VIGENCIA 2026

Código TRD 1000.27.16.001-2026

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
VALLECAUCANA DE AGUAS S.A. E.S.P.
ENERO 2026

Tabla de contenido

INTRODUCCION

Todos los riesgos de seguridad en torno a las tecnologías se basan en la manipulación y tratamiento del recurso humano, esto debido a que se debe motivar en seguir la normatividad y los diferentes procedimientos que incurren en la seguridad y la privacidad de la formación, el cual se, les asigna teniendo en cuenta sus actividades y funciones dentro de la Entidad. La evaluación y seguimiento del presente plan se diseña y elabora mediante un proceso sistemático y con directrices de la metodología SGSI "Sistema de Gestión de Seguridad Informática" Norma ISO 27001.

El plan de tratamiento de riesgos e Seguridad y Privacidad de la Información Vallecaucana de Aguas S.A. E.S.P., es de gran importancia para la gestión del riesgo de la información y con esta herramienta los encargados de sistemas, tienen como principal alcance evitar y/o minimizar los riesgos que conllevan a procesos malintencionados que produzcan la pérdida o daño de los activos informáticos e la entidad. Por tal motivo, se crean pautas que permite garantizar que los tipos de riesgos de seguridad informática sean prevenidos y controlados eficientemente.

1 GENERALIDADES DE LA ENTIDAD

Misión:

Gestionar e implementar proyectos integrales de inversión regional y municipal sostenibles, que mejoren cobertura, calidad, continuidad, crecimiento y viabilidad empresarial de los servicios de agua potable, saneamiento básico y ambiental para el Departamento del Valle del Cauca, y sus actividades complementarias, de acuerdo con su conveniencia financiera y estratégica, generando rentabilidad sin detrimento de la calidad, para cumplir con su función social y contribuir a mejorar la calidad de vida de la comunidad, el desarrollo sostenible de la región y el bienestar de sus trabajadores.

Visión:

Ser la empresa Vallecaucana reconocida por el mayor impacto social en las condiciones de vida de los vallecaucanos, relacionadas con el sector de agua potable y saneamiento básico y el respeto por el medio ambiente.

Ser administrada con enfoque empresarial que la conduzca a lograr su sostenibilidad, rentabilidad y crecimiento dentro de un clima organizacional que propicie conductas éticas y actuaciones transparente, que genere en sus empleados sentido de pertenencia, desarrollo profesional y técnico.

2. OBJETIVO GENERAL:

Definir estrategia de trabajo para la gestión de riesgos de seguridad de la información digital que, permita mantener la integridad, confidencialidad y disponibilidad de la información mediante la gestión de riesgos asociados a los activos de información Institucional.

2.1. Objetivos específicos

- ✓ Identificar riesgos en cada uno de los procesos institucionales que afecten la información, basados en los activos de información reportados.
- ✓ Establecer e implementar controles específicos a través de planes.
- ✓ Reducir la probabilidad de materialización de los riesgos sobre los activos de información.
- ✓ Identificar las debilidades y amenazas que afecten los activos informáticos de la entidad
- ✓ Realizar seguimiento de los planes de manejo para el tratamiento de los riesgos

3. NORMATIVIDAD

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Decreto 1078 del 26 de mayo del 2015 "Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones"

- Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Resolución 500 del 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"

- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Departamento Administrativo de la Función Pública 2020.

- Guía de gestión del riesgo, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

- Modelo Nacional de Gestión de Riesgos de Seguridad Digital, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

- Guía de orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, territoriales y sector público, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013

- Norma Técnica Colombiana NTC-ISO 31000:2011
- CONPES 3854 de 2016. Política Nacional de Seguridad digital
- Ley 1581 de 2012, "por medio de la cual se dictan disposiciones para la protección de datos personales".

4. ALCANCES Y LIMITACIONES

4.1. Alcances

- ✓ Lograr el compromiso de Vallecaucana de Aguas 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.

4.1.2 Limitaciones

Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en Vallecaucana de Aguas S.A. E.S.P.

5. GESTIÓN DE RIESGOS

5.1 Importancia de la gestión del riesgo

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 Vallecaucana de Aguas 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.

5.1.2 Definición Gestión del Riesgo

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como "la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización".

5.1.3 Identificación del riesgo

Dentro de la entidad pública se puede presentar los siguientes riesgos:

I. **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico 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.

II. **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

III. **Riesgos 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 y de la articulación entre dependencias.

IV. **Riesgos 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.

V. **Riesgos 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 acuerdo con su misión.

VI. **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

5.1.4 Situación no deseada

- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión
- Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.
- Baja Cobertura de internet.
- Daño de equipos y de información
- Atrasos en la entrega de información
- Atrasos en asistencia técnica
- Fuga de información
- Manipulación indebida de información

6. IDENTIFICACIÓN DEL RIESGO

Dentro de la entidad pública se puede presentar los siguientes riesgos:

Riesgos Estratégicos	Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico 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
Riesgos de imagen	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
Riesgos Operativos	Comprenden riesgos provenientes dl 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 las dependencias.
Riesgos 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 cobre los bienes
Riesgos de Cumplimientos:	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 acuerdo con su misión.
Riesgos de Cumplimientos:	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 acuerdo con su misión.
Riesgos de Tecnología:	Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

6.1 Origen del plan de gestión de riesgos

Dar cumplimiento a los lineamientos de la política de gobierno digital, iniciando un proceso de modernización institucional que permita a Vallecaucana de Aguas S.A. E.S.P., implementar medidas para mitigar los riesgos presentes e inherentes al tratamiento de activos de información.

