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

Objetivo:
Establecer la gestión para el tratamiento de los riesgos de la seguridad y privacidad de la información en Idartes.

Alcance:
El presente plan define las actividades para el tratamiento adecuado de los riesgos asociados a los activos de información y recursos informáticos de proceso de gestión de las tecnologías de Instituto Distrital de las Artes - Idartes

Fecha de aprobación	Responsable del documento	Ubicación
16-01-2022	Oficina Asesora de Planeación y Tecnologías de la Información	Intranet Comunicarte

Histórico de cambios		
Versión	**Fecha de emisión**	**Cambios realizados**
01	25/07/2018	Emisión inicial
02	30/01/2019	Actualización de riesgos de seguridad y privacidad de la información
03	31/01/2020	Actualización normativa
04	31/01/2021	Actualización de riesgos de seguridad y privacidad de la información
05	16/01/2022	Actualización de riesgos de seguridad y privacidad de la información

Elaboró	Revisó	Aprobó	Avaló
14/01/2022 **Andrés Briceño Díaz** Contratista Oficial de Seguridad de la Información	**17/01/2022** **Aurora Camila Crespo Murillo** Contratista de la Oficina Asesora de Planeación y Tecnologías de la Información	**14/01/2022** **Edgar Alfonso Cipagauta Pedraza** Profesional Especializado OAP-TI **18/01/2022** **Carlos Alfonso Gaitán Sánchez** Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información	**18/01/2022** **Carlos Alfonso Gaitán Sánchez** Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información

TABLA DE CONTENIDO

Contenido

INTRODUCCIÓN

Cualquier tipo de organización independiente de su tamaño y tipo afronta factores tanto internos como externos que pueden afectar uno de los activos más importante de la organización: la información. Todas las actividades de una entidad involucran riesgos y de una forma u otra los gestionan mediante su identificación, análisis y su respectivo tratamiento. El presente documento establece las líneas de acción para la gestión del riesgo basándose en la guía para la administración del riesgo y diseño de controles en entidades públicas de MinTIC, en el marco de la implementación y apropiación de la estrategia de Gobierno Digital, contemplando los estándares internacionales como la NTC-ISO 31000 y la NTC-ISO 27001.

Es responsabilidad del Idartes implementar líneas de acción que permitan el tratamiento de los riesgos de seguridad y privacidad de la información. El recurso humano del Idartes, en cumplimiento de los objetivos misionales y administrativos del instituto, por lo tanto, es necesario establecer los controles necesarios para identificar las causas y consecuencias de la materialización de los riesgos. Por lo anterior este plan pretende trazar la ruta a seguir para orientar y facilitar el tratamiento de riesgos de seguridad de la información, de forma eficiente y efectiva, desde la identificación hasta la definición de controles para su gestión.

OBJETIVO

Diseñar un plan de gestión para el tratamiento de riesgos articulado con las herramientas y procedimientos que permitan evitar que se materializan las vulnerabilidades y amenazas en los servicios y sistemas TI que hacen parte integral de la infraestructura tecnológica de Idartes y poder realizar acciones ante eventuales sucesos internos o externos que produzcan fallas totales o parciales en la operación, aplicando una metodología de gestión de riesgos a los activos de información del Instituto Distrital de las Artes - IDARTES

ALCANCE

La identificación, análisis y gestión de los riesgos conforme a los activos de información que tienen una clasificación dentro del inventario de activos de información y buscan interactuar con las diferentes partes interesadas que forman parte de las unidades de gestión para lograr articular actividades desde los servicios TI hacia las operaciones misionales del Idartes.

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.

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

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 la 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 (Stakeholder)	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.

Propósitos

- 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 las Entidades.
- Establecer procedimientos de seguridad que permitan a las Entidades 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.

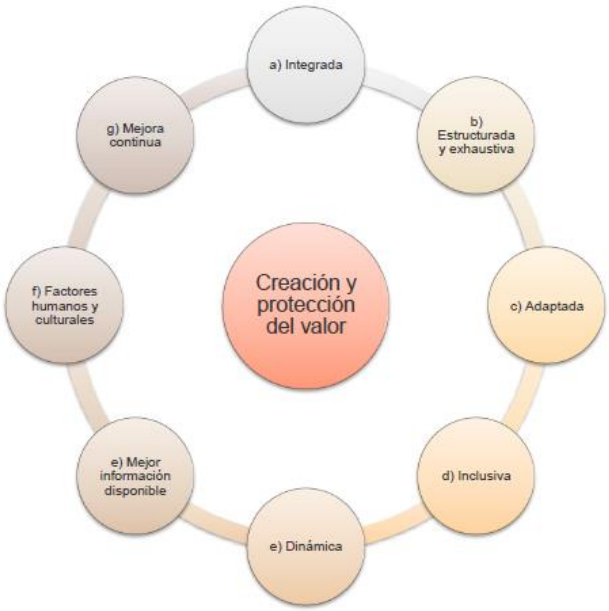

Ilustración. Principios. Norma ISO 31000:2018 2da. edición

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.

