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

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

ALCALDÍA MAYOR
DE BOGOTÁ D.C.

BOGOTÁ

HISTÓRICO DE CAMBIOS		
Versión	**Fecha de Emisión**	**Cambios realizados**
1	25/07/2018	Emisión inicial
2	30/01/2019	Actualización de riesgos de seguridad y privacidad de la información
3	31/01/2020	Actualización normativa
4	31/01/2021	Actualización de riesgos de seguridad y privacidad de la información
5	31/01/2022	Actualización de riesgos de seguridad y privacidad de la información
6	31/01/2023	Actualización de riesgos de seguridad y privacidad de la información
7	13/02/2024	Actualización de riesgos de seguridad y privacidad de la información

ELABORÓ	REVISÓ	APROBÓ	AVALÓ
Jorge Farigua Gutiérrez Contratista de la Oficina Asesora de Planeación y Tecnologías de la información	**Jonathan González Bolaños** Profesional Universitario Oficina Asesora de Planeación y Tecnologías de la Información **Maryury Forero Bohorquez** Contratista Oficina Asesora de Planeación y Tecnologías de la Información **María Cristina Herrera Calderón** Contratista Oficina Asesora de Planeación y Tecnologías de la Información	**Daniel Sánchez Rojas** Jefe de la Oficina Asesora de Planeación y Tecnologías de la información	**Daniel Sánchez Rojas** Jefe de la Oficina Asesora de Planeación y Tecnologías de la información

TABLA DE CONTENIDO

Tabla de Figuras

Tabla de tablas

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 de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos 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 medida, objetivo, justificación, responsable de la medida y su prioridad, el Idartes define medidas que serán aplicadas en la vigencia 2024.

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.

2. Objetivo

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información y de Seguridad Digital que el Idartes pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

3. Alcance

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información y de Seguridad Digital, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Alineado a una gestión de tratamiento de riesgos de Seguridad y Privacidad de la Información, donde se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el Idartes. El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los diferentes niveles acorde con los lineamientos definidos por el Idartes.

4. Metodología

La gestión del riesgo es iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas, dado que es parte de la gobernanza y el liderazgo considerada como parte fundamental para gestionar la organización contribuyendo a la mejora de los sistemas de gestión TI.

El análisis de los riesgos es parte de todas las actividades asociadas con la organización e incluye la interacción con las partes interesadas, donde se considera los contextos externo e interno de la organización, incluido el comportamiento humano y los demás factores, ya que está basada en los principios, el marco de referencia y el proceso identificado.

5. Responsables

Oficina Asesora de Planeación y Tecnologías de la Información – OAPTI

6. 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

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.
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 (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 Pública Reservada	Es aquella información que estando en poder o custodia de un sujeto obligado 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, anonimización 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.
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.

7. Condiciones generales

- Proporcionar a los sujetos obligados mecanismos, lineamientos e instrumentos de implementación claros que les permitan adoptar, implementar y apropiar el MSPI con mayor facilidad.
- Aportar en el desarrollo e implementación de la estrategia de seguridad digital de la Entidad.
- Establecer procedimientos de seguridad que permitan 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 las Entidades.
- 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, de cada entidad, a través del plan de seguridad y privacidad de la información.

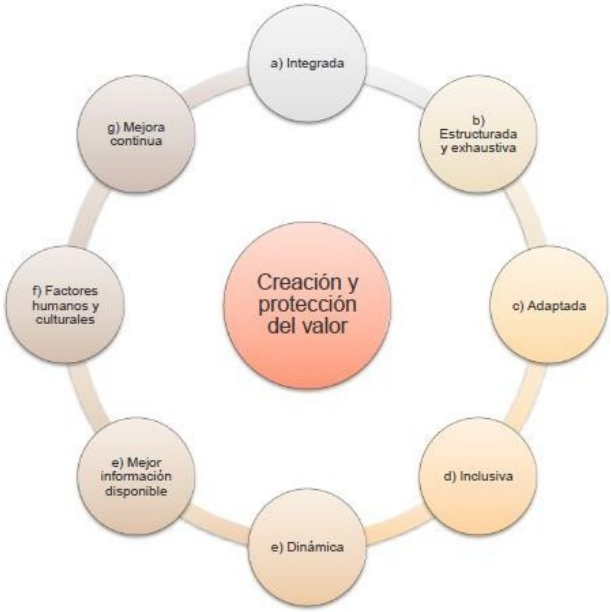

Figura 1. Principios. Norma ISO 31000:2018 2da. edición

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 organización 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 organización. 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

8. Marco de referencia

8.1. Generalidades

El Idartes utiliza como marcos de referencia la Guía para gestión del riesgo y el diseño de controles en Entidades Públicas, emitida por MinTIC 2020 y la Norma Técnica Colombiana NTC-ISO 31000:2018.

