ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA RECREACION Y DEPORTE
Instituto Distrital de las Artes

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GTI-P-01

V.9

26/01/2026

Instituto Distrital de las Artes -IDARTES-
Carrera 8 No. 15 - 46 - Bogotá
+57 (601) 379 5750
Código postal: 111711

BOGOTÁ

TABLA DE CONTENIDO

TABLA DE TABLAS

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad, Perdida de Integridad y Perdida de Disponibilidad) de los activos de información y recursos tecnológicos, evitando aquellas situaciones que impidan el logro de los objetivos estratégicos del IDARTES, por esta razón, se genera el Plan de Tratamiento de Riesgo con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la acción, objetivo, justificación, responsable y su prioridad, el IDARTES define medidas que serán aplicadas en la vigencia 2026.

Las anteriores medidas se definieron teniendo en cuenta la información del análisis de riesgos, el cual brindó información acerca de las necesidades del Proceso de Gestión de Tecnologías de la Información en cuanto a la seguridad de la información y proporcionó las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

1. OBJETIVO

Definir y aplicar lineamientos integrales para gestionar los riesgos asociados a la Seguridad y Privacidad de la Información, así como a la Seguridad Digital, a los que pueda estar expuesto el IDARTES. Esto permitirá alcanzar los objetivos, la misión y la visión institucional, garantizando la protección y preservación de la integridad, confidencialidad, disponibilidad y autenticidad de la información.

Establecer y aplicar lineamientos integrales para la gestión de los riesgos relacionados con la Seguridad y Privacidad de la Información, así como con la Seguridad Digital, a los que pueda estar expuesto el IDARTES. Estos lineamientos contribuirán al cumplimiento de los objetivos, la misión y la visión Institucional, asegurando la protección y preservación de la integridad, confidencialidad, disponibilidad y autenticidad de la información.

2. ALCANCE

Implementar una gestión eficiente de los riesgos asociados a la Seguridad y Privacidad de la Información, así como a la Seguridad Digital, que permita incorporar buenas prácticas en los procesos de la entidad. Esto contribuirá a prevenir incidentes que puedan comprometer el logro de los objetivos estratégicos del IDARTES. Esta gestión estará alineada con un enfoque integral de tratamiento de riesgos, que incluye lineamientos para identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la entidad. El Plan de Tratamiento de Riesgos considerará los riesgos presentes en los diferentes niveles y activos de información, de acuerdo con los lineamientos establecidos por el IDARTES.

3. METODOLOGÍA

La gestión del riesgo es un proceso iterativo que apoya a la entidad en el establecimiento de su estrategia, el logro de sus objetivos y la toma de decisiones informadas. Al estar integrada en la gobernanza y el liderazgo, se considera una herramienta fundamental para la administración de la entidad, contribuyendo a la mejora continua de los sistemas de gestión de TI.

El análisis de riesgos abarca todas las actividades relacionadas con la entidad e implica la interacción con las partes interesadas. Este análisis tiene en cuenta los contextos externo e interno de la entidad, incluyendo factores como el comportamiento humano y otros elementos relevantes.

Es importante señalar que la gestión de los riesgos de seguridad de la información se llevará a cabo conforme a los lineamientos establecidos por la Oficina Asesora de Planeación y Tecnologías de la Información-OAPTI en esta materia, los cuales estarán alineados con las directrices del Departamento Administrativo de la Función Pública.

4. RESPONSABLES

Oficina Asesora de Planeación y Tecnologías de la Información – OAPTI.

5. DEFINICIONES

Directrices

- Riesgo es el efecto de la incertidumbre sobre el logro de los objetivos, es la probabilidad de que suceda algún tipo de evento que impacte o tenga consecuencias a los objetivos organizacionales o de los procesos.
- La valoración del riesgo se percibe como una amenaza, en este sentido, los esfuerzos organizacionales se deben dirigir a reducir, mitigar o eliminar su ocurrencia.
- Existe también la percepción del riesgo como una oportunidad, lo cual implica que su gestión está dirigida a maximizar los resultados que éstos generan

Administración del riesgo

- Un proceso efectuado por la alta dirección y por todo el personal para proporcionar a la organización un aseguramiento razonable con respecto al logro de los objetivos.
- El enfoque de riesgos no se determina solamente con el uso de una metodología, sino logrando que la evaluación de los riesgos se convierta en una parte habitual de los procesos de planificación y operación de la organización.

