Empresa Regional Aguas del Tequendama S.A. E.S.P.
Anapoima – La Mesa.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

La Mesa, enero de 2023

Sede Administrativa y PQR:
Diagonal 8 No. 1 – 37 Barrio Quintas de San Pablo
La Mesa, Cundinamarca. Teléfono 8471213
usuario@aguasdeltequendama.com
info@aguasdeltequendama.com

Oficina PGR Anapoima - Cundinamarca. Carrera 3 # 1- 41 Sur San José
Celular PGR 3142807615
pqranapoima@aguasdeltequendama.com
www.aguasdeltequendama.com

CONTENIDO

1. INTRODUCCIÓN

Con el fin de garantizar el manejo eficaz de la información con la cual trabaja la Empresa Regional Aguas del Tequendama S.A E.S.P por medio de los equipos, aplicaciones informáticas y demás medios con los cuales interactúan diariamente los funcionarios y usuarios en general, se hace necesario identificar y gestionar las actividades que se relacionan con la Seguridad de la Información.

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan todo el ciclo de vida del servicio.

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 de la Empresa Regional Aguas del Tequendama S.A E.S.P. 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.

En la actualidad, la seguridad en la información es una de las preocupaciones más grandes que puede llegar a tener una compañía, ya que se refiere a garantizar la calidad, disponibilidad, veracidad y confidencialidad de su activo más preciado: la información.

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

Hoy en día las empresas que manejen sistemas de información han generado la necesidad del aseguramiento de la información, generando políticas y controles, buscando garantizar la estabilidad y confiabilidad de la información, proyectándose ser reconocidas a nivel nacional como internacional, teniendo buena credibilidad y ubicándose siempre en los primeros lugares.

Teniendo en cuenta la obligatoriedad de cumplimiento de lo definido en la estrategia de Gobierno en Línea, y el conjunto de normativas que rigen al respecto, además de la situación actual del sistema de información y los servicios tecnológicos Empresa Regional Aguas del Tequendama S.A E.S.P., se hace

necesario levantar una línea de base sobre la cual se articulen diferentes esfuerzos encaminados a ofrecer la seguridad en la información, teniendo en cuenta las distintas amenazas y vulnerabilidades que pueden comprometer la integridad de los datos, en las redes, en los servicios y demás herramientas tecnológicas dispuestas para tal fin.

Es importante aclarar que este proyecto se encamina a formar las bases para una declaratoria de lineamientos progresivamente aplicables que vayan dando forma al Plan de Seguridad Informática partiendo desde las copias de seguridad, su protección, integralidad, restricción de acceso y demás elementos a tener en cuenta.

Los principales beneficiarios son en primera medida la Alta Dirección, ya que se ofrecerá disponibilidad y veracidad en la información que se usa para la toma de decisiones. Por otra parte, los usuarios finales del sistema de información que alimentan y requieren de agilidad y seguridad al momento de ingresar información que puede o no ser pública, a través de los servicios tecnológicos de la entidad.

2. PLATAFORMA ESTRATÉGICA

Misión

Prestar los Servicios Públicos de Acueducto, Alcantarillado y Aseo en los Municipios de La Mesa y Anapoima, aplicando como principios el compromiso y la eficiencia, contribuyendo al mejoramiento de la calidad de vida de nuestros usuarios.

Visión

En el año 2035, La Empresa Regional Aguas del Tequendama S.A. E.S.P, será una Empresa líder y reconocida en la prestación de los Servicios Públicos de Acueducto, Alcantarillado y Aseo, cumpliendo estándares de calidad, continuidad y eficiencia, siendo referente en la región aplicando políticas de protección ambiental y desarrollo sostenible.

3. PRINCIPIOS Y VALORES INSTITUCIONALES

- **RESPONSABILIDAD:** Es un valor ético que implica el compromiso de los directivos y funcionarios de La ERAT S.A E.S.P., en el cumplimiento de sus funciones y actividades establecidas en la normatividad vigente, en los estatutos de la empresa, en el reglamento interno de trabajo y en el código de ética encaminados a fortalecer la Misión de la empresa y satisfacer las expectativas de los grupos de interés: Clientes, accionistas, proveedores y sociedad en general y la conservación del medio ambiente.

- **TRABAJO EN EQUIPO:** Es un comportamiento pilar en La ERAT S.A E.S.P, que busca siempre el crecimiento personal, permitiendo así que sus funcionarios adopten conductas de armonía y trabajo en equipo para una vida laboral saludable.

