los riesgos existentes por ende deben proponer estrategias para tratarlos y minimizar su impacto en la empresa.

- **La Dirección:** Aprueba las directrices para la administración del riesgo de la seguridad de la información de la entidad.

- **El proceso de Calidad:** En cuanto a la administración del riesgo en la entidad, orienta, coordina, y ajusta los requisitos normativos en El Sistema Integrado de gestión de la calidad.

- **Los Líderes del proceso de Planeación y Sistemas de Información:** Apoyan la gestión en cuanto a Liderazgo.

- **El Líder de Soporte Tecnológico**: Apoya la gestión en el desarrollo de las actividades.

- **Los Líderes SIG.** Apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos.

- **Los funcionarios internos y Contratistas:** Son llamados a ejecutar los controles y acciones definidas para la administración de los riesgos con el fin de aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos de la entidad.

- **El área de Control Interno:** Se encarga de realizar evaluación y seguimiento a los sistemas y su posible impacto en la entidad.

8. **IMPORTANCIA DE LA GESTIÓN DE RIESGOS**

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.

La Empresa Regional Aguas del Tequendama S.A E.S.P, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

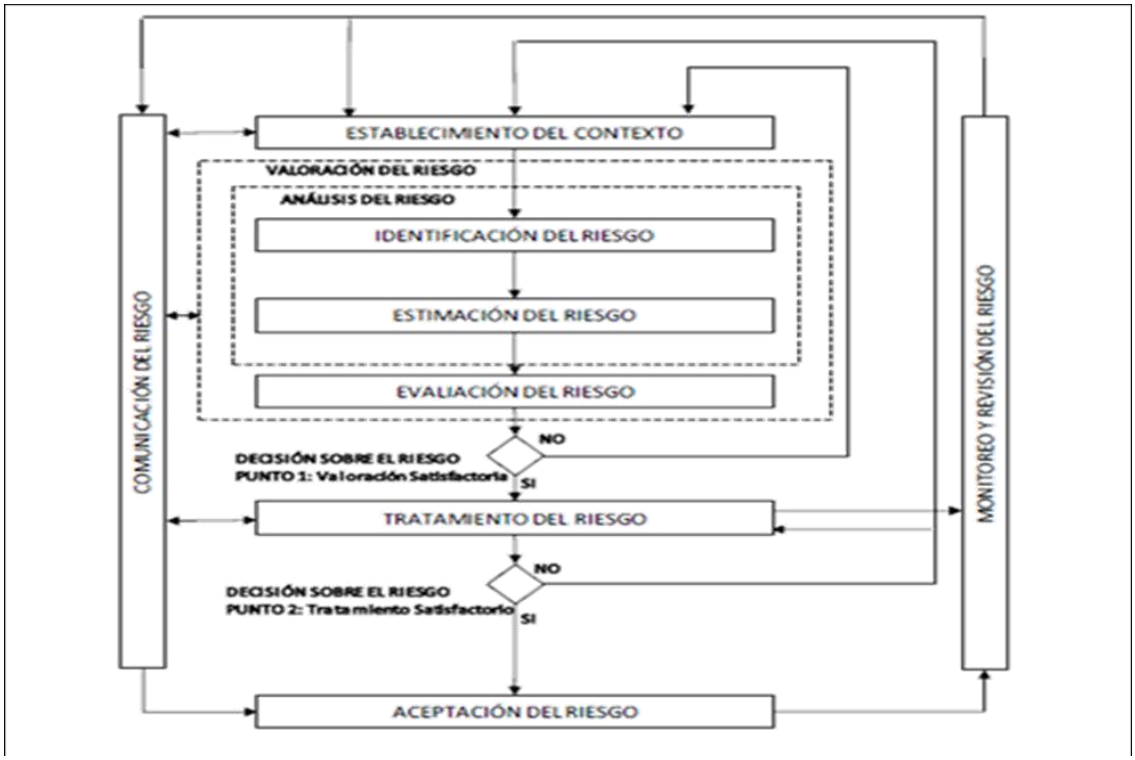
Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de la Empresa Regional Aguas del Tequendama S.A E.S.P, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

9. **ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO**

El proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Este enfoque puede incrementar la profundidad y el detalle de la valoración en cada iteración como se muestra en la figura tomada de la NTC ISO IEC 27005.