Conceptos aplicados

Tabla 1. Conceptos aplicados

CONCEPTO	DESCRIPCIÓN
Auditoría	Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que

	se cumplen los criterios de auditoría. (ISO/IEC 27000).
Autorización	Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
Apetito de riesgo	Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
Bases de Datos Personales	Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
Capacidad de riesgo	Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

CONCEPTO	DESCRIPCIÓN
Causa	todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Causa Inmediata	Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo
Causa Raíz	Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.
Ciberseguridad	Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
Ciberespacio	Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
Confidencialidad	Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados
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.
Consecuencia	Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
Datos Abiertos	Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
Datos Personales	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
Datos Personales Públicos	Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias

	judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3) .
Datos Personales Privados	Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
Datos Personales Mixtos	Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
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. (Decreto 1377 de 2013, art 3)
Derecho a la Intimidad	Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural

CONCEPTO	DESCRIPCIÓN
	(Jurisprudencia Corte Constitucional).
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.
Encargado del Tratamiento de Datos	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).
Evento	Ocurrencia o cambio de un conjunto particular de circunstancias: Un evento puede tener más de una ocurrencia y puede tener varias causas y varias consecuencias. Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre. Un evento puede ser una fuente de riesgo.
Fuente de riesgo	Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.
Factores de Riesgo	Son las fuentes generadoras de riesgos.
Gestión del riesgo	Actividades definidas para dirigir y controlar una organización con respecto al riesgo
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. (ISO/IEC 27000).
Incertidumbre	Es el desconocimiento si un hecho o situación ocurrirá.
Información Pública Clasificada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
Información	Es aquella información que estando en poder o custodia de un sujeto obligado

Pública Reservada	en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
Integridad	Propiedad de exactitud y completitud.
Impacto	Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
Ley de Habeas Data	Se refiere a la Ley Estatutaria 1266 de 2008.
Ley de Transparencia y Acceso a la Información Pública	Se refiere a la Ley Estatutaria 1712 de 2014.
Mecanismos de protección de datos personales	Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimizarían o cifrado.
Nivel de riesgo	Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser: Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

CONCEPTO	DESCRIPCIÓN
Plan de continuidad del negocio	Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
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. (ISO/IEC 27000).
Principios	El propósito de la gestión del riesgo es la creación y la protección del valor. Mejora el desempeño, fomenta la innovación y contribuye al logro de objetivos
Probabilidad	Es la probabilidad que algo suceda en un determinado tiempo
Registro Nacional de Bases de Datos	Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25) .
Responsabilidad Demostrada	Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
Responsable del Tratamiento de Datos	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. (Ley 1581 de 2012, art. 3).
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. (ISO/IEC 27000).

Riesgo de Seguridad de la Información	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. (ISO/IEC 27000)
Riesgo de Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado
Seguridad de la información	Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
Seguridad digital	Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
Titulares de la información	Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
Tolerancia del riesgo	Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
Tratamiento de Datos Personales	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
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. (ISO/IEC 27000).
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
Partes interesadas	Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
Riesgo inherente	Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
Riesgo residual	Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo. Es aquel que subsiste, después de haber implementado controles.

6. CONDICIONES GENERALES

- Proporcionar mecanismos, lineamientos e instrumentos de implementación para adoptar, implementar y apropiar el Modelo de Seguridad y Privacidad de la Información.
- Aportar en el desarrollo e implementación de la estrategia de seguridad digital de la Entidad.
- Establecer procedimientos de seguridad que permita a la Entidad apropiar el habilitador de seguridad en la política de Gobierno Digital.
- Institucionalizar la seguridad y privacidad de la información en los procesos y procedimientos de la Entidad.
- Mediante la implementación eficiente, eficaz y efectiva del MSPI, se busca contribuir al incremento de la transparencia en la gestión pública.
- Contribuir en el desarrollo y ejecución del plan estratégico institucional, a través del plan de seguridad y privacidad de la información y el plan de tratamiento de riesgos de seguridad y privacidad de la información.

