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

AGUAS DE BARRANCABERMEJA S.A. E.S.P.

2024-2027

Vigencia 2026

	ELABORADO POR	REVISADO POR	APROBADO POR
Firma			
Cargo	Profesional III Adscrito a la Subgerencia Administrativa y Financiera	Presidente Comité Institucional de Gestión y Desempeño	Presidente Comité Institucional de Coordinación de Control Interno
Nombre	Rafael Andres Lastre Gomez	Erika Osorio Cardona	Sandra Paola León Diaz
Fecha	Enero 2026	Acta No 1 del 22 de Enero de 2026 CIGyD	Acta No 1 del 28 Enero de 2026 CICCI

CONTROL DE CAMBIOS		
VERSION	**FECHA DE APROBACION**	**DESCRIPCION DEL CAMBIO**
1		Creación del Documento.

INTRODUCCIÓN

La Administración de Riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas, consecuencias de la materialización de dichos riesgos y los posibles controles que se puedan implementar para el tratamiento de dichos riesgos.

En este plan se pretende establecer las acciones de control que permitan una eficaz, eficiente y efectiva gestión del riesgo en el contexto de la seguridad y privacidad de la información, desde la identificación hasta el monitoreo; enfatizando en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y de lineamientos sencillos y claros para su adecuado tratamiento.

TABLA DE CONTENIDO

1. OBJETIVOS

1.1 Objetivo general

Definir las acciones necesarias que permitan la administración de los riesgos de seguridad y privacidad de la información contemplando: Identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo en la empresa Aguas de Barrancabermeja SA ESP.

1.2 Objetivos específicos

- Realizar un análisis y valoración de los riesgos de seguridad de la información identificados para determinar la medida a implementar que permita lograr un nivel aceptable del riesgo.
- Identificar las medidas de protección que contribuyan al correcto tratamiento de los riesgos a través de una adecuada selección y relación de controles.

2. ALCANCE

En este plan de tratamiento se cubrirán todos aquellos riesgos asociados a los activos de información de la empresa Aguas de Barrancabermeja SA ESP (desde la identificación hasta el tratamiento para su mitigación).

3. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

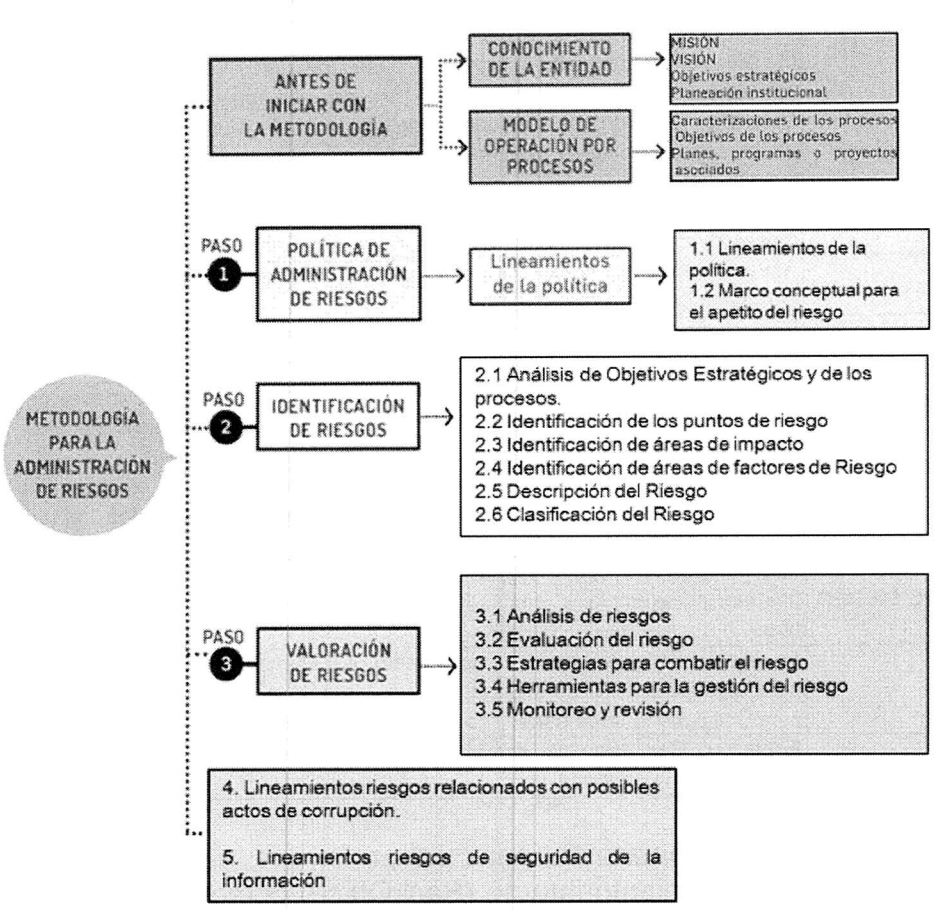
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

- **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- **Riesgo de corrupción:** posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional.
- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

4. TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para el tratamiento de los riesgos de seguridad y privacidad de la información se toma como base la estructura establecida por el DAFP "Guía para la Administración del Riesgo y el Diseño de Controles de las Entidades Públicas del DAFP v6" y Política para la gestión del Riesgo y Diseño de Controles vigente en nuestra entidad.

