Acueducto y Alcantarillado de Popayán S.A. E.S.P

DIVISION SISTEMAS
GESTION INFORMATICA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
ACTUALIZADO 2026

Contenido

INTRODUCCION

Hoy en día con la inclusión de las tecnologías de la información en cada proceso de las empresas aportando a su desarrollo y la importancia de tener la información adecuadamente identificada y segura para todos los involucrados, obligan todos a darle un adecuada tratamiento, manejo y clasificación bajo una correcta administración y conservación.

La protección de la información como un activo valioso ante las amenazas actuales que atentan contra los principios de confidencialidad, integridad, y disponibilidad con medidas de control de seguridad de la información que permitan gestionar los riesgos y los impactos que puedan generar.

OBJETIVO

Establecer las políticas, procedimientos y metodologías para identificar, analizar, valorar, monitorear, medir y controlar los riesgos de mayor probabilidad de ocurrencia que puedan afectar el cumplimiento de la Misión, y los Objetivos de los procesos del Sistema de Gestión de la Calidad (SGC).

METODOLOGIA PARA LA ADMINISTRACION DEL RIESGO

Términos y Definiciones

Consecuencia

Resultado de un evento expresado cuantitativa o cualitativamente, como por ejemplo una pérdida, lesión desventaja o ganancia. Puede haber una serie de resultados posibles asociados con un evento.

Evento

Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo particular.

Frecuencia

Medida de la tasa de ocurrencia de un evento, expresada como el número de ocurrencia de un evento en un tiempo determinado (véase posibilidad y probabilidad)

Posibilidad

Se emplea como una descripción cualitativa de la probabilidad o frecuencia.

Pérdida

Cualquier consecuencia negativa, financiera u otra.

Probabilidad

Posibilidad de que ocurra un evento o resultado específico, medida por la relación entre los eventos o resultados específicos y el número total de eventos y resultados posibles.

Riesgo

Posibilidad de que suceda algo que tendrá impacto en los objetivos. Se mide en términos de consecuencias y posibilidad de ocurrencia.

Análisis de riesgo

Uso sistemático de la información disponible, para determinar la frecuencia con la que pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

Valoración del riesgo

Proceso general de análisis del riesgo y evaluación del riesgo.

Evitar el riesgo

Decisión informada de no involucrarse en una situación de riesgo.

Identificación del riesgo

Proceso para determinar lo que puede suceder, por qué y cómo.

Gestión del riesgo

Cultura, procesos y estructuras que se dirigen hacia la gestión eficaz de las oportunidades potenciales y los efectos adversos.

Transferencia del riesgo

Traslado de la responsabilidad o carga por la pérdida a otra parte, por medio de la legislación, contratos, seguros u otros medios. La transferencia del riesgo también se puede referir al traslado de un riesgo físico o parte de mismo a cualquier otra parte.

Tratamiento del riesgo

Selección e implementación de las opciones apropiadas para ocuparse del riesgo.

ANÁLISIS DEL RIESGO

El análisis permite establecer un mejor entendimiento y comprensión del riesgo, al considerar las consecuencias, posibilidad (causas), el impacto en caso de que llegue a materializarse y la probabilidad (frecuencia) de ocurrencia. La metodología para un adecuado análisis del riesgo se lleva a cabo en las siguientes fases:

CONSECUENCIAS: *Una vez identificado el riesgo, se deben establecer las posibles consecuencias que se pueden presentar en caso de que el riesgo se materialice, es decir que se vuelva una situación real.*

POSIBILIDAD: *Posteriormente se deberá establecer la posibilidad o causa que origina la presencia del riesgo.*

CONTROLES EXISTENTES: *Establecida la posibilidad o causa, se deberán reconocer los controles existentes en la Empresa para mitigar o reducir el impacto del riesgo, es posible que no se cuente en el momento de la valoración con mecanismos de control asociados al riesgo, por lo tanto el impacto negativo para la consecución de los objetivos en caso de materializarse el riesgo será mayor.*