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 de los procesos	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

MARCO DE REFERENCIA

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

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:

Línea Estratégica
Primera Línea de Defensa
Segunda Línea de Defensa
Tercera Línea de Defensa.

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
		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

Línea de defensa	Rol	Responsabilidad
		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

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.

Beneficios

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

TRATAMIENTO DEL RIESGO

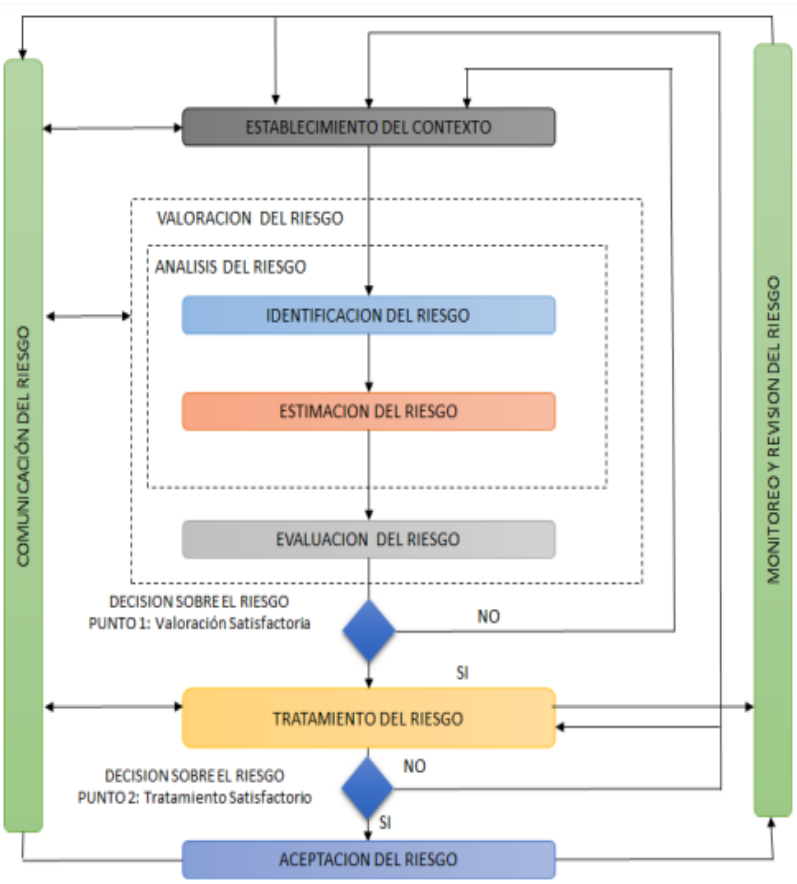

Ilustración. Proceso de gestión del riesgo de la seguridad de la información

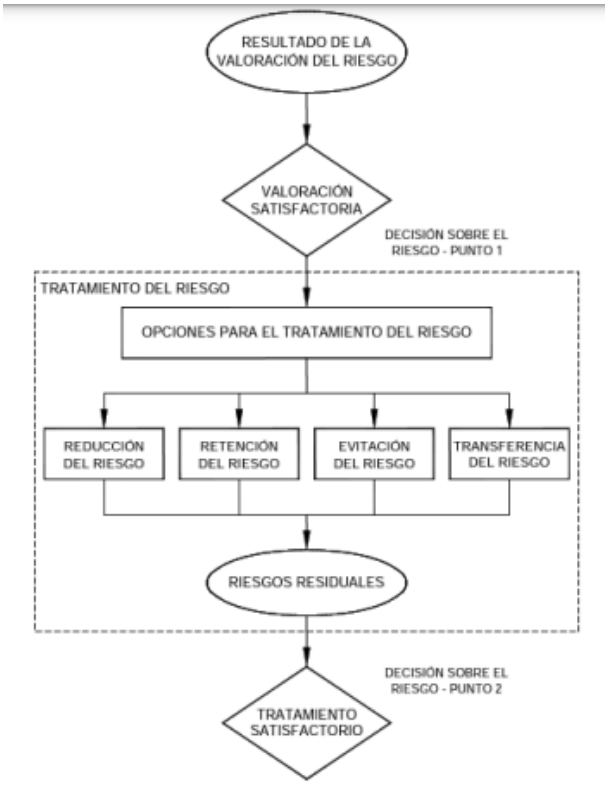

Ilustración. Tratamiento del riesgo Norma ISO 27005

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.

TIPO	**NIVEL**	**DESCRIPTOR**	**DESCRIPCIÓN** En caso que el riesgo se materialice el impacto y afectación sería…
	1	INSIGNIFICANTE	Se afecta a una persona en particular.

TIPO	NIVEL	DESCRIPTOR	DESCRIPCIÓN En caso que el riesgo se materialice el impacto y afectación sería…
CONFIDENCIALIDAD EN LA INFORMACIÓN	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 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

Opción de manejo del riesgo

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

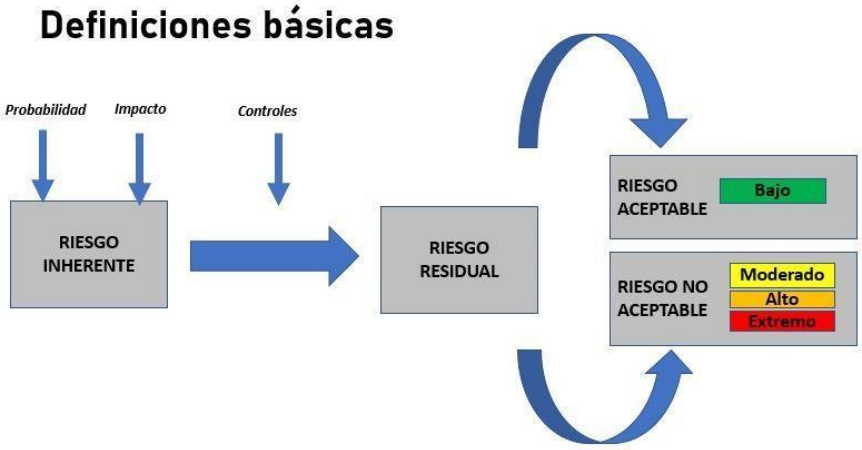

Ilustración. Aceptación de riesgo. Fuente propia

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 2021 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.

ID del riesgo
R01
Riesgo
Pérdida de disponibilidad TI
Análisis
En Idartes se puede presentar amenazas materializando vulnerabilidades como la pérdida o daño total o parcial de los equipos de cómputo, servidores y equipos activos causando pérdida de integridad e indisponibilidad de la información, dado que la información no se encuentra disponible en el momento que se necesita para cumplir la operación o funciones propias en la Entidad debido a que la información como un activo vital para la gestión institucional no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones, y