6.1.2 Propósito del plan de gestión de riesgo

- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

7. ANÁLISIS DE VULNERABILIDADES

7.1 Descripción de vulnerabilidades

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, Vallecaucana de Aguas S.A. E.S.P., se encontraron otras amenazas e impactos como los siguientes:

I. La red de internet implementada no es la más adecuada teniendo en cuenta que la mayor parte de EVA tiene conexión Wifi y la señal se torna débil o no llega a algunas oficinas. Debido a que la infraestructura física es amplia, compleja y la señal debe atravesar paredes. El internet lento y la perdida de señal afecta de forma directa los tiempos de producción laboral y desempeño de las funciones.

II. En el área técnica del tercer piso de EVA no hay aún puntos de red, y los ubicados en cada una no son suficientes. No existe una estructura o protocolo fijo y establecido para la infraestructura física de Vallecaucana de Aguas S.A. E.S.P.

III. En el área administrativa y técnica, algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.

IV. Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:

a. Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.
b. En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.
c. La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.
d. No hay control para el uso de memorias portátiles en los equipos de EVA, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

e. No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la entidad.
f. No existen procesos de copias de seguridad establecidos. Las copias de seguridad se están realizando en discos externo a cada computador requerido, se solicita habilitar un segundo servidor para que funcione como espejo para backup.
g. Esta solución no es óptima, ya que existe riesgo de pérdida total de información en caso de ocurrir desastres naturales, incendios u otros que afecten las copias de respaldo almacenadas en el servidor ubicado dentro de la misma entidad; se requiere servicio de backup en la nube.
h. No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de EVA. (en caso de incendio o desastre natural existen altas probabilidades de perder la información del servidor y equipos de cómputo)
i. EVA no cuenta con planta de energía, y cuenta con una UPS alquilada que tiene una duración máxima de unos 15 minutos; al no contar con ups instalada más potente y propia que respalden más tiempo tiende a perder información al momento que se han presentado cortes de energía suspendiendo los procesos laborales de todas las oficinas.

7.2 Matriz de vulnerabilidades y Mitigación del Riesgo

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACION	ANALISIS CALIFICACION	ANALISIS EVALUACION	VALORACIÓN - MITIGACION DEL RIESGO	VIGENCIA DE CUMPLIMIENTO
Fallas eléctricas	Las conexiones no son suficientes, no cumplen con las exigencias el tamaño de la red de equipos de cómputo (cables Sueltos, inadecuada estructura y adecuación)	Inadecuada conexión de cableado eléctrico	Posible pérdida de información	*Riesgo tecnológico *Riesgo físico *Riesgo humano	40	Riesgo moderado	Plantear un nuevo diseño de la red eléctrica	Año 2026
Afectación de activos de información y activos informáticos.	Desconocimiento de las políticas y normas de seguridad de la información.	No socialización No capacitación de las políticas y normas de seguridad.	Acciones no adecuadas en el tratamiento de los activos de información e informáticos	• Riesgo Tecnológico. Riesgo en Servicio. • Riesgo de la Información. • Riesgo en personal	60	Riesgo Alto	Diseñar, socializar e implementar un Manual de políticas y normas de seguridad de la información en la alcaldía municipal.	Año 2026
Pérdida de información *Pérdida de tiempo productivo en funciones laborales.	La red implementada no es la más adecuada para la estructura física de la alcaldía y la cantidad de equipos informáticos. Las fallas en la señal de internet son constantes.	Señal inalámbrica	Señal débil en las oficinas. Retraso en tiempos de producción para los funcionarios .	*Riesgo Tecnológico *Riesgo en Servicio *Riesgo de información	40	Riesgo Importante	Implantar un modelo de red basado en cableado estructurado.	Año 2026
Incumplimiento de las actividades de seguridad de la información.	El personal encargado de los sistemas no es suficiente. No se están siguiendo protocolos y normas para garantizar la seguridad de la información en la entidad.	No existe personal encargado del proceso de aseguramiento de la información	Ausencia de transferencia de conocimiento y falta de capacitación	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	60	Riesgo Alto	Encargar a personal capacitado para el aseguramiento de la información. Capacitar al personal de EVA para el cumplimiento de procesos y actividades de seguridad de la información	Año 2026