IMPACTO: *El impacto del riesgo se mide en términos de las consecuencias que pueda generar el riesgo en la consecución de los objetivos y se debe considerar la existencia o no de controles. Se puede dar una relación inversa entre el número de controles y las consecuencias del riesgo, es decir, que a mayor número de controles eficaces, menores serán las consecuencias del riesgo en caso de materializarse. Para la medición se definió la Tabla 1 IMPACTO donde se establecen rangos:*

Tabla 1 Impacto

Nivel	Descripción	Orientación o Características del Nivel
1	Insignificante	El riesgo no genera impacto negativo sobre los objetivos. Ningún daño, Sin pérdidas financieras. Sin impactos ambientales negativos. No se afecta la capacidad del proceso. No se ve afectada la facturación, la potabilización, la distribución o la recolección y el transporte de aguas servidas.
2	Menor	Efectos que no disminuyen la capacidad del proceso y que se remedian fácilmente. Sin Pérdidas financieras. Interrupción de la prestación del servicio por periodos cortos (Menores a 3 horas).
3	Moderado	Algunos objetivos o metas afectadas. Pérdidas financieras menores a 15 SMMLV. Se generan problemas o demoras para la facturación de un ciclo o parte de un ciclo. Interrupción de la prestación del servicio por periodos inferior a 6 horas.
4	Mayor	Algunos objetivos importantes no se pueden lograr. Pérdida financiera entre 16 y 50 SMMLV, pérdida de la capacidad de prestación del servicio. Interrupción de la prestación del servicio entre 6 y 24 horas. Retraso en la facturación de un ciclo completo. Deficiencias en el recaudo. Impactos Ambientales Negativos,
5	Catastrófico	Más del 50% de los objetivos o sus metas no se pueden lograr. Pérdida financiera mayor a 50 SMMLV Suspensión de la prestación del servicio por más de 24 horas. Incremento significativo de la cartera. Incremento del índice de Agua No Contabilizada IANC por encima del 50%.

PROBABILIDAD: *Se debe determina la Probabilidad de que ocurra un evento o resultado específico en términos de frecuencia (N° de veces), para ello se estableció la Tabla 2.*

Tabla 2 Probabilidad

Nivel	Descripción	Características
A	Casi Cierto	Se espera que ocurra en la mayoría de las circunstancias, varias veces en el semestre, varias veces durante un proyecto, en más de 4 ciclos de facturación. Interrupción del servicio más de 5 veces al mes en un mismo sector hidráulico o sanitario. Incremento sistemático (4 meses consecutivos) de la cartera, el IANC o el número de reformados por encima de las metas establecidas.
B	Probable	Se espera que ocurra en el año o durante el proyecto dos o tres veces. En 2 o 3 ciclos de facturación. Interrupción del servicio 3 o 4 veces al mes en un mismo sector hidráulico o sanitario. Incremento sistemático por encima de las metas establecidas durante 3 meses consecutivos de la cartera o el IANC
C	Posible	Puede ocurrir de vez en cuando o en algún lugar durante un proyecto, menos de tres veces al año o durante el proyecto.
D	Improbable	No se espera que ocurra durante el año, durante el proyecto o durante la consecución del objetivo.
E	Raro	Evento que puede ocurrir solamente en circunstancias excepcionales (una vez al año o más) durante el proyecto o la consecución del objetivo y que no genera impacto significativo sobre las metas propuestas.

NIVEL: *Para finalizar la etapa de análisis, se debe establecer el nivel del riesgo, es decir, confrontar el impacto contra la probabilidad de ocurrencia, esto se logra haciendo un cruce en la Matriz de Análisis Cualitativo del Riesgo.*

Prob.		Impacto				
		Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
Raro	A	B	B	M	A	A
Improbable	B	B	B	M	A	E
Posible	C	B	M	A	E	E
Probable	D	M	A	A	E	E
Casi Cierto	E	A	A	E	E	E

Una vez realizado el cruce, la Matriz establece un Nivel de Riesgo que se clasifica de la siguiente manera:

E:	Riesgo Extremo; se requiere acción inmediata
A:	Rieso Alto; Revisar o redefinir controles, opcional acciones preventivas
M:	Riego Moderado; Mantener controles, no requiere acciones preventivas.
B:	Riesto Bajo; gestionar mediante procedimientos de rutina

Etapas para la gestión de riesgos

Etapa de medición

PROBABILIDAD

Nivel		Descriptor	Orientación
	A	Raro	Evento que puede ocurrir solamente en circunstancias excepcionales (una vez cada 2 años) durante el proyecto o la consecución del objetivo y que no genera impacto significativo sobre las metas propuestas.
	B	Improbable	No se espera que ocurra durante el año, durante el proyecto o durante la consecución del objetivo. En caso de presentarse puede ocurrir máximo 1 vez al año durante el proyecto. Interrupción del servicio más de 10 veces al mes, en un mismo sector hidráulico o sanitario. Incumplimiento sistemático de proveedores (En cada pedido, en cada entrega, en cada obra).
	C	Posible	Puede ocurrir durante un proyecto entre 2 y 5 veces al año. En 2 ciclos de facturación. Interrupción del servicio 2 o 3 veces al mes en un mismo sector hidráulico o sanitario.
	D	Probable	Se espera que ocurra en el año o durante el proyecto (Entre 6 y 10 veces). En 3 o 4 ciclos de facturación. Interrupción del servicio 4 o 5 veces al mes en un mismo sector hidráulico o sanitario. Incremento sistemático de al Cartera o el IANC por encima de los rangos admisibles durante 3 meses consecutivos.
	E	Casi cierto	Se espera que ocurra en la mayoría de las circunstancias, varias veces en el año (Más de 10 veces) o varias veces durante un proyecto, en más de 4 ciclos de facturación. Interrupción del servicio más de 5 veces al mes en un mismo sector hidráulico o sanitario. Incremento sistemático (4 meses consecutivos) de la cartera, el IANC o el número de reformados por encima de los rangos admisibles o las metas establecidas por la empresa.

IMPACTO

Nivel	Descriptor	Orientación
1	Insignificante	El riesgo no genera impacto negativo sobre los objetivos. Ningún daño, sin pérdidas financieras. Sin impactos ambientales negativos. No se afecta la capacidad del proceso. No se ve afectada la facturación, la potabilizción, la distribución o la recolección y el transporte de aguas servidas. Caudal de captacion 850 lps
2	Menor	Efectos que no disminuyen la capacidad del proceso y que se remedian fácilmente. Sin Pérdidas financieras. Interrupción de la prestación del servicio por periodos cortos (Menores a 3 horas). Caudal de captación entre 800 y 850
3	Moderado	Algunos objetivos o metas afectadas. Pérdidas financieras menores a 15 SMMLV. Se generan problemas o demoras para la facturación de un ciclo o parte de un ciclo. Interrupción de la prestación del servicio por periodos inferior a 6 horas. Caudal de captacion entre 750 y 849 lps
4	Mayor	Algunos objetivos importantes no se pueden lograr. Pérdida financiera entre 16 y 50 SMMLV, pérdida de la capacidad de prestación del servicio. Interrupción de la prestación del servicios entre 6 y 24 horas. Retraso en la facturación de un ciclo completo. Deficiencias en el recaudo. Impactos Ambientales Negativos. Incremento del IANC hasta un 50%. Caudal de captación entre 500 y 749 lps
5	Catastrófico	Más del 50% de los objetivos o sus metas no se pueden lograr. Pérdida financiera mayor a 50 SMMLV. Suspensión de la prestación del servicio por más de 24 horas. Incremento significativo de la cartera. Incremento del índice de Agua No Contabilizada IANC por encima del 50%. Caudal de captación menor a 300 lps

IMPACTO

PROBABILIDAD

Prob.		Impacto				
		Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
Raro	A	B	B	M	A	A
Improbable	B	B	B	M	A	E
Posible	C	B	M	A	E	E
Probable	D	M	A	A	E	E
Casi Cierto	E	A	A	E	E	E

