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

INTRODUCCIÓN

En la actualidad, el activo más importante de cualquier empresa es la información, es por ello, que es de vital importancia, velar por la seguridad y protección de este activo tan valioso, siendo este un recurso indispensable para el desarrollo y cumplimiento misional, y teniendo en cuenta que es de gran importancia protegerlo 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.

El presente documento identifica y recopila los riesgos a los que se encuentra expuesto la privacidad y la seguridad de la información, así como cuales deben ser los lineamientos a seguir, para tratar y prevenir estos riesgos, protegiendo así la seguridad y privacidad de la información que se maneja al interior de la Empresa de Acueducto de Alcantarillado y Aseo de El Espinal ESP.

OBJETIVO

Establecer las políticas, procedimientos y metodologías para identificar, analizar, valorar, monitorear, medir y controlar los riesgos de mayor probabilidad de ocurrencia, con el fin de proteger los activos de información, el manejo de medios, control de acceso y gestión de usuarios, que puedan afectar el cumplimiento de la misión, y los objetivos de La Empresa de Acueducto alcantarillado y Aseo de El Espinal ESP.

1. ALCANCE

Este plan se basa en las recomendaciones y definiciones que brinda la norma ISO 27005, y establece la metodología que se debe aplicar en la gestión de los riesgos que afecten la seguridad de la información, desde todos los procesos de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, orientando la ruta que se debe recorrer, desde el momento que se identifica un riesgo, hasta su monitoreo y control. De este modo, se busca que la gestión del riesgo sea un proceso continuo, y permita analizar lo que puede suceder y cuáles serían las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable (Icontec, 2008).

La aplicación de este documento obedece al interés por parte de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP. en diseñar, implementar y sostener el Sistema de Gestión de la Seguridad y privacidad de la Información –SGSI-, el cual deberá tener en cuenta y estar alineado con un Sistema Integrado de Gestión, en cada uno de sus componentes: Sistemas de Gestión de Calidad, Control Interno, Talento Humano y Asuntos Ambientales.

2. 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…) que tenga valor para la organización.

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Tecnología de la Información:** Se refiere al hardware y software operado por La Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP. o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la misma, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

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

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de La Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP..

- **Administración de Riesgos:** Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

- **Responsable de Seguridad Informática:** Es la persona profesional con experiencia en seguridad informática que cumple la función de supervisar el cumplimiento del presente documento y de asesorar en materia de seguridad de la información a todos los funcionarios de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP y contratistas que así lo requieran.

- **Incidente de Seguridad:** Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la entidad tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación.

- **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.

- **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.

- **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 consecuencias.

- **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, basándose en un enfoque de gestión y de mejora continua.

- **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 puede ser explotada por una o más amenazas.

3. OBJETIVOS

General

Establecer la metodología, que deben ser considerada para realizar un correcto tratamiento de los riesgos, que eventualmente pueden comprometer la seguridad de la información en la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, de acuerdo a un plan de gestión de la seguridad de la información y el establecimiento y uso de las políticas, las cuales se construyen a partir de los lineamientos propuestos por las normas técnicas NTCISO/IEC 27000, incluyendo 27005 para la gestión del riesgo en la seguridad de la información.

Específicos

- Capacitar a los funcionarios de la Empresa de la Acueducto Alcantarillado y Aseo de El Espinal ESP, desde la alta gerencia, hasta los funcionarios operativos, respecto a la importancia que tiene la gestión del riesgo en un Sistema de Gestión de la Seguridad de la Información, y la manera como estos se tratan una vez han sido identificados y evaluados.

- Involucrar a todas las partes interesadas, en la gestión activa de los riesgos documentados, asociados a la seguridad de la información.

- Divulgar y promover la aplicación consciente de las políticas de la seguridad de la información, generando una cultura organizacional, enfocada a fortalecer el entendimiento, que cada funcionario aporta a que el Sistema de Gestión de la Seguridad de la Información, fomentando la responsabilidad de hacerlo cumplir, en la ejecución de las actividades de su puesto de trabajo.