8.2. 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:

8.3. 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
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

9. 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.

10. 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.

11. Tratamiento del riesgo

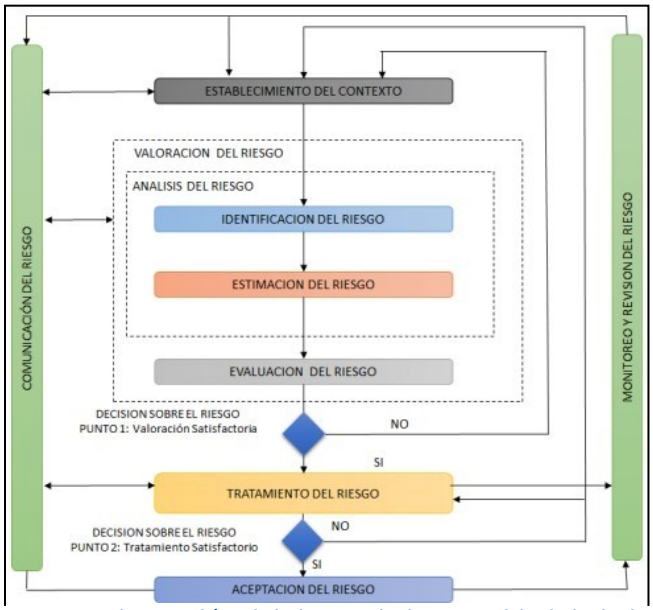

Figura 2. Proceso de gestión del riesgo de la seguridad de la información

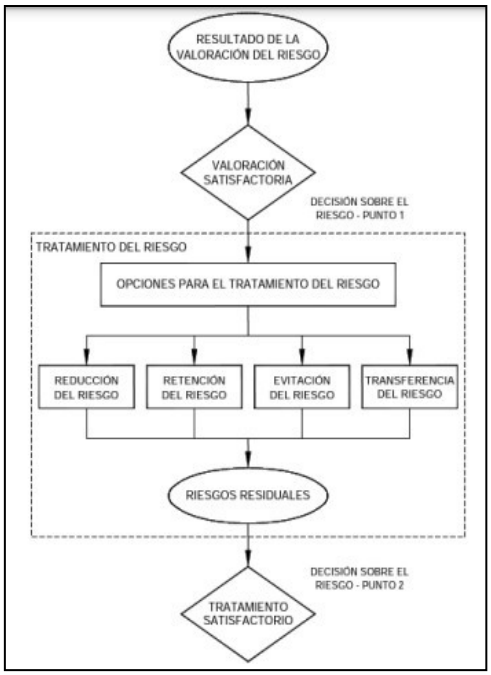

Figura 3. Tratamiento del riesgo Norma ISO 27005

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

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.
		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.

		5		CATASTRÓFICO		Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.
OPERATIVO		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

12. Gestión del riesgo

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

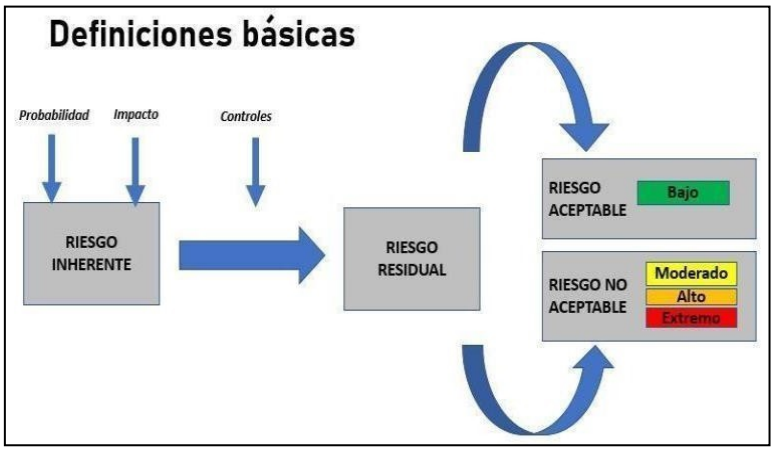

Figura 4. Aceptación de riesgo

13. Identificación de los riesgos Idartes

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 2022 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 importante establecer el impacto sobre los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible y revisar los procesos según la clasificación.