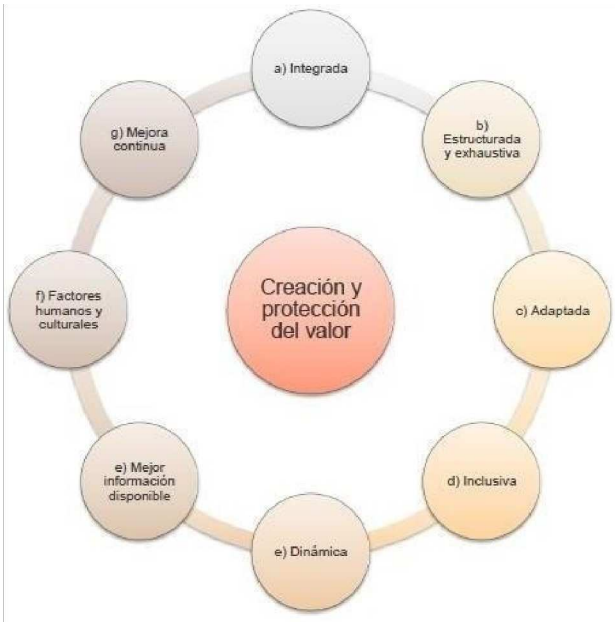

Ilustración 1. Principios. Norma ISO 31000:2018

Tabla 2. Principios de la gestión de riesgos

Principios de la gestión de riesgos	
Integrada	La gestión del riesgo es parte integral de todas las actividades de la organización.
Estructurada y exhaustiva	Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.
Adaptada	El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la entidad relacionados con sus objetivos.
Inclusiva	La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones.
Dinámica	Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la entidad. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
Mejor Información Disponible	Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras.
Factor humano	El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
Mejora continua	La gestión del riesgo mejora continuamente mediante el aprendizaje y experiencia.

Tabla 3. Objetivos del análisis y gestión de los riesgos

Objetivos del análisis y gestión de los riesgos	
Crear valor y proteger	Contribuye a la consecución de los objetivos demostrables y la mejora del rendimiento
Ser parte integral del proceso	Forma parte de las responsabilidades de gestión y de los procesos.
Apoyo para la toma de decisiones	Ayuda a tomar decisiones y priorizar acciones.
Contemplar la explícitamente incertidumbre.	La incertidumbre y su naturaleza
Aportar a la mejora continua de la organización	Mejorar su grado de madurez de gestión de riesgos

7. MARCO DE REFERENCIA

7.1 Generalidades

El IDARTES emplea como marcos de referencia la Guía para la Gestión del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por MinTIC, las Normas Técnicas Colombianas NTC-ISO 31000 y NTCISO 27005, así como el inventario de activos de información.

7.2 Roles y responsabilidades

La gestión del riesgo se desarrolla bajo el esquema de líneas de defensa, modelo de control que establece y clasifica los roles y responsabilidades de todos los actores del riesgo, para proporcionar aseguramiento de la gestión y prevenir la materialización de los riesgos, los roles establecidos son:

7.3 Línea Estratégica

- Primera Línea de Defensa
- Segunda Línea de Defensa
- Tercera Línea de Defensa.

Tabla 4. Líneas estratégicas

Línea de defensa	Rol	Responsabilidad
Línea Estratégica	Alta Gerencia	Revisar los cambios en el direccionamiento estratégico del contexto y dar las directrices para evaluar la necesidad de actualizar los documentos de riesgos de la entidad.
		Solicitar a los responsables de los procesos la revisión de los riesgos y el seguimiento de las acciones de control

Línea de defensa	Rol	Responsabilidad
		Revisar los informes emitidos por las unidades de gestión encargadas de la evaluación y control, sobre los resultados de las acciones para el tratamiento de riesgos.
		Hacer seguimiento a las acciones de tratamiento de los riesgos para garantizar el cumplimiento de las líneas y que los procesos tomen acciones de mejora continua.
Primera línea	Responsable del proceso de tecnología de la información	Apropiar documentos al interior del proceso con el fin de determinar actividades de control.
		Analizar los riesgos identificados determinando la probabilidad de ocurrencia y consecuencias para establecer el riesgo inherente.
		Diseñar y clasificar controles para el tratamiento de riesgos.
		Aplicar en las frecuencias establecidas los controles definidos dejando la documentación correspondiente.
		Tratar los riesgos definidos mediante implementación de actividades con el fin de reducir su materialización.
		Definir acciones de contingencia y aplicarlas en caso de materialización de los riesgos.
		Coordinar con el recurso humano el seguimiento y la apropiación de las acciones de control.
		Apropiar documentos al interior del proceso con el fin de determinar actividades de control.
Segunda línea	Supervisores contractuales	Hacer seguimiento, evaluación y monitoreo de los riesgos definidos en los procesos durante la ejecución de los contratos hasta la liquidación.
		Informar al ordenador del gasto respectivo sobre los resultados del seguimiento a los riesgos durante la ejecución contractual.
	Responsables de acompañamiento de calidad	Establecer contacto para definir lineamientos para la presentación de documentos con estándares de calidad.
		Apoyar la actualización los documentos y herramientas de gestión conforme a los avances de tratamiento del riesgo.
Tercera línea	Oficina de Control Interno	Realizar el seguimiento periódico al tratamiento de riesgos y a las actividades definidas en el mismo con el fin de generar acciones que evidencien los avances en el tratamiento del riesgo y la mejora continua.
		Evaluar de manera objetiva la efectividad del tratamiento y la gestión realizada a los riesgos identificados por la entidad.
		Llevar a cabo el seguimiento a los riesgos y la actualización en los documentos de gestión referente al avance en el tratamiento de los mismos.
		Revisar la aplicación de los controles e instrumentos de gestión relacionados al tratamiento y la gestión de riesgos.