Confidencialidad e Integridad de la información	En la entidad se trabaja en la campaña cero papel, sin embargo se han encontrado dentro del papel reutilizable información personal de algunos pobladores del municipio beneficiarios de programas sociales.	Exposición de datos personales en papel reutilizable.	incumplimiento de confidencialidad e integridad de la información	*riesgo de Información	60	Riesgo Alto	Socializar con los funcionarios de la entidad acerca de las políticas de seguridad y confidencialidad de la información.	Año 2026
Pérdida total de Información	No se cuentan con los tipos de extintores adecuados para cada necesidad.	No se cuentan con los tipos de extintores adecuados para cada necesidad.	*No hay extintores *La planta de energía no funciona	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	60	Riesgo Alto	*Crear un instructivo de copias de seguridad *Capacitar al personal de la alcaldía municipal para el dominio de este tema. *Adquirir un servidor para almacenar las copias de seguridad. *Adquisición de una nube para almacenamiento de información. *Crear cuentas de usuario con claves.	Año 2026
Perdida de información	El DataCenter no cuenta con todas las especificaciones exigidas para el correcto funcionamiento y adecuación de un área de tal importancia.	Incendios, ingreso de personal no autorizado, posible robo de servidores,	Perdida de información por catástrofe o riesgo en manos	*Riesgo en Servicio *Riesgo en información	40	Riesgo Moderado	Adecuación del Datacenter de la alcaldía Municipal, cumpliendo con las características exigidas por normas y estándares en Colombia. (Piso falso, cámara de seguridad, extintores adecuados, entre otros)	Año 2026

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACION	ANALISIS CALIFICACION	ANALISIS - EVALUACION	VALORACIÓN - MITIGACION DEL RIESGO	VIGENCIA DE CUMPLIMIENTO
Perdida de la información y/o deterioro físico	La documentación en información en papel o física está siendo archivada en sitios no adecuados para ello.	No se ha iniciado la ejecución de la digitalización de la información	Daño de documentos y deterioro del papel	* Riesgo de información	40	Riesgo importante	Iniciar la ejecución de la digitalización y almacenamiento de la información contenida en papel.	Año 2026
No hay respaldo de información en sistemas de información	No existe un proceso establecido de copias de seguridad dentro y fuera de la entidad para la información generada en los sistemas de información. No Existe un sistema de información para la documentación sensible, como contratos y acuerdos.	No hay procesos de copias de seguridad establecidos	Perdida de información	*Riesgo Tecnológico *Riesgo de información	60	Riesgo Importante	*Crear procesos de copias de seguridad. *Invertir en un software o sistema de información para el almacenamiento y consulta de la documentación física existente en la alcaldía.	Año 2026
Transición IPv4 a IPv6	No existen transición de protocolo de IP	No existen transición de protocolo de IP	No existen transición de protocolo de IP	*Riesgo tecnológico	20	Riesgo Bajo	*establecer normas para la transición de IPv4 a IPv6 debido a que todos los equipos informáticos de la entidad soportan la nueva versión de IP	Año 2026

8. PROPUESTA DE SEGURIDAD

- ✓ Se debe cambiar la red inalámbrica actual por cableado estructurado, para minimizar el problema de internet lento y caídas de señal.
- ✓ Implementar un firewall para la red que se utiliza en EVA.
- ✓ Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de los computadores en cada piso.
- ✓ Replantear las políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.
- ✓ Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.
- ✓ Socializar las políticas de seguridad y privacidad de la información con el personal de EVA.
- ✓ Creación de cuentas de usuario y claves para tratar de mitigar los riesgos de pérdida de información en manos de otro funcionario que use el equipo compartido.
- ✓ El personal de sistemas puede crear las cuentas y claves, socializando al personal de EVA la creación de claves en forma correcta.
- ✓ Crear un rubro del presupuesto para la adquisición de la licencia del sistema ofimático Office para los equipos de la Alcaldía.
- ✓ Crear los procesos de la oficina de sistemas para la entidad.
- ✓ Implementar el sistema de documentación digital en EVA para reducir riesgos de pérdida de información física.
- ✓ Comprometer a la administración municipal con la campaña cero papeles.

8.2 Plan continuidad del negocio

I. Socializar con los directivos, secretaría general y oficina de Sistemas la importancia del Plan de Continuidad de Negocio, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.

II. Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.

III. Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

- Detectar el riesgo
- Plantear controles y efectuar las implementaciones respectivas.
- Mitigar el riesgo.

IV. Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:

- Política de copia de seguridad de datos
- Procedimientos de almacenamiento fuera de la alcaldía
- Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones.

MOISES CEPEDA RESTREPO
Gerente General
VALLECAUCANA DE AGUAS S.A. E.S.P.

Elaboró y proyectó: Jesús Migdonio Mosquera Mena, CPS Sistemas de Información.
Aprobó: Dr. Juan Facier Moerno Rivas– Director Administrativo.
Copia: Archivo.