Figura 4 Metodología para la administración del riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Estructura que ha permitido la identificación y valoración inicial de riesgos, cuyo resultado es insumo principal para la formulación del Plan de Tratamiento de Riesgos de Seguridad Y Privacidad De La Información.

Es de anotar que para la identificación de los riesgos se tuvo en cuenta la identificación de los Activos de Seguridad Digital e información, entre los que se mencionan: aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información - TI- o Tecnologías de la Operación - TO-) que utiliza la empresa para su funcionamiento.

TIPO DE ACTIVO	DESCRIPCION
INFORMACIÓN	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
SOFTWARE	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
HARDWARE	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.
SERVICIOS	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
INTANGIBLES	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros.
COMPONENTES DE RED	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.
PERSONAS	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
INSTALACIONES	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Identificar los activos es importante para saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (Front Office).

En el cuadro siguiente se detallan las cuatro (4) fases a seguir del proceso del Modelo de Seguridad y Privacidad de la Información (MSPI) que son:

ETAPAS MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
PLANEAR	Establecer Contexto.
	Valoración del Riesgo.
	Planificación del Tratamiento del Riesgo.
IMPLEMENTAR	Implementación del Plan de Tratamiento de Riesgo
GESTIONAR	Monitoreo y Revisión Continuo de los Controles asociados a los Riesgos.
MEJORA CONTINUA	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

5. METODOLOGIA PARA LA IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

5.1 Seguimiento de los Lineamientos de la Política de Administración de Riesgos de la empresa

Para Aguas de Barrancabermeja S.A. E.S.P., la gestión del Riesgo es el proceso efectuado por la Gerencia, su equipo directivo y por todo el personal para proporcionar a la administración, un aseguramiento razonable con respecto al logro de los objetivos.

Así mismo, en relación con la gestión de los riesgos de seguridad digital y de seguridad de la información, la empresa ha designado como responsable de Seguridad Digital y Seguridad de la Información a la Subgerencia Administrativa y Financiera bajo la coordinación del Profesional III de Sistemas, líder del proceso Gestión Informática.

5.2 Actividades para la formulación e implementación del Plan de Tratamiento de Riesgos

1. Priorización de los riesgos a tratar (Valorar del riesgo y del riesgo residual)

2. Seguimiento y control a los riesgos asociados a la Seguridad y Privacidad de la información, una vez aplicados controles internos.

3. Evaluación de los riesgos (efectividad de los controles asociados a los posibles riesgos).

4. Formulación de las medidas a asumir frente a los riesgos

5. Implementación de medidas a seguir para el tratamiento de los riesgos asociados a la Seguridad y Privacidad de la información.

5.3 Cronograma de actividades

CRONOGRAMA DE ACTIVIDADES PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y DE LA INFORMACION																
ACTIVIDAD	Trimestres Vigencia 2024				Trimestres Vigencia 2025				Trimestres Vigencia 2026				Trimestres Vigencia 2027			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. Priorizacion de los riesgos a tratar (Valoracion del Riesgo y del Riesgo Residual)	X				X				X				X			
2. Seguimiento y control a los riesgos asociados a la seguridad y privacidad de la informacion, una vez aplicado los controles internos.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3. Evaluacion de los riesgos (Efectividad de los controles asociados a los posibles riesgos)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4. Formulacion de las medidas asumir frente a los riesgos	X				X				X				X			
5. Implementacion de las medidas a seguir para el tratamiento de los riesgos asociados a la seguridad y privacidad de la información.		X	X	X		X	X	X		X	X	X		X	X	X

5.4 Cumplimiento de Implementación

De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo con lo establecido por el Aguas de Barrancabermeja SA ESP.