por 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 las funciones y operaciones, así como por el 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. En este sentido se contempla este riesgo teniendo en cuenta que la administración de la continuidad de los servicios TI y las operaciones de la entidad no puede concebirse como una disciplina exclusiva de la Oficina asesora de planeación y tecnologías de la información, sino que debe formar parte integral de la disciplina de continuidad del negocio y debe estar coordinada a nivel institucional dado que la pandemia por COVID-19 ha obligado a una transformación digital de la misión institucional desde las diferentes unidades de gestión y por ende no tendría ningún sentido tener servicios y sistemas TI funcionales sin contar con la interoperabilidad con el recurso humano entre otros.
Probabilidad
Posible
Impacto
Mayor
Opción de manejo
Reducir

ID del riesgo
R02
Riesgo
Posible afectación de la confidencialidad, integridad y disponibilidad de la información
Análisis

En las unidades de gestión existen vulnerabilidades en la seguridad de la información dado que no se realiza un seguimiento a las bitácoras de control de acceso y los seguimientos a actividades para evitar que la información pueda ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas de información o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente, y contemplando que la información no se encuentra disponible por ausencia o falla en los sistemas de información y servicios tecnológicos que hacen parte de los procesos u operaciones de las diferentes áreas se puede afectar la operación de la entidad con amenazas de acceso indebido a los sistemas y a la información de los mismos aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano. Así mismo, se ha evidenciado que en el marco de la seguridad de la información que se utiliza en Idartes para proteger los datos que tiene, maneja y dispone, se deben contemplar vulnerabilidades como las generadas por las nuevas tecnologías del trabajo en casa a raíz de la pandemia que han modificado la forma de utilizar la seguridad de la información a gran velocidad.
Probabilidad
Probable
Impacto
Mayor
Opción de manejo
Reducir