Proceso para la administración del riesgo en seguridad de la información - Tomado de la NTC-ISO/IEC 27005.

LAS ETAPAS A CONSIDERAR DURANTE LA ADMINISTRACIÓN DEL RIESGO PARA ERAT S.A E.S.P. SON LAS SIGUIENTES:

- **Contexto estratégico:** Se determinarán los factores externos e internos del riesgo.
- **Identificación:** Se identificarán las causas, riesgo, consecuencias y clasificación del riesgo.
- **Análisis:** Se calificará y evaluará el riesgo inherente.
- **Valoración:** se identificará y evaluaran los controles; se deberá incluir la determinación del riesgo residual.
- **Manejo:** Se determinará, si es necesario, acciones para el fortalecimiento de los controles.

- **Seguimiento:** Se evaluará los riesgos de manera integral.

10. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en La ERAT S.A E.S.P., se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI (Modelo de Seguridad y Privacidad de la Información):

- Diagnosticar
- Planear
- Hacer
- Verificar
- Actuar

Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Actividades

- Realizar Diagnóstico
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
- Realizar la Identificación de los Riesgos con los líderes del Proceso,(Entrevistar con los líderes del Proceso)
- Valorar del riesgo y del riesgo residual
- Realizar Mapas de calor donde se ubican los riesgos
- Plantear al plan de tratamiento de riego aprobado por los lideres

11. FACTORES EXTERNO E INTERNOS DE RIESGO

CONTEXTO FACTORES EXTERNOS E INTERNOS DE RIESGO	
FACTORES EXTERNOS	**FACTORES INTERNOS**
Económicos: disponibilidad de capital, emisión de deuda o no pagode la misma, liquidez, mercados financieros, desempleo, Competencia.	**Infraestructura:** disponibilidad de activos, capacidad de losactivos, acceso al capital.
Medioambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	**Personal:** capacidad del personal, salud, seguridad.
Políticos: cambios de gobierno, legislación, políticas públicas, regulación.	**Procesos:** capacidad, diseño, ejecución, proveedores, entradas, salidas, conocimiento.
Sociales: demografía, responsabilidad social, terrorismo.	**Tecnología:** integridad de datos, disponibilidad de datos ysistemas, desarrollo, producción, mantenimiento.
Tecnológicos: interrupciones, Comercio electrónico, datos externos, tecnología emergente.	

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 desarrollo y seguridad de los datos, para conocer el contexto La ERAT S.A 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.

CLASES DE RIESGO	
CLASE	**DESCRIPCIÓN**
ESTRATEGICO	Se asocia con la forma en que se administra la Entidad. Se enfoca a asuntos globalesrelacionados 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 sistemasde 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 ejecuciónpresupuestal, 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 susnecesidades 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	Están relacionados con las Perdidas por contaminación de recursos naturales; Pérdidas generadas por situaciones de emergencia ambiental, pagos de sanciones dela 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	Está relacionado con Pérdidas por decisiones políticas que afectan a la organización.
COMERCIAL	Está relacionado con las Pérdida de clientes o mercados; Pérdidas económicas porpérdida de clientes; Perdidas por reclamaciones y atención de garantías
DE ORDEN PUBLICO	Están Relacionados con la Pérdida derivada del conflicto armado; Pérdidas porafectación 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 laorganización y la continuidad del negocio

CLASIFICACIÓN DE RIESGO

De acuerdo a la definición anterior de las clases, se han establecido una serie de definiciones para poder establecer un valor para la probabilidad de la ocurrencia del riesgo de acuerdo a la descripción y frecuencia establecidas a continuación:

MATRIZ DE CALIFICACIÓN DEL RIESGO			
PROBABILIDAD	**VALOR**	**DESCRIPCIÓN**	**FRECUENCIA**
Improbable	1	Puede suceder en circunstancias excepcionales	No se ha presentado en los últimos 5 años.
Posible	2	Es probable que **NO** suceda en la mayoría de las circunstancias	Al menos de 1 vez en los últimos 5 años.
Probable	3	Significativa Probabilidad de Ocurrencia	Al menos de 1 vez en los últimos 2 años.
Casi seguro	4	Se espera que suceda en la mayoría de las circunstancias	Más de 1 vez al año.