Tabla 9. inventario de riesgos

ID del riesgo
R01
Riesgo
Pérdida de Integridad de la información de las unidades de gestión
Análisis
Se puede presentar una posible afectación reputacional por pérdida de integridad de la información contenida en las bases de datos generadas por los sistemas de información institucionales debido a la ausencia o deficiencia en los controles en el proceso de autenticación por parte de los usuarios de los aplicativos permitiendo el acceso a la información almacenada y/o procesada en los sistemas de información.
Probabilidad
Posible
Impacto
Menor
Opción de manejo
Reducir

ID del riesgo

R02
Riesgo
Pérdida de Disponibilidad de la información institucional
Análisis
Puede presentarse una posible afectación reputacional por Pérdida de Disponibilidad en información contenida en las bases de datos o matrices de información de las unidades de gestión debido al Almacenamiento sin protección permitiendo un inadecuado almacenamiento, disposición final, custodia, asignaciones equivocada de permisos de acceso o destrucción segura de la información contenida en las bases de datos.
Probabilidad
Posible
Impacto
Moderado
Opción de manejo
Reducir

ID del riesgo
R03
Riesgo
Pérdida de Confidencialidad en la infraestructura tecnológica que respalda y apoya los servicios tecnológicos de la entidad
Análisis
Conforme a la operación de los servicios y sistemas TI y el propósito de garantizar el correcto funcionamiento y la disponibilidad, se evidencian amenazas que se aprovechan de las vulnerabilidades generadas en el uso indebido de los equipos y herramientas de la plataforma tecnológica lo cual puede generar la Posible afectación reputacional por pérdida de la disponibilidad en las bases de datos y matrices construidas por las unidades de gestión ya que se tiene almacenamiento sin protección generando extravío o no disponibilidad de la información, resulta complejo contar con la infraestructura tecnológica perfecta para garantizar al recurso humano de las unidades de gestión un funcionamiento libre de fallas, pero es posible tener procesos organizados y herramientas con fortaleza para asegurar respuestas frente a diferentes vulnerabilidades por lo anterior se han reforzados desde la estrategia TI herramientas y servicios que están interconectadas con herramientas, aplicativos, plataformas y otras interfaces tecnológicas, con el fin de que sean lo más efectivas y funcionales evitando amenazas y contratiempos.
Probabilidad
Posible
Impacto
Moderado
Opción de manejo
Reducir

14. Análisis para el tratamiento del riesgo

El Idartes en el marco de la estrategia TI y la implementación del plan de tratamiento de riesgos definió los siguientes objetivos con el fin de estructurar el presente documento

Formular y seleccionar acciones y/o actividades para el tratamiento del riesgo
Planificar e implementar el tratamiento del riesgo
Evaluar la eficacia del tratamiento implementado para reducir el riesgo

Definir si el riesgo residual es aceptable o no aceptable
Actuar si el riesgo no es aceptable y efectuar tratamiento adicional.