ID del riesgo
R03
Riesgo
Fallas en la infraestructura tecnológica hardware/software 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 estar derivado de un tratamiento inadecuado de la información y correcto uso por desconocimiento de políticas, controles y buenas prácticas que son causa directa de las fallas en el hardware y software que soporta la infraestructura tecnológica de Idartes, y por ende permitir en cierto momento que se presenten errores en el control y mantenimiento que evite una posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente. 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, y tomar las medidas para que no se repitan o se materialicen aprovechando el uso con falta de controles de la interacción de la información que se hace actualmente a través de dispositivos móviles y ordenadores portátiles de Idartes y personales, y 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
Probable
Impacto
Moderado
Opción de manejo
Reducir

ID del riesgo
R04
Riesgo
Afectación por accesos no permitidos a información crítica de la Entidad
Análisis
La información debe ser protegida apropiadamente contra el acceso no autorizado, modificación, divulgación, pérdida o destrucción, sin importar la fuente en donde esté almacenada (computadores, librerías, portátiles, medios extraíbles como discos duros externos, USB, DVD, cintas backup, Etc., contratos, documentos, comunicaciones, etc.). Desde éste punto de vista, es importante determinar el papel que cumplen las unidades de gestión, partes internas o externas y funcionarios que por diversos motivos están involucrados en el tratamiento de la información del Idartes.
Probabilidad
Probable
Impacto
Moderado
Opción de manejo
Reducir

ID del riesgo
R05
Riesgo
Pérdida de integridad de la información por compartir información de aplicativos y sistemas de información con entidades externas permitiendo acceso a código e información
Análisis
En el marco de la interoperabilidad que realiza la entidad con otras entidades externas, así como con aplicaciones y aplicativos de la entidad, se gestiona un tráfico bidireccional, la administración de información en las unidades de gestión y en organizaciones con quienes se comparte información es un proceso cada vez más vulnerable frente al riesgo de pérdida de la información, razón por la cual se deben implementar controles que permitan mitigar dichos riesgos, siendo imperativo conocer los posibles factores de riesgo a los cuales se encuentran expuestos.

Probabilidad
Probable
Impacto
Moderado
Opción de manejo
Reducir

Objetivos del 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
- Decidir si el riesgo residual es aceptable o no aceptable
- Actuar si el riesgo no es aceptable y efectuar tratamiento adicional.

MATRIZ DE TRATAMIENTO DE RIESGOS

Identificación

Tipo de Activo de Información	Activo de Información	IDENTIFICACIÓN DEL RIESGO					
		Nro	Propiedad que afecta el Riesgo	Descripción del Riesgo	Responsable de determinar la materialización del riesgo	Amenazas	Causa
Información	Sistemas de información y aplicaciones de Software	1	Perdida de disponibilidad	Posible interrupción de la continuidad de los servicios TI u operaciones de la entidad	Oficial de Seguridad de la Información	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos	Retraso en la salida de información de los sistemas
						No hay sede de respaldo ante desastre	No se cuenta con equipos de respaldo
						Dificultad en el soporte y acceso a la información	No hay estandarización en los lineamientos para la construcción de software con calidad y seguridad
						Los sistemas y aplicaciones suceptibles a ataques de seguridad	No se cuenta con el debido aseguramiento de las aplicaciones en desarrollos