E:	RIESGO EXTREMO:	*Eliminar la actividad que lo genera en la medida de lo posible. Establecer el tratamiento mediante controles:* ***PREVENTIVOS*** *para evitar o disminuir la Probabilidad, o* ***DE PROTECCIÓN*** *para disminuir el Impacto, como compartir o transferir el Riesgo. Si durante la valoración del riesgo, el impacto ha sido calificado como Catastrófico, se deben elaborar Planes de Contingencia para protegerse de su ocurrencia. La División Control Interno debe realizar seguimiento a la ejecución de las acciones de tratamiento formuladas y a la aplicación de los controles definidos.*
A:	RIESGO ALTO:	*El tratamiento del riesgo es opcional. El responsable del proceso debe asegurarse que los controles identificados son efectivos y la División Control Interno debe establecer un seguimiento permanente al cumplimiento de los controles establecidos. Si durante la valoración del riesgo, el impacto ha sido calificado como Catastrófico, se deben elaborar Planes de Contingencia para protegerse de su ocurrencia.*
M:	RIESGO MODERADO:	*El nivel del riesgo Moderado y Bajo, es aceptable y la empresa lo puede Asumir mediante procedimientos de rutina y la aplicación continua de los controles ya establecidos.La División Control Interno debe establecer un seguimiento permanente al cumplimiento de los controles establecidos.*
B:	RIESGO BAJO:	

Etapa de control

Valoración de controles

La valoración de los controles se realiza respondiendo las siguientes preguntas:

VALORACIÓN GENERAL DEL CONTROL					
Existe?	Documentado?	Se aplica	Respon Aplicac	frecu. Adecua	Efectivo
5	5	20	5	15	50

Esta valoración busca disminuir la subjetividad en la evaluación del riesgo, de manera que se puede determinar si un control es efectivo o no; es importante en la medida que se disponga de datos numéricos relacionados con el riesgo, se utilicen de manera proporcional para valorar sobre todo la efectividad del riesgo

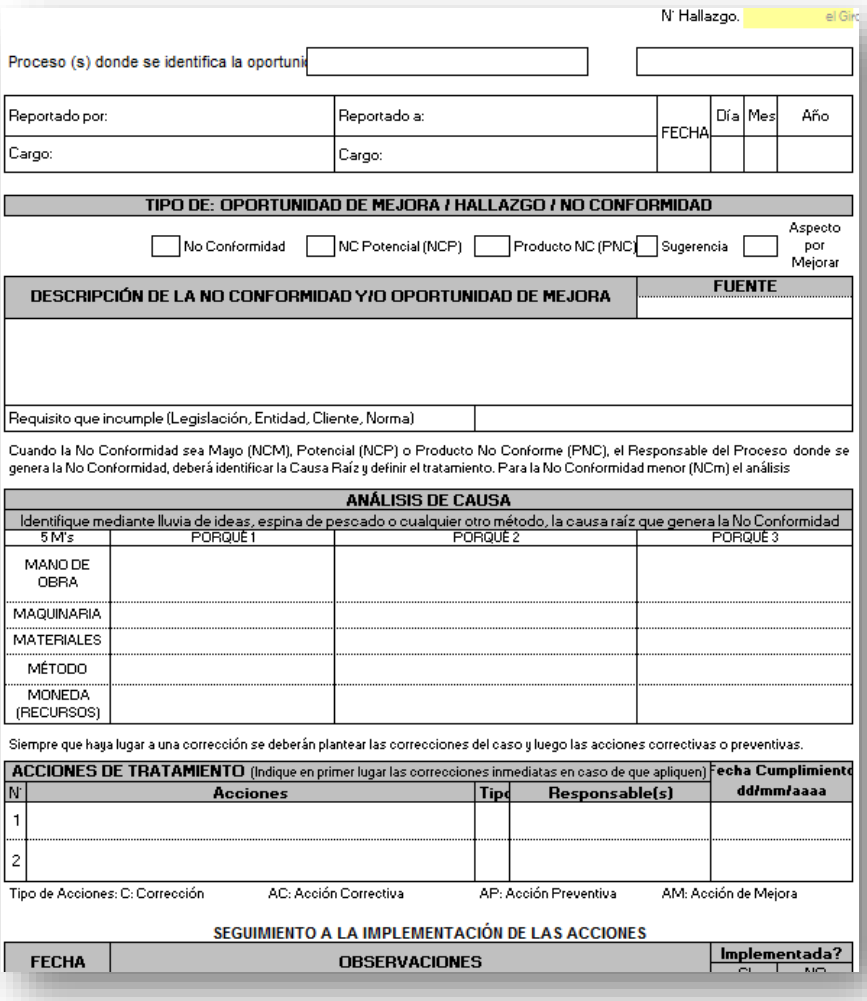
	VALORACIÓN GENERAL DEL CONTROL						ANÁLISIS		EVALUACIÓN	
VALORACIÓN	Existe?	Documentado?	Se aplica	Respon Aplicac	frecu. Adecua	Efectivo	Impacto	Probabilidad	NIVEL (E-A-M-B)	PRIORIDAD DEL RIESGO
Puntaje Total	5	5	20	5	15	50				
95	5	5	20	5	15	45				