15. Matriz de tratamiento de riesgos

15.1. Identificación

Referencia	Impacto ¿Que?	Causa Inmediata ¿Cómo?	Tipos de activo de Información	Activo de Información	Causa Raíz/Vulnerabilidad	Amenaza	Descripción del riesgo
1	Posible afectación reputacional	Pérdida de Integridad	Bases de datos	Bases de datos de los sistemas de información	Ausencia o deficiencia en los sistemas de autenticación de los aplicativos	No se aplican controles permitiendo el acceso sin credenciales a la información almacenada y procesada en los datos de los sistemas de información.	Posible afectación reputacional por pérdida de integridad de la **informacion contenida** en las bases de datos generadas por los sistemas de información institucionales debido a la ausencia o deficiencia en los **controles en el proceso** de autenticación **por parte de los usuarios** de los aplicativos permitiendo el acceso a la información almacenada **y/o** procesada en los sistemas de información.
					Ausencia de controles de acceso a edición, modificación y/o eliminación de datos personales	No se aplican controles definidos para los accesos a drive y repositorios y/o propiedad de la información	Posible afectación reputacional y económica por pérdida de integridad **de la informacion contenida** en las bases de datos generadas por los sistemas de información institucionales debido a la ausencia o deficiencia de autenticación en los aplicativos permitiendo el acceso a la información con datos personales almacenados en los sistemas de información.

Referencia	Impacto ¿Que?	Causa Inmediata ¿Cómo?	Tipos de activo de Información	Activo de Información	Causa Raíz/Vulnerabilidad	Amenaza	Descripción del riesgo
2	Posible afectación reputacional	Pérdida de Disponibilidad	Bases de datos	Bases de datos o matrices de las unidades de gestión	Almacenamiento sin protección	Extravío o no disponibilidad de equipos o información debido a un inadecuado tratamiento en el almacenamiento, disposición final, custodia o destrucción segura de los mismos.	Posible afectación reputacional por Pérdida de Disponibilidad en las Base de datos o matrices **de información** de las unidades de gestión debido al Almacenamiento sin protección permitiendo un inadecuado almacenamiento, disposición final, custodia o destrucción segura de la información contenida en las bases de datos.
			Software	Sistemas de información y aplicaciones de Software	Ausencia de un espacio de contingencia o respaldo de los servicios y sistemas TI	Las fallas en los equipos tecnológicos o redes de comunicación debido a agentes externos, ambientales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de	Posible afectación reputacional por Pérdida de Disponibilidad en sistemas de información y aplicaciones de software debido a la Ausencia de un espacio de contingencia o respaldo de los servicios y sistemas TI permitiendo **fallos** en los equipos tecnológicos o redes de comunicación debido a agentes externos, ambientales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de las funciones y operaciones

Referencia	Impacto ¿Que?	Causa Inmediata ¿Cómo?	Tipos de activo de Información	Activo de Información	Causa Raiz/Vulnerabilidad	Amenaza	Descripción del riesgo
3	Posible afectación reputacional	Pérdida de Confidencialidad	Software	Bases de datos de los sistemas de información	Transferencia de contraseñas	Falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente.	Posible afectación reputacional por pérdida de la disponibilidad en las bases de datos y matrices construidas por las unidades de gestión ya que se tiene almacenamiento sin protección generando extravío o no disponibilidad de la información

15.2. Análisis y tratamiento

Descripción del riesgo	Clasificación del riesgo (Seleccionar)	Frecuencia (Seleccionar)		Probabilidad inherente	%	Impacto inherente (Seleccionar)		%		Zona de riesgo inherente
Posible afectación reputacional por pérdida de integridad de la **informacion contenida** en las bases de datos generadas por los sistemas de información institucionales debido a la ausencia o deficiencia en los **controles en el proceso** de autenticación **por parte de los usuarios** de los aplicativos permitiendo el acceso a la información almacenada **y/o** procesada en los sistemas de información.	Daños a activos fijos/ eventos externos	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	500	Media	60%	El riesgo afecta la imagen de algún área de la organización.	Leve	20%	Media	Moderado
Posible afectación reputacional y económica por pérdida de integridad **de la informacion contenida** en las bases de datos generadas por los sistemas de información institucionales debido a la ausencia o deficiencia de autenticación en los aplicativos permitiendo el acceso a la información con datos personales almacenados en los sistemas de información.	Usuarios, productos y prácticas	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	500	Media	60%	Entre 30 y 150 SMLMV	Menor	40%	Media	Moderado