Tipo de Activo de Información	Activo de Información	IDENTIFICACIÓN DEL RIESGO					
		Nro	Propiedad que afecta el Riesgo	Descripción del Riesgo	Responsable de determinar la materialización del riesgo	Amenazas	Causa
Información	Información y datos de la entidad	2	Perdida de Integridad	Posible afectación de la confidencialidad, integridad y disponibilidad de la información	Oficial de Seguridad de la Información	Deficiencia en la autorización de permisos y respaldos de la información	Debido a un Almacenamiento sin protección
						Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	no se tienen controles de seguridad física a espacios donde se custiodia el almacenamiento
						Ausencia de reportes de fallas en los registros de administradores y operadores	no se realiza un seguimiento y control de la manipulacion de los medios de almacenamiento
Hardware plataforma tecnologica	Dispositivos de Tecnologías de información-Hardware	3	Perdida de disponibilidad	Fallas en la infraestructura tecnológica hardware/software que respalda y apoya los servicios tecnológicos de la entidad	Oficial de Seguridad de la Información	Respuesta inadecuada de mantenimiento de servicio	Debido a unas actividades de mantenimiento insuficiente
						las adecuaciones de infraestructura para adecuaciones de sedes es insuficiente	No existen aprovisionamientos adecuados para sedes de la entidad
						Entrenamiento insuficiente en seguridad	los medios de almacenamiento son mal manipulados por el personal que los administra

Tipo de Activo de Información	Activo de Información	IDENTIFICACIÓN DEL RIESGO					
		Nro	Propiedad que afecta el Riesgo	Descripción del Riesgo	Responsable de determinar la materialización del riesgo	Amenazas	Causa
Información	Servicios	4	Perdida de confidencialidad	Afectacion por accesos no permitidos a informacion critica de la Entidad	Oficial de Seguridad de la Información	Ausencia de procedimiento formal para la autorización de la información disponible	Deficiencia en la actualización y control de usuarios activos e inactivos, credenciales de accesos a los sistemas de información, aplicativos, herramientas tecnológicas y servicios de red
						Asignación errada de los derechos de acceso	Falta de actualización políticas para administración y uso de credenciales de acceso
						Falla de conciencia acerca de la seguridad	Las personas no custodian debidamente y no dan buen uso a sus credenciales de acceso

Tipo de Activo de Información	Activo de Información	IDENTIFICACIÓN DEL RIESGO					
		Nro	Propiedad que afecta el Riesgo	Descripción del Riesgo	Responsable de determinar la materialización del riesgo	Amenazas	Causa
Información	Sistemas de información y aplicaciones de Software	5	Perdida de Integridad	Compartir informacion de aplicativos y sistemas de informacion con entidades externas permitiendo acceso a codigo e informacion	Oficial de Seguridad de la Información	perdida de la integridad y confidencialidad de la información por acceso indebido	no existe documentacion para lineamiento de entrega de repositorio a las entidades externas
						perdida de la accesibilidad de la informacion	El repositorio esta en ela nube por tanto si no hay una conexión constante de internet no se guardan los ultimos cambios realizados
						Ausencia de documentos o acuerdos de acceso y uso de la informacion de carácter pública clasificada y/o pública reservada contenida en cualquier aplicativo o sistema que reciba de la Entidad	No existe lienamientos oficiales que permitan definir las condiciones de acceso a la informacion asi como las implicaciones de incumplimiento por la perdida de la integridad o disponibilidad de la informacion de los sistemas y aplicativos compartidos

Análisis y tratamiento

IDENTIFICACIÓN DEL RIESGO		ANÁLISIS DEL RIESGO INHERENTE			IDENTIFICACIÓN DE CONTROLES			RIESGO RESIDUAL		
Nro	Descripción del Riesgo	Probabilidad	Impacto	Zona de Riesgo	Opciones de manejo del riesgo	Descripción del control	Responsable de ejecutar el control	Probabilidad	Impacto	Zona de Riesgo Residual
1	Posible interrupción de la continuidad de los servicios TI u operaciones de la entidad	Posible	Mayor	ZONA DE RIESGO ALTA	Reducir	Respaldos de archivos funcionales y tecnicos Generar instrumentos de aseguramiento de los sistemas	Grupo TI	**Posible**	**Menor**	ZONA DE RIESGO MODERADA

IDENTIFICACIÓN DEL RIESGO		ANÁLISIS DEL RIESGO INHERENTE			IDENTIFICACIÓN DE CONTROLES			RIESGO RESIDUAL		
Nro	Descripción del Riesgo	Probabilidad	Impacto	Zona de Riesgo	Opciones de manejo del riesgo	Descripción del control	Responsable de ejecutar el control	Probabilidad	Impacto	Zona de Riesgo Residual
2	Posible afectación de la confidencialidad, integridad y disponibilidad de la información	Probable	Mayor	ZONA DE RIESGO ALTA	Reducir	Generacion de protocolos de autenticacion Generacion de sistemas de seguridad fisica identificacion de recursos para control y seguimiento de accesos	Grupo TI	**Posible**	**Menor**	ZONA DE RIESGO MODERADA
3	Fallas en la infraestructura tecnológica hardware/software que respalda y apoya los servicios tecnológicos de la entidad	**Probable**	Moderado	ZONA DE RIESGO ALTA	Reducir	Uso de instrumentos de seguimiento a actividades de mantenimiento Gestion de requerimientos para diagnosticos Generacion de capacitaciones y entrenamiento en temas de seguridad	Grupo TI	**Posible**	**Menor**	ZONA DE RIESGO MODERADA