8. INSTITUCIONALIDAD

Conforme a lo establecido en la Guía de Administración del Riesgo del DAFP, el modelo integrado de planeación y gestión (MIPG) define para su para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo.

9. BENEFICIOS DE LA GESTIÓN DE RIESGOS

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- Apoyo a la toma de decisiones
- Garantizar la operación normal de la organización
- Minimizar la probabilidad e impacto de los riesgos
- Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)
- Fortalecimiento de la cultura de control de la organización
- Incrementa la capacidad de la entidad para alcanzar sus objetivos
- Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente

Conforme a lo anterior, el IDARTES debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos, elaborando una declaración de aplicabilidad o documento que contenga los controles necesarios, su estado de implementación y la justificación de posible exclusión. Lo anterior con el fin de definir el tratamiento de riesgos que contenga, fechas y responsables con el objetivo de realizar trazabilidad, y que se asigne a roles para gestión de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.

10. TRATAMIENTO DEL RIESGO

El tratamiento del riesgo es la etapa del proceso de administración del riesgo en la cual se definen, evalúan y ejecutan las acciones orientadas a modificar los riesgos identificados, con el propósito de reducir su probabilidad de ocurrencia, minimizar su impacto o llevarlos a niveles aceptables para la entidad. Este proceso se desarrolla una vez realizada la identificación, análisis y evaluación de los riesgos, y debe estar alineado con los objetivos institucionales, la capacidad de gestión y el apetito de riesgo definido.

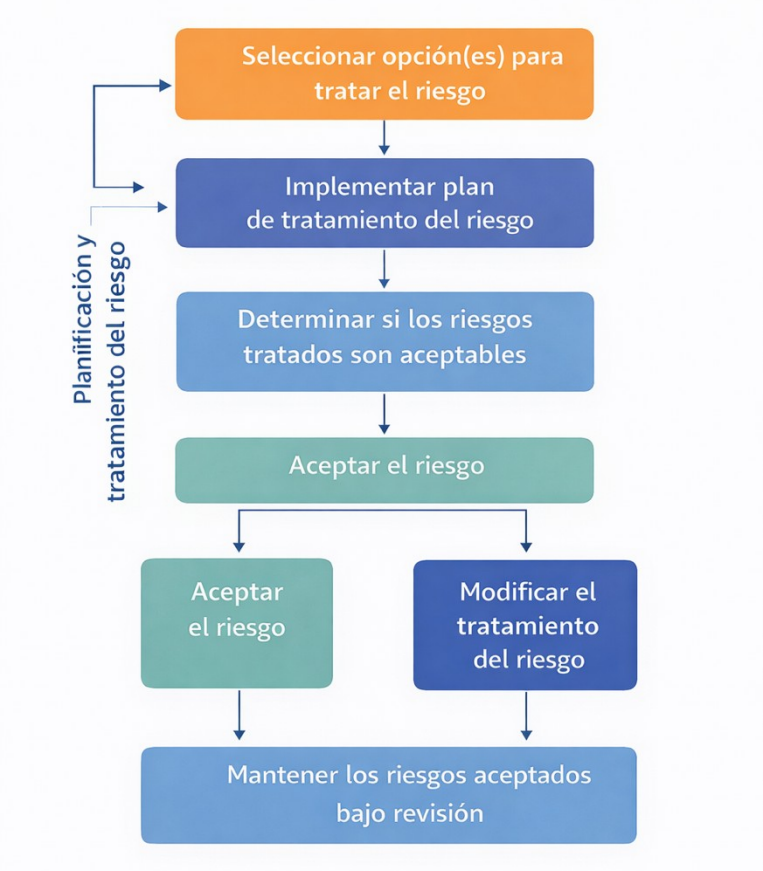

Ilustración 2. Tratamiento del riesgo. Norma ISO27005

Tabla 5. Tabla de Probabilidad

TABLA DE PROBABILIDAD			
Nivel	**Descriptor**	**Descripción (factibilidad)**	**Frecuencia**
1	RARO	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años.
2	IMPROBABLE	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
3	POSIBLE	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
4	PROBABLE	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Tabla 6.Tabla de impacto

TIPO	**NIVEL**	**DESCRIPTOR**	**DESCRIPCIÓN** en caso que el riesgo se materialice el impacto y afectación sería…
Confidencialidad en la información	1	INSIGNIFICANTE	Se afecta a una persona en particular.
	2	MENOR	Se afecta a un grupo de trabajo interno del proceso.

TIPO	NIVEL	DESCRIPTOR	DESCRIPCIÓN en caso que el riesgo se materialice el impacto y afectación sería…
	3	MODERADO	Se afecta a todo el proceso.
	4	MAYOR	La afectación se da a nivel estratégico.
	5	CATASTRÓFICO	La afectación se da a nivel institucional.
Credibilidad o imagen	1	INSIGNIFICANTE	Se afecta al grupo de funcionarios y contratistas del proceso.
	2	MENOR	Se afecta a todos los funcionarios y contratistas de la entidad.
	3	MODERADO	Se afecta a los usuarios de la Sede Central de la entidad.
	4	MAYOR	Se afecta a los usuarios de las Direcciones Territoriales.
	5	CATASTRÓFICO	Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales.
Legal	1	INSIGNIFICANTE	Se producen multas para la entidad.
	2	MENOR	Se producen demandas para la entidad.
	3	MODERADO	Se producen investigaciones disciplinarias.
	4	MAYOR	Se producen investigaciones fiscales.
Operativo	5	CATASTRÓFICO	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.
	1	INSIGNIFICANTE	Se tendrían que realizar ajustes a una actividad concreta del proceso.
	2	MENOR	Se tendrían que realizar ajustes en los procedimientos del proceso.
	3	MODERADO	Se tendrían que realizar ajustes en la interacción de procesos.
	4	MAYOR	Se presentan intermitencias o dificultades en la operación del proceso
	5	CATASTRÓFICO	Se presentaría paro o no operación del proceso.

Tabla 7.Tabla de clasificación de riesgo

TABLA DE CLASIFICACIÓN DEL RIESGO						
Concepto		**Impacto**				
		1	2	3	4	5
Probabilidad		**Insignificante (1)**	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
	VALOR	**1**	**2**	**3**	**4**	**5**
Rara vez (1)	**1**	**11**	**12**	**13**	**14**	**15**
Improbable (2)	**2**	**21**	**22**	**23**	**24**	**25**

Posible (3)	**3**	**31**	**32**	**33**	**34**	**35**
Probable (4)	**4**	**41**	**42**	**43**	**44**	**45**
Casi seguro (5)	**5**	**51**	**52**	**53**	**54**	**55**

ZONA DE RIESGO BAJA
ZONA DE RIESGO MODERADA
ZONA DE RIESGO ALTA
ZONA DE RIESGO EXTREMA

11. GESTIÓN DEL RIESGO

La gestión del riesgo es un proceso sistemático y continuo mediante el cual la entidad identifica, analiza, evalúa, trata, monitorea y comunica los riesgos que pueden afectar el cumplimiento de sus objetivos estratégicos, misionales, operativos y de apoyo. Este proceso permite anticipar eventos que puedan generar impactos negativos y establecer acciones preventivas y correctivas para reducir su probabilidad de ocurrencia y/o sus consecuencias.