- **EFICACIA Y EFICIENCIA**: Estamos dispuestos a cumplir oportunamente nuestro compromiso de prestar los servicios públicos de acueducto, alcantarillado, aseo y alumbrado públicos a la comunidad bajo los principios de austeridad, integridad racionalidad, honestidad y transparencia.

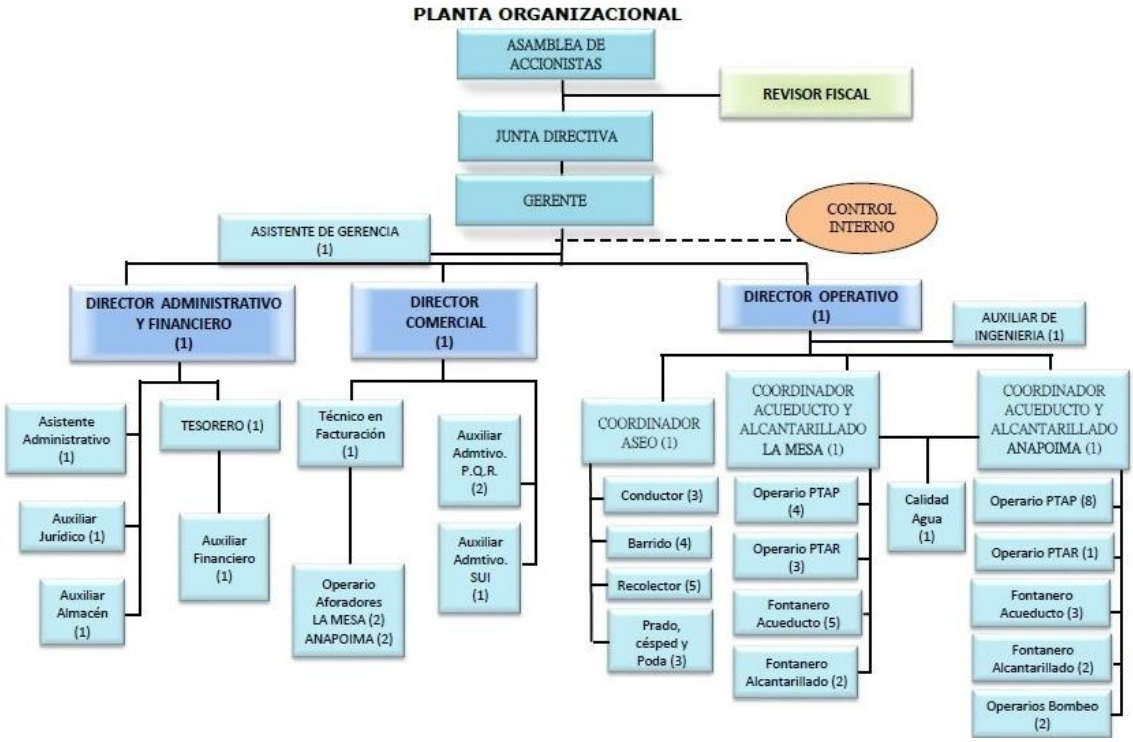
- **SENTIDO DE PERTENENCIA:** Es un comportamiento pilar en La ERAT S.A E.S.P, que busca siempre el crecimiento personal, permitiendo así que sus funcionarios adopten conductas de armonía y trabajo en equipo para una vida laboral saludable

- **LIDERAZGO:** Estamos comprometidos en dar ejemplo, influyendo positivamente en el trabajo de los demás, generando resultados exitosos.

- **CREATIVIDAD:** Nuestra capacidad de generar nuevas ideas, acciones y estrategias novedosas, nos permite transformar nuestro entorno por medios de soluciones originales a los problemas.

- **EXCELENCIA:** Perseguimos incasablemente el éxito en lo que hacemos, por lo que nos exigimos a diario para ofrecer un servicio con calidad.

4. ESTRUCTURA ORGANIZACIONAL



Descripción de la estructura orgánica

Empresa Regional Aguas del Tequendama S.A E.S.P

Asamblea de Accionistas: Órgano de administración y fiscalización dentro de la sociedad anónima, donde se toman las decisiones clave funcionamiento de la sociedad.

Revisor Fiscal: Delegatario de los socios para ejercer inspección permanente a la administración y validar los informes que está presente, debiendo rendir informes a los mismos en las reuniones estatutarias.

Gerente: Planear, organizar, integrar dirigir y controlar las actividades generales de la Empresa, velando por el cumplimiento de su plan estratégico, implementando herramientas administrativas, financieras y operativas que redunden en el desarrollo y optimización de la Empresa, en concordancia con sus planes administrativos y operativos, representando legalmente a la entidad ante los diferentes organismos de vigilancia, control y regulación.

Control Interno: Asesorar, dirigir, organizar, formular políticas y adoptar planes, programas y proyectos para la implementación y manejo adecuado del Sistema de Control Interno de la entidad.

Director Administrativo y Financiero: Planear, organizar, integrar dirigir y controlar las actividades administrativas y financieras de la Empresa, coordinando sus funciones con la Gerencia General y las demás Áreas, procurando la oportuna consecución y adecuado manejo custodia de los valores y medios de pago de la Empresa.

Director Comercial: Planear, organizar, integrar dirigir y controlar las actividades comerciales relacionadas con los procesos de facturación de la Empresa, coordinando sus funciones con la Gerencia General y demás Áreas.

Director Operativo: Planear, organizar, integrar dirigir y controlar las actividades técnicas y operativas de la Empresa, coordinando sus funciones con la Gerencia y las demás Áreas, ejecutando adecuadamente los procesos que garanticen la correcta prestación de los servicios de acueducto, alcantarillado y aseo a cargo de la Empresa.

5. OBJETIVO GENERAL

Establecer una guía metodológica para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información de la Empresa Regional Aguas del Tequendama S.A E.S.P 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.

6. OBJETIVOS ESPECÍFICOS

- Consolidar una administración de riesgos acorde con las necesidades de La ERAT S.A E.S.P.
- Proteger los activos de información de La ERAT S.A E.S.P., de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y disponibilidad.
- Crear compromiso en los usuarios del proceso en la Formulación y desarrollo del presente plan en aras de la prevención y administración del riesgo de seguridad de la información.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

7. ALCANCE

- La guía metodológica contempla la implementación y la administración de la gestión del tratamiento riesgo de seguridad de la información en la Empresa Regional Aguas del Tequendama S.A E.S.P, la cual será la pauta para desarrollar las actividades a través de la metodología PHVA (Planear – Hacer – Verificar - actuar) y las directrices de MINTIC.

- Lograr el compromiso de la Empresa Regional Aguas del Tequendama S.A E.S.P para emprender la implementación del plan de gestión del riesgo en la seguridad de la información.

- Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.

- Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

- La gestión de riesgos de seguridad de la información y su tratamiento, podrá será aplicada sobre cualquier proceso de La Empresa Regional Aguas del Tequendama S.A 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.

8. 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 (Stakeholder):** 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).

9. 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."

10. LAS RESPONSABILIDADES, LOS ROLES, LOS RECURSOS Y LA METODOLOGÍA DE LA GESTIÓN DEL RIESGO Y SEGURIDAD DE LA INFORMACIÓN.

LOS RESPONSABLES Y LOS ROLES

- **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.

11. 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.

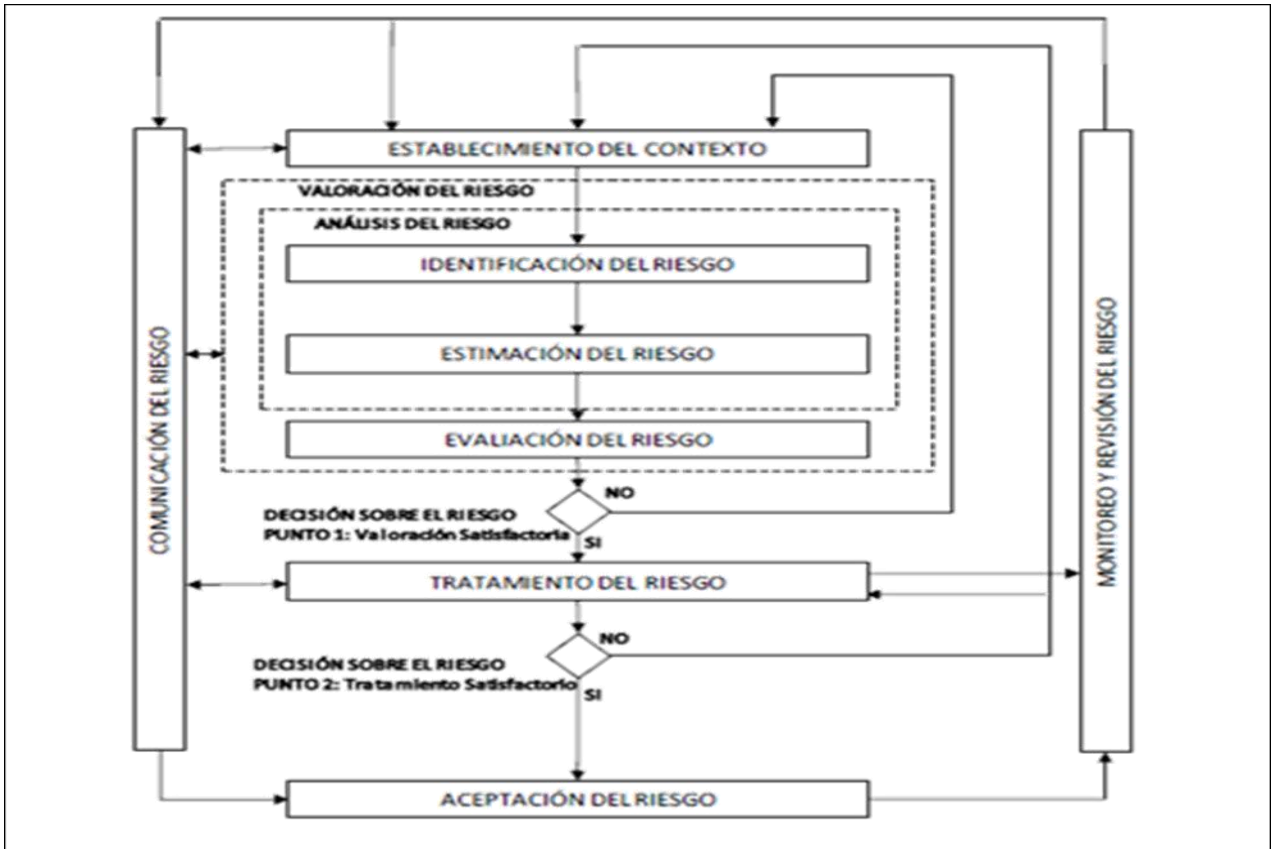
Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando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

12. 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

13. 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.

14. 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

15. 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.	

16. 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

17. 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 lamayoría de las circunstancias	Al menos de 1 vez en los últimos 5 años.
Probable	3	Significativa Probabilidad deOcurrencia	Al menos de 1 vez en los últimos 2 años.
Casi seguro	4	Se espera que suceda en la mayoríade las circunstancias	Más de 1 vez al año.

18. 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 mínimossobre la entidad y el proceso.
MODERADO	10	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectossobre la entidad y el proceso.
MAYOR	20	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobrela entidad y el proceso.
CATASTROFICO	40	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectossobre la entidad y el proceso.

19. 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.

20. CRONOGRAMA

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023												
ACTIVIDAD	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMPRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Realizar el Diagnostico												
Elaborar el alcance del plan de tratamiento de riesgo de seguridad y privacidad de la información												
Realizar la identificacion de los riesgos con los lideres del proceso												
Entrevista con los lideres del proceso												
Valoracion de los riesgos y los riesgos residuales												
Mapas de calor donde se ubican los riesgos												
Plantear el plan de tratamiento de riegos de seguridad												
Seguimiento y control												

21. SEGUIMIENTO Y EVALUACIÓN

Cada seis (6) meses Control Interno realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- **Cumplimiento de las políticas y directrices para la administración del riesgo:** metodología de Administración del Riesgo (diseño y funcionamiento).

- **Administración de los riesgos por proceso e institucionales:** calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

  Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

22. APROBACIÓN

	ELABORADO POR	REVISADO POR	APROBADO POR
Nombre	Daniel Felipe Suárez Montilla	Dora Alicia Díaz Torres	José William Tejedor Bayona
Cargo	Asesor MIPG	Directora Administrativa	Gerente
Firma	**FIRMADO EN ORIGINAL**	**FIRMADO EN ORIGINAL**	**FIRMADO EN ORIGINAL**
Fecha	31-01-2023	31-01-2023	31-01-2023