IDENTIFICACIÓN DEL RIESGO		ANÁLISIS DEL RIESGO INHERENTE			IDENTIFICACIÓN DE CONTROLES			RIESGO RESIDUAL		
Nro	Descripción del Riesgo	Probabilidad	Impacto	Zona de Riesgo	Opciones de manejo del riesgo	Descripción del control	Responsable de ejecutar el control	Probabilidad	Impacto	Zona de Riesgo Residual
4	Afectacion por accesos no permitidos a informacion critica de la Entidad	**Probable**	**Moderado**	ZONA DE RIESGO ALTA	Reducir	Depuracion de usuarios inactivos Autodiagnosticos y documentos para generacion de politicas y lineamientos Creacion de instrumentos documentles para gestion de credenciales	Grupo TI	**Posible**	**Menor**	ZONA DE RIESGO MODERADA

Nro	Descripción del Riesgo	Probabilidad	Impacto	Zona de Riesgo	Opciones de manejo del riesgo	Descripción del control	Responsable de ejecutar el control	Probabilidad	Impacto	Zona de Riesgo Residual
5	Compartir informacion de aplicativos y sistemas de informacion con entidades externas permitiendo acceso a codigo e informacion	Probable	Moderado	ZONA DE RIESGO ALTA	Reducir	Repositorio con seguridad de la informacion Se creo el servidor para configuracion de seguridad perteneciente a la entidad El oficial de seguridad de la informacion adelanta un modelo de acuerdo de confidencialidad para la entidad que aplique a los diferentes convenios	Grupo TI	**Posible**	**Menor**	ZONA DE RIESGO MODERADA

Controles e indicador

IDENTIFICACIÓN DEL RIESGO						
Nro	**Descripción del Riesgo**	**Controles**	**Actividad**	**Responsable de Ejecutar el control**	**Periodo / Fecha de Ejecución**	**Indicador**
1	Posible interrupción de la continuidad de los servicios TI u operaciones de la entidad	Actualizar los acuerdos de servicio acorde a las politicas definidas para sistemas de informacion y aplicacciones	Actualizacion de documento de ANS para sistemas de informacion	OAP-TI	Diciembre 31 de 2022	EFICACIA: Índice de cumplimiento de las actividades programadas (# de actividades cumplidas/# de actividades programadas *100)
		Generar espacios de respaldo y contingencia de los sistemas de informacion y aplicaciones	Creacion de documento de aprobacion de espacios para contingencia	OAP-TI	Diciembre 31 de 2022	
		Aplicar arquitectura hexagonal que estandarice los desarrollos de software de la entidad	Implementacion de Politica de desarrollo de software incluyendo la Arquitectura Hexagonal	OAP-TI	Diciembre 31 de 2022	
		Establecer politicas alineadas con procedimientos para el aseguramiento de sistemas de informacion y aplicaciones	Implementacion de Politica de desarrollo de software	OAP-TI	Diciembre 31 de 2022	

IDENTIFICACIÓN DEL RIESGO						
Nro	**Descripción del Riesgo**	**Controles**	**Actividad**	**Responsable de Ejecutar el control**	**Periodo / Fecha de Ejecución**	**Indicador**
2	Posible afectación de la confidencialidad, integridad y disponibilidad de la información	Generar procesos de autenticacion para aseguramiento de la informacion	Integracion de Single site on	OAP-TI	Diciembre 31 de 2022	EFICACIA: Índice de cumplimiento de las actividades programadas (# de actividades cumplidas/# de actividades programadas *100)
		Generar acciones de seguridad fisica y del entorno	Implementar seguridad biometrica	OAP-TI	Diciembre 31 de 2022	
		Generar medios de seguimiento y control para acceso a la informacion	Implementacion de bitacoras digitales de acceso a la informacion y seguimiento de logs	OAP-TI	Diciembre 31 de 2022	
3	Fallas en la infraestructura tecnológica hardware/software que respalda y apoya los servicios tecnológicos de la entidad	Generar actividades continuas de mantenimiento a la infraestrucutra	Creacion de documento para seguimiento y control de mantenimientos	OAP-TI	Diciembre 31 de 2022	EFICACIA: Índice de cumplimiento de las actividades programadas (# de actividades cumplidas/# de actividades programadas *100)
		Coordinacion de adecuaciones a las sedes de la entidad	Creacion de documentos para adecuaciones de infraestrucutura de las sedes de la Entidad	OAP-TI	Diciembre 31 de 2022	
		Definicion de instrumentos documentales para lineamientos en uso de medios donde se maneja la informacion	Creacion de documentos para la seguridad de la informacion	OAP-TI	Diciembre 31 de 2022	