Descripción del riesgo	Clasificación del riesgo (Seleccionar)	Frecuencia (Seleccionar)		Probabilidad inherente	%	Impacto inherente (Seleccionar)		%		Zona de riesgo inherente
Posible afectación reputacional por Pérdida de Disponibilidad en las Base de datos o matrices **de información** de las unidades de gestión debido al Almacenamiento sin protección permitiendo un inadecuado almacenamiento, disposición final, custodia o destrucción segura de la información contenida en las bases de datos.	Usuarios, productos y prácticas	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	10	Baja	40%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.	Menor	40%	BajaM	Moderado
Posible afectación reputacional por Pérdida de Disponibilidad en sistemas de información y aplicaciones de *software* debido a la Ausencia de un espacio de contingencia o respaldo de los servicios y sistemas TI permitiendo **fallos** en los equipos tecnológicos o redes de comunicación debido a agentes externos, ambientales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de las funciones y operaciones	Fallas tecnológicas	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	100	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.	Menor	40%	Media	Moderado

Descripción del riesgo	Clasificación del riesgo (Seleccionar)	Frecuencia (Seleccionar)		Probabilidad inherente	%	Impacto inherente (Seleccionar)		%		Zona de riesgo inherente
Posible afectación reputacional por pérdida de confidencialidad en bases de datos de los sistemas de información debido Elevación de **privilegios y/o acceso** no autorizado a la información permitiendo que Las operaciones realizadas con la información no pueden rastrearse o no presenta claramente quién y qué se ha realizado con la misma.	Daños a activos fijos/ eventos externos	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	50	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.	Menor	40%	Media	Moderado
Posible afectación reputacional por Pérdida de Confidencialidad en el Recurso Humano debido a la Ausencia de procedimiento formal para la autorización de la información disponible permitiendo el Tratamiento inadecuado de la información por desconocimiento de políticas, controles y buenas prácticas de seguridad y privacidad de la información establecidas por la Entidad por parte del	Usuarios, productos y prácticas	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	80	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.	Menor	40%	Media	Moderado

15.3. Controles e indicador

			Valoración del Riesgo											
			Afectación		Atributos									
Descripción del riesgo	Descripción del Control	Soporte documental	Probabilidad (Controles preventivos y Detectivos)	Impacto (Controles Correctivos)	Tipo (Seleccionar)	Implementación (Seleccionar)	Concatenar	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual	Probabilidad Residual Final
Posible afectación reputacional por pérdida de integridad de la **informacion contenida** en las bases de datos generadas por los sistemas de información institucionales debido a la ausencia o deficiencia en los **controles en el proceso** de autenticación **por parte de los usuarios** de los aplicativos permitiendo el acceso a la información almacenada **y/o** procesada en los sistemas de información.	Control 1: A.9.2.3 Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Procedimiento Gestión de cuentas de usuario Políticas de seguridad de la Información Gestión de Bases de Datos Política de Desarrollo Seguro	X		Preventivo	Manual	PreventivoManual	40%	Documentac	Continu	Reporte de cumplimiento plan de seguridad y privacidad en la información	36%	Baja
Posible afectación reputacional y económica por pérdida de integridad **de la informacion contenida** en las bases de datos generadas por los sistemas de información institucionales debido a la ausencia o deficiencia de autenticación en los aplicativos permitiendo el acceso a la información con datos personales almacenados en los sistemas de información.	Control: A.18.1.4 Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.	Políticas de seguridad de la Información Política de Desarrollo Seguro **Política de tratamiento de datos personales**	X		Preventivo	Manual	PreventivoManual	40%	Documentac	Continu	Reporte de cumplimiento del PETI	36%	Baja

Descripción del Control	Soporte documental	Afectación		Atributos							Probabilidad Residual	Probabilidad Residual Final	%	Impacto Residual Final	%		Zona de Riesgo Final	Tratamiento	Debe establecer Plan de Acción Si/No
		Probabilidad (Controles preventivos y Detectivos)	Impacto (Controles Correctivos)	Tipo (Seleccionar)	Implementación (Seleccionar)	Concatenar	Calificación	Documentación	Frecuencia	Evidencia									
Control A.12.3.1 Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo	Procedimiento copias y respaldos Políticas de seguridad de la Información Gestión de Bases de Datos		X	Correctivo	Manual	CorrectivoManual	25%	Documentad	Continu	Reporte de cumplimiento plan de seguridad y privacidad en la información	30%	Baja		Menor	40%	BajaMenor	Moderado	Reducir - Mitigar	SI
Control A.17.1.2 La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de **continuidad de los sistemas de información** para la seguridad de la	Plan de continuidad TI Políticas de seguridad de la Información		X	Correctivo	Manual	CorrectivoManual	25%	Documentad	Continu	Reporte de cumplimiento plan de seguridad y privacidad en la información	45%	Media		Menor	40%	MediaMenor	Moderado	Reducir - Mitigar	SI
Control A.9.2.2 Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	Políticas de seguridad de la Información **Procedimiento administración cuentas de usuario**		X	Correctivo	Manual	CorrectivoManual	25%	Documentad	Continu	Reporte de cumplimiento plan de seguridad y privacidad en la información	45%	Media		Menor	40%	MediaMenor	Moderado	Reducir - Mitigar	SI