IMPACTO DEL RIESGO

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

IMPACTO	VALOR	DESCRIPCIÓN
MENOR	5	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad y el proceso.
MODERADO	10	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad y el proceso.
MAYOR	20	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad y el proceso.
CATASTROFICO	40	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad y el proceso.

EVALUACIÓN DEL RIESGO

La evaluación del riesgo es el factor más importante a analizar, de este valor se realiza la respectiva clasificación para proceder a realizar los planes de mitigación con sus respectivas acciones, para poder establecer la evaluación del riesgo se multiplica el valor establecido en la clasificación del riesgo por el valor del impacto.

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:

MATRIZ DE EVALUACIÓN DEL RIESGO					
PROBABILIDAD	**VALOR**	NIVEL DE RIESGO			
Improbable	1	ACEPTABLE (5)	ACEPTABLE (10)	TOLERABLE (20)	GRAVE (40)
Posible	2	ACEPTABLE (10)	TOLERABLE (20)	GRAVE (40)	INACEPTABLE (80)
Probable	3	ACEPTABLE (15)	TOLERABLE (30)	GRAVE (60)	INACEPTABLE (120)
Casi seguro	4	TOLERABLE (20)	GRAVE (40)	INACEPTABLE (80)	INACEPTABLE (160)
	VALOR	5	10	20	40
	IMPACTO	Menor	Moderado	Mayor	Catastrófica

EVALUACIÓN DEL RIESGO	
ACEPTABLE	5 A 15
TOLERABLE	20 A 30
GRAVE	40 A 60
INACEPTABLE	80 A 160

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 capazde 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.

12. **SEGUIMIENTO Y EVALUACIÓN**

El seguimiento y la evaluación del cumplimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025 se llevará a cabo mediante la medición del siguiente

Indicador de Cumplimiento: Efectividad de las estrategias implementadas en la gestión de riesgos de seguridad y privacidad de la información.

Nombre del indicador	Objetivo	Tipo	Meta	Fórmula	Frecuencia de medición	Registro
Porcentaje de cumplimiento del PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025	Garantizar la protección integral de los activos de información de la Empresa Regional Aguas del Tequendama S.A E.S.P., mediante la identificación, evaluación y tratamiento de los riesgos, implementando controles de seguridad efectivos que reduzcan la probabilidad de incidentes y mitiguen su impacto.	Eficacia	Cumplir con el **100%** de las actividades programadas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	**% Cumplimiento PTRSPI** = (Total de actividades del PTRSPI ejecutadas en el periodo / Total de actividades del PTRSPI programadas en el periodo) × 100	Mensual	Cronograma de actividades programadas versus ejecutadas con sus respectivos soportes.

Medición: La medición se realiza bajo las siguientes estrategias:

- Estrategia de identificación y evaluación de riesgos: Medir la capacidad para identificar, analizar y priorizar los riesgos asociados a la seguridad y privacidad de la información.
- Estrategia de implementación de controles de seguridad: Evaluar la efectividad de los controles implementados para mitigar los riesgos detectados y reducir la probabilidad de incidentes.
- Estrategia de monitoreo y respuesta ante incidentes: Medir la capacidad de respuesta y mitigación de impactos en caso de incidentes de seguridad.
- Estrategia de capacitación y concienciación: Evaluar el nivel de conocimiento y adopción de buenas prácticas en seguridad de la información por parte del personal.

Además, se adoptarán los estándares y mejores prácticas definidas en los marcos normativos y regulatorios aplicables para la gestión de la seguridad y privacidad de la información, alineándose con normativas nacionales e internacionales.

NELSON IVAN GARCIA TARQUINO
Gerente General
Empresa Regional Aguas del Tequendama S.A. E.S.P.

	Nombre	Cargo	Firma
Proyecto	Mauricio Sanchez Herrera	Profesional apoyo Sistemas	
Revisó	Dora Alicia Diaz Torres	Dir. Administrativa y Financiera	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a la norma y disposiciones legales y/o técnicas vigentes y, por tanto, bajo nuestra responsabilidad lo presentamos para la firma del remitente.			