usuario:
En 2013 Se redujeron en un 79.5% los Derechos de Petición respondidos por fuera de términos, se bajo de 49 en 2012 a 10 en 2013.
07/04/2015 En 2014 se redujero a 5 los DP que se respondieron por fuera de terminos. Se considera que las acciones y controles son 90% más efectivos, con relación a diciembre de 2012, fecha en la cual se identificó el riesgo.

Etapa de monitoreo

Tratamiento del riesgo

Según lo definido en la Política de Administración del Riesgo, se deben formular acciones preventivas para los riesgos que en durante la etapa de valoración su resultado sea Nivel Extremo y por lo tanto la prioridad para el tratamiento será la número 1; para los riesgos en los niveles Alto, Moderado o Bajo, la formulación de acciones preventivas será opcional.
El tratamiento del riesgo requiere la elaboración de acciones preventivas en el formato SOLICITUD ACCIÓN DE MEJORA.



N° Hallazgo.

Proceso (s) donde se identifica la oportuni

Reportado por:	Reportado a:	FECHA	Día	Mes	Año
Cargo:	Cargo:				

TIPO DE: OPORTUNIDAD DE MEJORA / HALLAZGO / NO CONFORMIDAD

☐ No Conformidad ☐ NC Potencial (NCP) ☐ Producto NC (PNC) ☐ Sugerencia ☐ Aspecto por Mejorar

DESCRIPCIÓN DE LA NO CONFORMIDAD Y/O OPORTUNIDAD DE MEJORA	FUENTE

Requisito que incumple (Legislación, Entidad, Cliente, Norma)

Cuando la No Conformidad sea Mayo (NCM), Potencial (NCP) o Producto No Conforme (PNC), el Responsable del Proceso donde se genera la No Conformidad, deberá identificar la Causa Raíz y definir el tratamiento. Para la No Conformidad menor (NCm) el análisis

ANÁLISIS DE CAUSA

Identifique mediante lluvia de ideas, espina de pescado o cualquier otro método, la causa raíz que genera la No Conformidad

5 M's	PORQUÉ 1	PORQUÉ 2	PORQUÉ 3
MANO DE OBRA			
MAQUINARIA			
MATERIALES			
MÉTODO			
MONEDA (RECURSOS)			

Siempre que haya lugar a una corrección se deberán plantear las correcciones del caso y luego las acciones correctivas o preventivas.

ACCIONES DE TRATAMIENTO (Indique en primer lugar las correcciones inmediatas en caso de que apliquen)

N°	Acciones	Tipo	Responsable(s)	Fecha Cumplimiento dd/mm/aaaa
1				
2				

Tipo de Acciones: C: Corrección AC: Acción Correctiva AP: Acción Preventiva AM: Acción de Mejora

SEGUIMIENTO A LA IMPLEMENTACIÓN DE LAS ACCIONES

FECHA	OBSERVACIONES	Implementada?