Descripción del riesgo	Descripción del Control	Soporte documental	Probabilidad (Controles preventivos y Detectivos)	Impacto (Controles Correctivos)	Tipo (Seleccionar)	Implementación (Seleccionar)	Concatenar	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual	Probabilidad Residual Final	%	Impacto Residual Final	%		Zona de Riesgo Final	Tratamiento	Debe establecer Plan de Acción Si/No
Posible afectación reputacional por pérdida de confidencialidad en bases de datos de los sistemas de información debido Elevación de **privilegios y/o acceso** no autorizado a la información permitiendo que Las operaciones realizadas con la información no puedan rastrearse o no presenta claramente quién y qué se ha realizado con la misma.	Control A.12.4.1 Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Políticas de seguridad de la Información Procedimiento Copia y Restauración de la Información Procedimiento Incidentes de Seguridad de la Información		X	Correctivo	Manual	CorrectivoManual	25%	Documentad	Continu	Reporte de cumplimiento plan de seguridad y privacidad en la información	45%	Media		Menor	40%	MediaMenor	Moderado	Reducir - Mitigar	SI
Posible afectación reputacional por Pérdida de Confidencialidad en el Recurso Humano debido a la Ausencia de procedimiento formal para la autorización de la información disponible permitiendo el Tratamiento inadecuado de la información por desconocimiento de políticas, controles y buenas prácticas de seguridad y privacidad de la información establecidas por la Entidad por parte del	Control A.9.3.1 Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Procedimiento Gestión de cuentas de usuario Políticas de seguridad de la Información Gestión de Bases de Datos		X	Correctivo	Manual	CorrectivoManual	25%	Documentad	Continu	Reporte de cumplimiento plan de seguridad y privacidad en la información	45%	Media		Menor	40%	MediaMenor	Moderado	Reducir - Mitigar	SI

16. Cronograma de Implementación del Plan

Tabla 10. Cronograma de implementación

Control	Nombre		Actividad	Fecha cumplimiento	Responsable
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Crear documento de gestión de contraseñas que cumpla con las siguientes condiciones: Revisar el sistema de gestión de contraseñas que incluya: a) cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas; b) permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada; c) Exigir por que se escojan contraseñas de calidad; d) Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez; e) Exigir por que se cambien las contraseñas en forma regular, según sea necesario: f) llevar un registro de las contraseñas usadas previamente, e impedir su reusó; g) no visualizar contraseñas en la pantalla cuando se está ingresando; h) almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones; i) almacenar y transmitir las contraseñas en forma protegida.	31/12/2024	Sistemas de información Administrador Directorio activo
A.11.2.8	Equipos de usuario desatendidos	Los usuarios deben asegurarse de	Establecer dentro del manual de políticas de seguridad que los equipos de usuarios desatendidos cumplan con las siguientes	31/12/2024	Oficial de Seguridad de la Información

Control	Nombre		Actividad	Fecha cumplimiento	Responsable
		que a los equipos desatendidos se les dé protección apropiada.	condiciones a) establecer que se cierren las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado (un protector de pantalla protegido con contraseña); b) establecer que es obligatorio salir de las aplicaciones o servicios de red cuando ya no los necesiten; c) asegurar que los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente (acceso con contraseña, cuando no están en uso).		
A.12.1.3	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	Revisar la documentación relacionada con la gestión de la demanda de capacidad, se incluyan: a) Eliminar datos obsoletos (espacio en disco); b) realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes; c) optimizar las consultas de bases de datos o lógicas de las aplicaciones; d) realizar una negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio (por ejemplo, video en tiempo real)	31/12/2024	Administrador Bases de datos
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto	Realizar la inclusión de las siguientes actividades en el procedimiento de desarrollo de software en los relacionado con la revisión técnica de las aplicaciones después de cambios en la plataforma de operación: a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones; b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la	31/12/2024	Sistemas de información Oficial de Seguridad de la Información

Control	Nombre		Actividad	Fecha cumplimiento	Responsable
		adverso en las operaciones o seguridad de la organización.	implementación; c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.		