- Revisión de la Política de Seguridad de la Información, incluida en el manual de Informática
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la parte operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

Con base en el resultado del análisis de riesgos de la información y con el fin de gestionar el riesgo residual, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de esta, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

6. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Para la elaboración del Plan de tratamiento de riesgos de seguridad y privacidad de la información se toma como base los riesgos identificados relacionados con la seguridad digital y de acuerdo con los dominios de establecidos en el cumplimiento de implementación se podrán seguir identificados los riesgos para ser tratados usando la metodología expuesta en este plan. Se identificaron los siguientes riesgos

IDENTIFICACIÓN DEL RIESGO												
						TIPO						CATEGORÍA
	PROCESO/ SUBPROCESO	IMPACTO	RIESGO	CAUSA INMEDIATA	CAUSA RAIZ	GESTIÓN	CORRUPCIÓN	SEGURIDAD DIGITAL	LABORATORIO	FISCAL		CLASIFICACIÓN DEL RIESGO
1	Gestión Informática	Afectación económica y reputacional	Pérdida de confidencialidad de los sistemas de información institucionales (comercial, financiero, nómina, orfeo, otros)	Incorrecta parametrización de los permisos sobre la información por un administrador del sistema o desarrollador de software				X				Ejecución y administración de procesos
2	Gestión Informática	Afectación económica y reputacional	Pérdida de confidencialidad de los equipos de cómputo	Acceso no autorizado al equipo de computo. Perdida o Robo del equipo de computo				X				Ejecución y administración de procesos
3	Gestión Informática	Afectación económica y reputacional	Pérdida de integridad de los sistemas de información institucionales (comercial, financiero, nómina, orfeo, otros)	Incorrecta administracion sobre la información. Incorrecta utilización de la plataforma tecnologica. Eliminacion o modificacion de la informacion por parte de un funcionario, contratista o tercero				X				Ejecución y administración de procesos
4	Gestión Informática	Afectación económica y reputacional	Pérdida de integridad de los componentes de red	Modificacion o eliminacion de configuraciones por administrador de red, funcionario o contratista				X				Ejecución y administración de procesos
5	Gestión Informática	Afectación económica y reputacional	Pérdida de disponibilidad de los sistemas de información institucionales (comercial, financiero, nómina, orfeo, otros)	Falla en funcionamiento del software o hardware				X				Fallas tecnológicas
6	Gestión Informática	Afectación económica y reputacional	Pérdida de disponibilidad de los componentes de red	Falla en funcionamiento del software o hardware				X				Fallas tecnológicas
7	Gestión Informática	Afectación económica y reputacional	Ataques informáticos internos/externos a la infraestructura tecnológica (páginas web, software misional, hardware, aplicaciones, equipos de comunicación, equipos de seguridad, red interna)	1. Vulnerabilidades técnicas sin conocer, uso de software desactualizado. 2. Falta de sensibilización del personal sobre ataques cibernéticos.				X				Usuarios, productos y prácticas Daños a activos fijos / eventos externos

De la identificación de los riesgos se prioriza cual es el riesgo que se va a minimizar en la vigencia 2026, del cual se determinó el riesgo de Realizar análisis de vulnerabilidades de los sistemas de información, Portal Web y servicios expuestos en Internet

6.1 CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – VIGENCIA 2026 –

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION																
ACTIVIDAD	Vigencia 2026															
	Pimer Trimestre				Segundo Trimestre				Tercer Trimetre				Cuarto Trimestre			
Riesgo 1. Realizar analisis de vulnerabilidades de los sistemas de información, Portal Web y servicios expuestos en Internet.	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Informe Analisis vulnerabilidades con recomendaciones para la mejora presentado en																
Jornada de sensibilizacion sobre buenas practicas organizaciónes para el uso de recursos compartidos																

CRONOGRAMA DE ACTIVIDADES DEL PLAN DE SEGURIDAD DE LA INFORMACION				
ACTIVIDAD	RECURSOS	PRESUPUESTO	AÑO	RESPONSABLE
Riesgo 1. Realizar análisis de vulnerabilidades de los sistemas de información, Portal Web y servicios expuestos en Internet	Humanos,	$0.00	2026	Profesional III

7. LÍNEAS DE DEFENSA

Para asegurar el cumplimento de las actividades del Plan de tratamiento de riesgos de seguridad de la información 2024-2027 se realizará en comité primario para la

primera línea de defensa y en CIGyD bajo el liderazgo de la Subgerencia de Planificación: Incluir dentro del Plan Acción Integrado de la empresa las actividades correspondientes a la vigencia para su ejecución durante el periodo establecido y el monitoreo por el área de planeación de manera trimestral con el fin de evaluar su cumplimiento y efectividad de la actividad estratégica establecida dentro del plan.

8. PUBLICACIÓN Y PARTICIPACIÓN CIUDADANA

Una vez aprobado el PETI por parte del comité Institucional de gestión y desempeño responsable de orientar la instrumentación del modelo integrado de planeación y gestión se procederá a socializar el plan con todos los funcionarios de la entidad.
Se hará difusión del Plan Tratamiento de Riesgos de Seguridad de la Información a través de página web institucional.

9. PUNTOS DE CONTROL

El profesional III monitoreara la matriz del plan de tratamiento de riesgos de seguridad de la información en el comité primario para la presentación de resultados previo a la presentación del comité de gestión y desempeño.