Tabla 8. Gestión de riesgo – ISO 31000

Referencia ISO-31000	
Aceptar	Consiste en retener el riesgo sin acción posterior, los riesgos se analizan y se viabiliza su aceptación si la frecuencia es baja y el impacto es leve o menor y no se pone en riesgo la estabilidad y operatividad del IDARTES.
Evitar	Evitar la actividad o la acción que da origen al riesgo particular, esta alternativa de tratamiento ocurre cuando su probabilidad es alta y representa un alto peligro para IDARTES, es de analizar si los costos para implementar los controles exceden los beneficios se puede viabilizar la decisión de evitar entonces el riesgo.
Reducir	Minimizar el impacto del riesgo, o reducir las posibilidades de que ocurra, es también una acción válida dentro de un proceso de Gestión de Riesgos, dado que mitigar significa que IDARTES puede limitar el impacto de un riesgo, de modo que, aunque este ocurra, el impacto sea mínimo y fácil de subsanar
Compartir	Transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular, la transferencia se puede realizar mediante un seguro, al transferir el riesgo a un tercero le damos responsabilidad para su administración, pero no significa que se elimine el riesgo.
Eliminar	Se puede eliminar la fuente del riesgo

12. IDENTIFICACIÓN DE LOS RIESGOS

El objetivo de la identificación de riesgos es determinar que podría suceder que cause una pérdida potencial y llegar a comprender el cómo, dónde y por qué podría ocurrir pérdida, durante la vigencia 2026 se identificaron riesgos a la seguridad y privacidad de la información que requieren ser tratados con unos controles y actividades que permitan disminuir las causas y la probabilidad de que se materialicen; las causas pueden ser internas o externas, según lo que haya identificado el IDARTES a través del contexto estratégico.

Es fundamental determinar el impacto en los activos críticos para asociarlos a los procesos correspondientes y, a partir de ello, generar un listado de procesos críticos. Esto incluye inventariar los activos de información sensible y revisar los procesos según su clasificación. Actualmente, los riesgos de seguridad de la información están identificados y gestionados a través del módulo de riesgos de PANDORA.

13. CRONOGRAMA IMPLEMENTACIÓN DEL PLAN

A continuación, se detallan las actividades previstas para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información durante el año 2026.

14. SEGUIMIENTO Y REVISIÓN

- Autocontrol por parte de la primera línea de defensa (TI), mediante el uso del instrumento de gestión interno PETI.
- Autoevaluación o monitoreo por parte de la segunda línea de defensa (OAP-TI), utilizando el instrumento de plan de acción integral 2025.
- Evaluación independiente por parte de la tercera línea de defensa, a cargo del área de Control Interno.

Es importante conocer de manera permanente los avances en la gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital y Seguridad Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de éstos en el Comité de Gestión Institucional y

Desempeño, como lo establece el MIPG. La Oficina Asesora de Planeación y Tecnologías de la Información debe realizar el seguimiento y control a la implementación y/o mantenimiento de la Seguridad de la Información.

Ajustes y modificaciones:

Después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el plan de seguridad y privacidad de la información, en este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

Monitoreo:

En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con sus equipos realizarán el monitoreo permanente a la gestión de seguridad y privacidad de la información en coordinación con el oficial de seguridad de la información.

Seguimiento:

Coordinar en conjunto con la oficina de control interno, o quien haga sus veces, acciones para adelantar seguimiento a la gestión de seguridad y privacidad de la información, en este sentido, por esto, es necesario que en sus procesos de seguimiento interno analicen las causas, los riesgos y la efectividad de los controles incorporados en el documento.

15. NORMATIVIDAD

Para este plan, se aplica la normativa establecida en el nomograma institucional correspondiente al proceso de Gestión de Tecnologías de la Información.

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
1	2018-07-25	Emisión Inicial
2	2019-01-30	Actualización de riesgos de seguridad y privacidad de la información
3	2020-01-31	Actualización normativa
4	2021-01-31	Actualización de riesgos de seguridad y privacidad de la información
5	2022-01-31	Actualización de riesgos de seguridad y privacidad de la información
6	2023-01-31	Actualización de riesgos de seguridad y privacidad de la información
7	2024-02-15	Actualización de riesgos de seguridad y privacidad de la información
8	2025-01-31	Se incorpora el cronograma de implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para el 2025.
9	2026-01-26	Actualización del cronograma de implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para el 2026.

CONTROL DE APROBACIÓN

ESTADO	FECHA	NOMBRE	CARGO
ELABORÓ	2026-01-21	MARYURY FORERO BOHORQUEZ	ENLACE MIPG
REVISÓ	2026-01-21	MARIA CRISTINA HERRERA CALDERON	REFERENTE MIPG
APROBÓ	2026-01-26	DANIEL SANCHEZ ROJAS	LIDER DE PROCESO
AVALÓ	2026-01-26	DANIEL SANCHEZ ROJAS	JEFE DE LA OFICINA ASESORA DE PLANEACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN

COLABORADORES

NOMBRE