17. Seguimiento y revisión

El objetivo del seguimiento y la revisión es asegurar la eficacia del diseño, la implementación y los resultados del tratamiento de los riesgos.

Para el seguimiento y la revisión, asignar responsabilidades.

- El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.
- Los resultados del seguimiento y la revisión son sujetos de análisis conforme a la inclusión en las actividades de gestión del desempeño
- Se debe revisar periódicamente por cada responsable de los procesos al interior de la entidad, junto con su equipo los siguientes aspectos
- 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 la matriz de riesgos. 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 su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos.
- Seguimiento: el jefe de control interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos. En este sentido, es necesario que en sus procesos de auditoría interna analicen las causas, los riesgos y la efectividad de los controles incorporados en la matriz de riesgos.

18. Normativa

Tabla 11. Normatividad

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 1360 de 1989	Presidencia de Colombia	Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 2150 de 1995	Ministerio de Justicia y del Derecho	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Ley 572 de 1999	Congreso de la República	Comercio Electrónico, Firmas Digitales, Intercambio electrónico de datos.
Documento Conpes 3072 de 2000	Departamento Nacional de Planeación	Agenda de Conectividad
Decreto 3816 de 2003	Presidencia de Colombia	Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública
Conpes 3292 de 2004	Departamento Nacional de Planeación	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
Directriz 5 de 2005	Alcaldía Mayor de Bogotá	Por la cual la Alcaldía Mayor de Bogotá define Políticas Generales y Directrices que orienten el desarrollo tecnológico.
Decreto 619 de 2007	Alcaldía Mayor de Bogotá	Por el cual se establece la Estrategia de Gobierno Electrónico en el Distrito.
Decreto 316 de 2008	Alcaldía Mayor de Bogotá	Por medio del cual se modifica parcialmente el artículo 3 del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.
Ley 1273 de 2009	Congreso de la República	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Congreso de la República	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Decreto 235 de 2010	Ministerio del Interior y de Justicia	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

Tipo de norma	Entidad que expide	Descripción normativa
Conpes 3701 de 2011	Departamento Nacional de Planeación	Lineamientos de política para la Ciberseguridad y Ciberdefensa
Ley 1581 de 2012	Congreso de la República	Por el cual se dictan disposiciones generales para la protección de datos personales
Decreto 884 de 2012	Presidencia de Colombia	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones
Decreto 2364 de 2012	Ministerio del Interior y Justicia	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones
Decreto 19 de 2012	Presidencia de Colombia	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
Resolución 396 de 2012	Instituto Distrital de las Artes	Por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - Idartes.
Ley 1618 de 2013	Presidencia de Colombia	Por medio de la cual se establecen las disposiciones para garantizar el pleno ejercicio de los derechos de las personas con discapacidad. Art 16. Derecho a la información y comunicaciones
Decreto 1377 de 2013	Presidencia de Colombia	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Decreto 596 de 2013	Alcaldía Mayor de Bogotá	Por el cual se dictan medidas para la aplicación del Teletrabajo en organismos y entidades del Distrito Capital
ley 1712 de 2014	Congreso de la República	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Resolución 383 de 2014	Instituto Distrital de las Artes	Por la cual se modifica la Resolución No 396 de 2012, "por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - Idartes".
Ley 1753 de 2015	Congreso de la República	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAÍS" Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 103 de 2015	Presidencia de Colombia	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 1081 de 2015	Presidencia de Colombia	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República
Decreto 1078 de 2015	Presidencia de Colombia	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Conpes 3854 de 2016	Departamento Nacional de Planeación	Política Nacional de Seguridad Digital. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
Decreto 415 de 2016	Departamento Administrativo de la Función Pública	Se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
Resolución 4 de 2017	Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas - CDS	Por la cual se modifica la Resolución 305 de 2008 de la CDS
Decreto 728 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de las zonas de acceso público a internet inalámbrico
Decreto 1413 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
Resolución 2710 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por la cual se establecen lineamientos para la adopción del protocolo IPv6