4. MATRIZ DE RIESGOS CRÍTICOS 2026

#	RIESGO	ACTIVO	PROB.	IMPACTO	RIESGO INICIAL	TRATAMIENTO	RIESGO RESIDUAL	RESPONSABLE
1	Caída GCI/GCIPRO	Sistema Comercial	Alta (4)	Catastrófico (5)	EXTREMO (20)	Backup diario	MODERADO (9)	Profesional Universitario - 219-03 - Gestión TIC
2	Ransomware	Servidores	Media (3)	Catastrófico (5)	ALTO (15)	Antivirus + parches	MODERADO (6)	Profesional Universitario - 219-03 - Gestión TIC
3	Phishing masivo	Usuarios	Alta (4)	Alto (4)	ALTO (16)	Capacitación + filtros	MODERADO (9)	Profesional Universitario - 219-03 - Gestión TIC + Admva.
4	Acceso no autorizado	Datos usuarios	Media (3)	Alto (4)	ALTO (12)	MFA + logs	BAJO (4)	Profesional Universitario - 219-03 - Gestión TIC
5	Falla Fortinet	Firewall	Media (3)	Alto (4)	ALTO (12)	Soporte + redundancia	MODERADO (6)	Profesional Universitario - 219-03 - Gestión TIC
6	Pérdida datos	Bases datos	Baja (2)	Catastrófico (5)	MODERADO (10)	Backup offsite	BAJO (4)	Profesional Universitario - 219-03 - Gestión TIC
7	Insider threat	Funcionarios	Media (3)	Medio (3)	MODERADO (9)	Políticas + auditoría	BAJO (4)	Comité Seguridad

#	RIESGO	ACTIVO	PROB.	IMPACTO	RIESGO INICIAL	TRATAMIENTO	RIESGO RESIDUAL	RESPONSABLE
8	DoS externo	Internet	Baja (2)	Medio (3)	MODERADO (6)	Monitoreo	BAJO (2)	Profesional Universitario - 219-03 - Gestión TIC
9	Falla UPS	Infraestructura	Baja (2)	Alto (4)	MODERADO (8)	Nuevo UPS	BAJO (2)	Recursos Físicos
10	Brecha Habeas Data	Datos personales	Media (3)	Medio (3)	MODERADO (9)	PPDP actualizado	BAJO (4)	Jurídica + TIC

5. PLAN DE ACCIÓN TRATAMIENTO RIESGOS 2026

RIESGO	ACCIÓN	FECHA	RESPONSABLE	INDICADOR
1. GCI caído	Implementar DRP probado	31/12/2026	Profesional Universitario - 219-03 - Gestión TIC	RTO ≤4h
2. Ransomware	Antivirus empresarial + parches auto	30/08/2026	Profesional Universitario - 219-03 - Gestión TIC	0 infecciones
3. Phishing	3 capacitaciones + filtros email	30/11/2026	Profesional Universitario - 219-03 - Gestión TIC	90% capacitados
4. Acceso no auth.	MFA GCI + logs auditables	31/12/2026	Profesional Universitario -	100% MFA

			219-03 - Gestión TIC	
5. Falla Fortinet	Contrato soporte 24/7	30/08/2026	Profesional Universitario - 219-03 - Gestión TIC	99% uptime
6. Pérdida datos	Backup offsite + pruebas	31/08/2026	Profesional Universitario - 219-03 - Gestión TIC	100% éxito backup
7. Insider	Auditoría accesos trimestral	15/12/2026	Comité Seguridad	0 accesos anómalos
8. DoS	Monitoreo proactivo	30/09/2026	Profesional Universitario - 219-03 - Gestión TIC	0 interrupciones
9. UPS	Mantenimiento UPS	31/10/2026	Profesional Universitario - 219-03 - Gestión TIC	100% cobertura
10. Habeas Data	PPDP actualizado	30/06/2026	Jurídica+TIC	100% cumplimiento

6. ROLES Y RESPONSABILIDADES

Para la Acueducto Alcantarillado y Aseo de El Espinal ESP, es importante que la gestión del riesgo se realice de forma sistemática y comprometida por parte de la alta dirección, funcionarios públicos, oficiales y contratistas, los cuales, se describen a continuación de forma general:

- **Alta dirección:** Por medio del Comité Institucional de Gestión y Desempeño, con funciones de comité de seguridad de la información, define el apetito del riesgo de seguridad de la información de la Acueducto Alcantarillado y Aseo de El Espinal ESP, y responde por el fortalecimiento de las políticas de seguridad de la información.