Seguimiento al plan de tratamiento del riesgo

Es necesario realizar seguimiento periódico a la eficacia, vigencia y conveniencia de las acciones implementadas para el tratamiento de los riesgos de TI, con el fin de determinar si el Plan continúa siendo pertinente o si requiere ajustes, fortalecimiento o la incorporación de nuevos controles tecnológicos más eficientes y acordes a las condiciones actuales del entorno digital.

Los factores que influyen en la probabilidad de ocurrencia y en el impacto de los riesgos de TI pueden cambiar debido a la evolución tecnológica, cambios en la infraestructura, actualizaciones de sistemas, modificaciones en los procesos o nuevas amenazas de ciberseguridad. En consecuencia, se debe reevaluar periódicamente el nivel de riesgo una vez implementadas las acciones definidas, considerando la necesidad de optimizar, automatizar o actualizar los controles existentes.

En la valoración de los controles asociados a los riesgos de TI, se debe establecer su frecuencia de aplicación, responsables, mecanismos de monitoreo y evidencias de cumplimiento, con el propósito de asegurar su correcta implementación y efectividad. Es importante señalar que los riesgos de TI no se eliminan por completo, ya que son inherentes al uso de la tecnología; sin embargo, es posible reducir su probabilidad de ocurrencia o su impacto mediante la aplicación continua, mejora progresiva y actualización de los controles.
El seguimiento a la implementación y efectividad de los controles de TI se realizará a través del formato SEGUIMIENTO CONTROLES ASOCIADOS AL RIESGO, y podrá ser efectuado por la División Control Interno y/o la Oficina de Calidad, en coordinación con la Division Sistemas de La Sociedad.

RIESGOS GESTION INFORMATICA

REF #	REQUISITOS DEL PROCESO	IDENTIFICACIÓN DEL RIESGO		
		EL RIESGO	POSIBILIDAD - CAUSA	CONSECUENCIAS
		Qué y cómo puede ocurrir	Por qué se presenta	
RGI1	Preservación de la información por desastres naturales	Posibilidad de daño de los sistemas de información por desastre natural (Terremoto, incendio, inundación, etc.), cortes de electricidad, fallos en el hardware, daño en el sistema de UPS y/o sus baterías, daño en el sistema de climatización.	Desastre natural. Fallas eléctricas. Intervención humana.	Interrupción de los procesos administrativos y operativos vinculados al sistema informático de la empresa. Daños y pérdida de equipos y aplicaciones. * Daños en las redes de comunicación.
RGI2	Preservación de la información ante amenazas externas	Posibilidad de indisponibilidad de los sistemas de información debido a fallas técnica que genere cortes de electricidad, fallos en el hardware, daño en el sistema de UPS, descarga de las baterías, mal funcionamiento del hardware, daño en el sistema de climatización del centro de datos.	Fallas eléctricas. Fallas Técnicas Intervención humana.	Interrupción de los procesos administrativos y operativos vinculados al sistema informático de la empresa.
RGI3	Controlar continuamente la seguridad de los servidores	Posibilidad de indisponibilidad de los sistemas de información por ataques cibernéticos de denegación de servicios (DDoS), daño y perdida en la comunicación entre equipos y servidores, que afecte la disponibilidad de los sistemas de información y sus bases de datos.	Ataques o denegación de servicios. Sabotaje o intervención humana	Vulnerabilidad del contenido de los sistemas de información y acceso libre a los procesos de los servidores.
RGI4	Preservación de la comunicación entre equipos	Posibilidad de acceso indebido a la plataforma tecnológica (Hardware, Software) de la empresa que pueda generar, perdida o alteración de la información ocasionadas por vulnerabilidades y que comprometa la seguridad, integridad, confidencialidad y disponibilidad de la información.	Robo, o secuestro de información. Sabotaje o intervención humana	Vulnerabilidad del contenido de los sistemas de información y acceso libre a los procesos de los servidores.