IDENTIFICACIÓN DEL RIESGO						
Nro	**Descripción del Riesgo**	**Controles**	**Actividad**	**Responsable de Ejecutar el control**	**Periodo / Fecha de Ejecución**	**Indicador**
4	Afectacion por accesos no permitidos a informacion critica de la Entidad	Adecuacion de plataforma para gestion de usuarios	Afinamiento de directorio activo	OAP-TI	Diciembre 31 de 2022	EFICACIA: Índice de cumplimiento de las actividades programadas (# de actividades cumplidas/# de actividades programadas *100)
		Seguimiento a avances en actividades de implementacion	Seguimiento planes de mejoramiento de autodiagnosticos TI	OAP-TI	Diciembre 31 de 2022	
		Seguimiento a actualizacion de procedimientos	Actiualizacion de procedimientos de gestion de tecnologias de la informacion	OAP-TI	Diciembre 31 de 2022	

IDENTIFICACIÓN DEL RIESGO						
Nro	Descripción del Riesgo	Controles	Actividad	Responsable de Ejecutar el control	Periodo / Fecha de Ejecución	Indicador
5	Compartir informacion de aplicativos y sistemas de informacion con entidades externas permitiendo acceso a codigo e informacion	Se requiere construccion de lineamientos para el uso y proteccion de la informacion que se incorpora al repositorio	Documento de protocolo para entrega y asignacion del repositorio a una entidad externa en el marco del convenio Documento de "Readme.md" que se encuentra en los repositorios que se entregan a la entidades externas	OAP-TI	Diciembre 31 de 2022	EFICACIA: Índice de cumplimiento de las actividades programadas (# de actividades cumplidas/# de actividades programadas *100)
		garantizar el funcionamiento de un repositorio de respaldo para gestion de la informacion	Configuracion de servidor con GitLab	OAP-TI	Diciembre 31 de 2022	
		Crear modelo de acuerdo de confidencialidad aplicado a entrega de codigos e informacion a entidades externas a traves de modalidades de convenio u otras relacionadas	Modelo a acuerdo de confidencialidad con roles y responsabilidades para entrega a entidades externas	OAP-TI	Diciembre 31 de 2022	

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 deberían ser incluidos en todas las actividades de gestión del desempeño, la medición informará organización.

Se debe revisar periódicamente por cada responsable de los procesos al interior de las entidades, 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.

NORMATIVA

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.
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	Conpes	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	Conpes	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.

Tipo de norma	Entidad que expide	Descripción normativa
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 Justicia	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Conpes 3701 de 2011	Conpes	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	Idartes	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	Alcaldía Mayor de	Por el cual se dictan medidas para la aplicación del Teletrabajo en

Tipo de norma	Entidad que expide	Descripción normativa
de 2013	Bogotá	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	Idartes	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.
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	Conpes	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	Secretaría General	Por la cual se modifica la Resolución 305 de 2008 de la CDS

Tipo de norma	Entidad que expide	Descripción normativa
de 2017	Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas - 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
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.

Tipo de norma	Entidad que expide	Descripción normativa
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	Conpes	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)
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	Conpes	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	Departamento	Estableciendo los lineamientos generales en el uso y operación de los

Tipo de norma	Entidad que expide	Descripción normativa
de 2020	Administrativo De La Función Pública	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

RECURSOS DOCUMENTALES

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA.
Guía para la administración del riesgo.
Bogotá. Diciembre 2014.

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
Guía para la administración del riesgo y diseño de controles en entidades públicas. Versión 5
Bogotá. 2020

ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN – ISO
Norma Internacional ISO 31000.
Ginebra, Suiza 2018