- **Directores de área:** Identifican, estiman, evalúan, valoran y monitorean los riesgos de seguridad de la información en su proceso, al menos una vez por año, y se responsabilizan de hacer cumplir las políticas de seguridad de la información, general y específicas, dentro del marco de su proceso, garantizando la interiorización del Sistema de Gestión de Seguridad de la Información, por parte de cada uno de los funcionarios que hace parte de su proceso.

- **Funcionarios públicos, oficiales y contratistas:** Son responsables de ejecutar los controles sobre los riesgos establecidos en las políticas de seguridad de la información. Son responsables de garantizar, dentro del alcance de la ejecución de sus actividades, que se cumplan los lineamientos de seguridad.

- **Gestión Control**: Realiza seguimiento y control sobre las políticas de seguridad de la información, y sobre la idoneidad de los controles asociados a la gestión de los riesgos.

7. Pasos para un adecuado Gestión del Riesgo en Seguridad de la Información

Los siguientes, son los componentes del proceso gestión del riesgo en Seguridad de la Información, los cuales hacen parte del Sistema de Gestión de la Seguridad de la Información.

Planificar:

- Identificar cual es ámbito de aplicación mediante el establecimiento del contexto.

- Aplicar los conceptos para la valoración del riesgo.

- Establecer y planificar el tratamiento del riesgo.

- Aceptación del riesgo y de sus consecuencias.

Hacer

- Implementar el plan de tratamiento del riesgo.

Verificar

- Monitorear y revisar continuamente los riesgos, su tratamiento, controles existentes y ejecución de indicadores.

Actuar

- Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

8. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

8.1 Establecer Contexto

Como parte fundamental del Sistema de Gestión Integrado, el Sistema de Gestión de la Seguridad de la Información, requiere un reconocimiento del contexto estratégico, asociado a lo que podría eventualmente comprometer la seguridad de la información.

Para esto, es importante que cada área de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, considere los siguientes elementos:

- Identificar los funcionarios, que, por sus responsabilidades, pueden tener mayor responsabilidad en el aseguramiento de la información, garantizando, dentro de su alcance, la confidencialidad, disponibilidad e integridad de la misma.
- Establecer los factores tanto internos como externos, que afectan la seguridad de la información en el proceso, y plasmarlo en la matriz Identificación de Amenazas y Vulnerabilidades de Seguridad de la Información.

8.2 Identificación de los Riesgos

Es la etapa que permite conocer los eventos potenciales, estén o no bajo el control de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, que pueden llegar a generar una pérdida de información. Para esto, es importante que cada proceso considere los siguientes elementos:

- Identificar los activos, y realizar el respectivo registro en el documento Inventario de Activos de Información

- Identificar las amenazas asociadas y sus orígenes según el activo de información identificado y registrarlas en documento Inventario de Activos de Información.

- Identificar los controles existentes, de modo que no exista una duplicidad, realizando una validación de suficiencia de cobertura de los mismos, en los riesgos en los cuales se están aplicando.

- Realizar un análisis de vulnerabilidades para cada uno de los procesos y registrarlo en el mapa de riesgos.

- Identificar las consecuencias de la materialización de cada riesgo, y registrarla en el mapa de riesgos.

8.3 Análisis del Riesgo

El análisis del riesgo se puede realizar dependiendo de la relevancia que puede presentar cada activo, la amplitud de las vulnerabilidades conocidas y los incidentes anteriores que implicaron en la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.

Para el caso de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, el análisis de riesgo asociado a la Seguridad de la Información, se plantea en las siguientes etapas:

8.4 Evaluación del Riesgo

Se realiza mediante la medición de la probabilidad y el impacto del riesgo.

PROBABILIDAD

Tabla Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

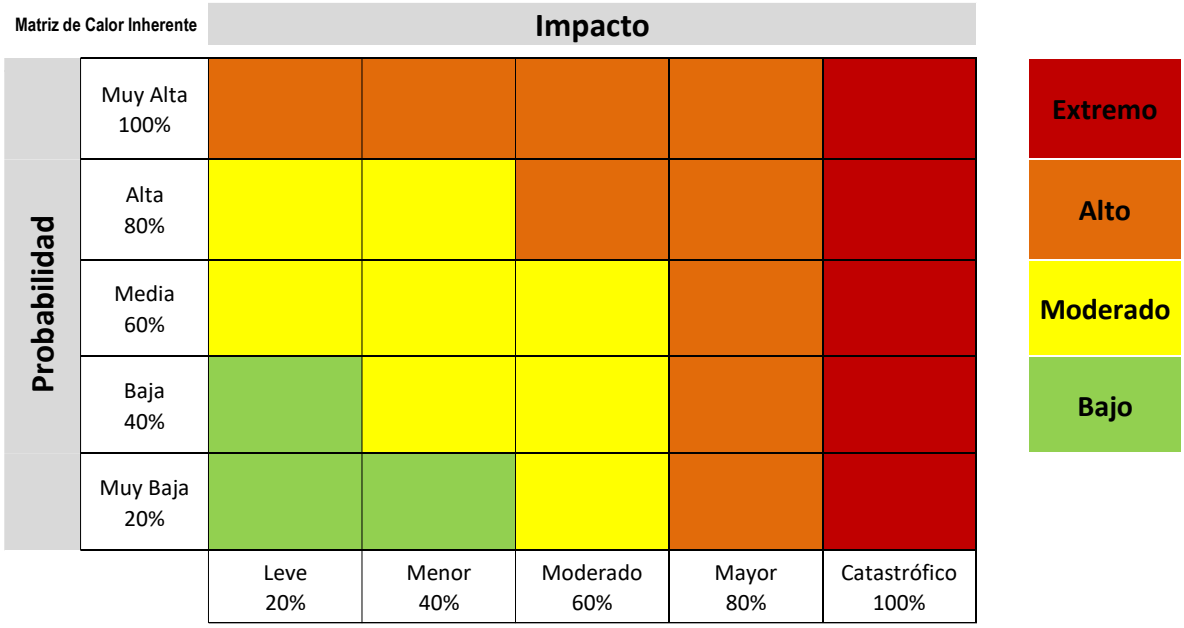
IMPACTO

Tabla Criterios para definir el nivel de impacto

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o de provedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país

8.5 Calificación del Riesgo

La calificación del riesgo se basa en el resultado del producto entre la probabilidad y el impacto. Para obtener estos valores, se deben tener en cuenta las siguientes escalas



8.6 Valoración del Riesgo

VALOR	CALIFICACIÓN	ACCIONES A TOMAR
E:	RIESGO EXTREMO	Eliminar la actividad que lo genera en la medida de lo posible. Establecer el tratamiento mediante controles: 9 **PREVENTIVOS** para evitar o disminuir la Probabilidad. 10 **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 oficina de Control Interno de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, 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 oficina de Control Interno de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, debe establecer un seguimiento permanente al cumplimiento de los controles establecidos.
B:	RIESGO BAJO	

8.7 Controles

8.7.1 Identificación de Controles

Los controles, son aquellas acciones que se ejecutan con el objetivo de prevenir la materialización de un riesgo, o en su defecto para minimizar el impacto de un riesgo que se ha materializado. Basado en esto, se debe considerar, que un control de cumplir con ciertas características, más aún cuando estamos tratando riesgos de seguridad de la información.

A continuación, se detallan las características principales que deben considerarse, para la identificación de los controles, que se deben ajustar a las posibles causas y consecuencias de la materialización de un riesgo que se pueda presentar en la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.

Característica	Descripción
Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener.
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo.
Realizables	Se deben definir controles que la entidad o el proceso este en capacidad de llevar a cabo.
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad.
Periódicos	Tienen frecuencia de aplicación en el tiempo.
Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo.
Asignables	Tienen responsables definidos para su ejecución.

8.7.2 Evaluación de los Controles.

Permite determinar, si los controles realmente permiten disminuir el riesgo o sus impactos, debe aplicarse a cada uno de los controles identificados.

Tabla Atributos de para el diseño del control

Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
*Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con Registro	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

*Nota 1: Los atributos de formalización se recogerán de manera informativa, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad.

CONTROL DE CAMBIOS

FECHA	DESCRIPCIÓN DEL CAMBIO	VERSIÓN
2023/01/02	Emisión original del documento	01
2024/01/16	Actualización de información para vigencia 2024	02
2025/01/07	Actualización de información para vigencia 2025	03
2026/01/19	Actualización de información para vigencia 2026	04