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 728 de 2017	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno
Circular 30 de 2017	Alta Consejería de TICs	Implementación CSIRT de Gobierno
Circular 36 de 2017	Alta Consejería de TICs	Lineamientos de avance del modelo de seguridad y privacidad de la información
Resolución 3436 de 2018	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.
Decreto 612 de 2018	Departamento Administrativo de la Función Pública	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.
Decreto 1008 de 2018	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Circular 2 de 2018	Ministerio de las Tecnologías de la Información y las Comunicaciones	Cumplimiento legal y normativo respecto a seguridad de la información
Conpes 3920 de 2018	Departamento Nacional de Planeación	Big Data, la política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
Guía 6 de 2019	Ministerio de las Tecnologías de la Información y las Comunicaciones	Guía para la construcción del Plan Estratégico de Tecnologías de Información PETI
Ley 1955 del 2019	Presidencia de Colombia	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 2106 de 2019	Departamento Administrativo De La Función Pública	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva
Conpes 3975 de 2019	Departamento Nacional de Planeación	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Decreto 620 de 2020	Departamento Administrativo De La Función Pública	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales
Resolución 00500 de 2021	Ministerio de las Tecnologías de la Información y las Comunicaciones	"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"
Resolución 00500 de 2021 Anexo 1	Ministerio de las Tecnologías de la Información y las Comunicaciones	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las Entidades del Estado
Directiva 09 de 2021	Secretaría Jurídica Distrital	Buenas prácticas en el uso de fotografías y videos para la protección de derechos de autor
Resolución número 00460 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Se dictan disposiciones sobre el Plan Nacional de Infraestructura de datos
Decreto 338 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el título 21 a la parte 2 del libro 2 del decreto único 1078 de 2015, reglamentario del sector de tecnologías de la información y las comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el modelo y las instancias de gobernanza de seguridad digital y se dictan otras disposiciones
Decreto 767 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Tipo de norma	Entidad que expide	Descripción normativa
Decreto 1263 de 2022	Ministerio de las Tecnologías de la	Por el cual se adiciona el título 22 a la parte 2 del libro 2 del decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las
	Información y las Comunicaciones	comunicaciones, con el fin de definir lineamientos y estándares aplicables a la transformación digital pública
Decreto 1389 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adiciona el título 24 a la parte 2 del libro 2 del decreto único 1078 de 2015, reglamentario del sector de tecnologías de la información y las comunicaciones, con el fin de establecer los lineamientos generales para la gobernanza en la infraestructura de datos, y se crea el modelo de gobernanza de la infraestructura de datos
Decreto 1449 de 2022	Ministerio de las Tecnologías de la Información y las Comunicaciones	Por el cual se adopta la estructura del Ministerio de Ciencia, Tecnología e Innovación y se dictan otras disposiciones; Art. 7 Num.13

Documento 20241200107583 firmado electrónicamente por:

DANIEL SÁNCHEZ ROJAS, Jefe Oficina Asesora de Planeación y Tecnologías de la Información, Oficina Asesora de Planeación, Fecha firma: 14-02-2024 17:09:01
MARYURY FORERO BOHORQUEZ, Contratista, Oficina Asesora de Planeación, Fecha firma: 14-02-2024 09:45:42
JORGE ALBERTO FARIGUA GUTIERREZ, , Oficina Asesora de Planeación, Fecha firma: 14-02-2024 11:30:10
MARIA CRISTINA HERRERA CALDERON, , Oficina Asesora de Planeación, Fecha firma: 14-02-2024 15:51:21
JONATHAN GONZÁLEZ BOLAÑOS, Profesional Universitario Código: 219 Grado: 01, Área de Tecnología, Fecha firma: 14-02-2024 11:40:32

Proyectó: SANDRA PATRICIA MORENO BOHORQUEZ - Técnico Administrativo - Área de Tecnología

7090526ae1128fe16a10852b7544e5ddfc3fe20daaf094176716c76dfc90025a
Codigo de Verificación CV: a2172 Comprobar desde: