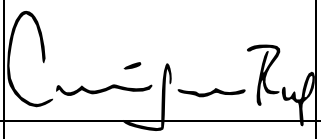
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Objetivo:
Establecer la gestión para el tratamiento de los riesgos de la seguridad y privacidad de la información en el Instituto Distrital de las Artes - 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
15-01-2021	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	14/01/2021	Actualización de riesgos de seguridad y privacidad de la información

Oficinas participantes			
Oficina Asesora de Planeación y Tecnologías de la Información			
Elaboró	Aprobó	Revisó	Avaló
Ingeniero Andrés Briceño Díaz	**Edgar Cipagauta Pedraza**	**Camila Crespo Murillo**	**Carlos Gaitán Sánchez**
			
Contratista Oficial de Seguridad de la Información	Profesional Universitario OAP-TI	Contratista Profesional OAP-TI	Jefe Oficina Asesora de Planeación y Tecnologías de la Información

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 controle s 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 (consecuencias) 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

Riesgo	Efecto de la incertidumbre sobre los objetivos.
Gestión del riesgo	Actividades definidas para dirigir y controlar una organización con respecto al riesgo
Parte interesada	
Fuente de riesgo	Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo

Riesgo	**Efecto de la incertidumbre sobre los objetivos.**
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.
Consecuencia	Resultado de un evento que afecta a los objetivos
Probabilidad	Es la probabilidad que algo suceda en un determinado tiempo
Control	Medida que mantiene y/o modifica un riesgo
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
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.
Incertidumbre	Es el desconocimiento si un hecho o situación ocurrirá.
Impacto	Resultados si se llegara a materializar el riesgo identificado.

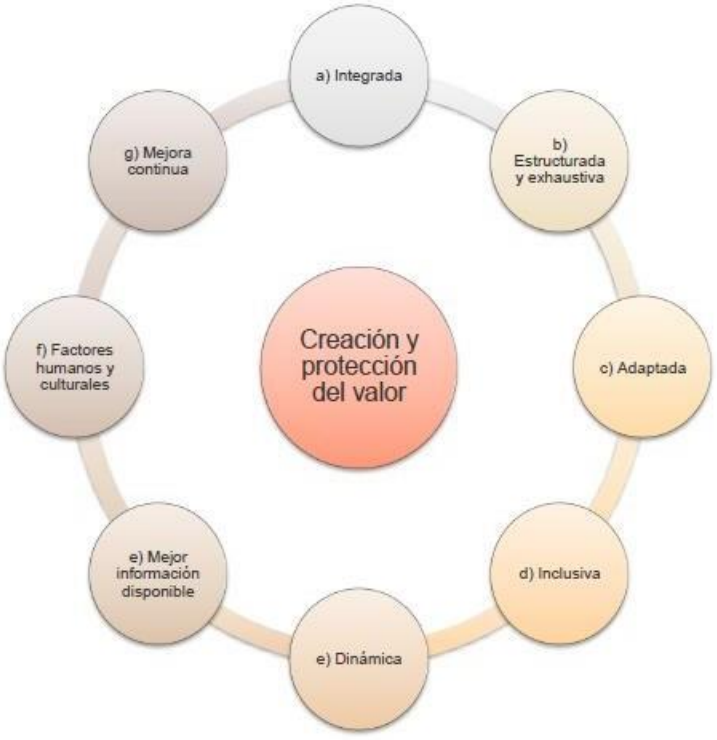


Ilustración. Principios. Norma ISO 31000:2018 2da. edición

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 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

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 Versión 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:

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
		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

Línea de defensa	Rol	Responsabilidad
Primera línea	Responsable del proceso de tecnología de la información	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 estos.
		Revisar la aplicación de los controles e instrumentos de gestión relacionados al tratamiento y la gestión de riesgos

TRATAMIENTO DEL RIESGO

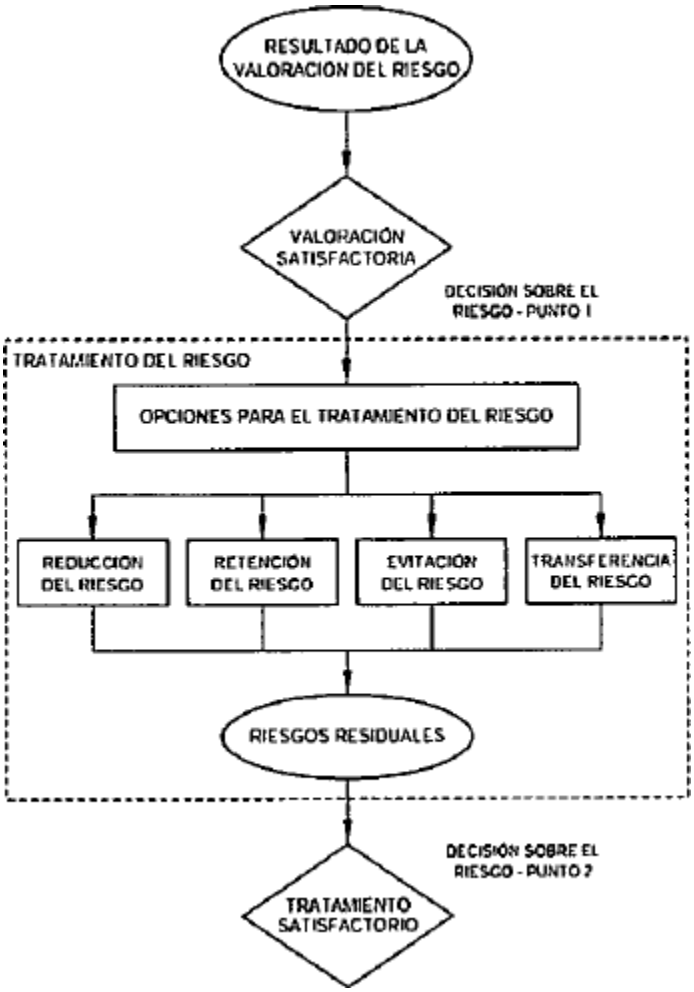


Ilustración. tratamiento del riesgo Norma ISO 27005

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 1 vez en los últimos 5 años.

TABLA DE PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN (FACTIBILIDAD)**	**FRECUENCIA**
3	POSIBLE	El evento podría ocurrir en algún momento.	Al menos 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 DE IMPACTO						
TIPO		**NIVEL**		**DESCRIPTOR**		**DESCRIPCIÓN** En caso de que el riesgo se materialice el impacto u 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.

TABLA DE IMPACTO						
TIPO		**NIVEL**		**DESCRIPTOR**		**DESCRIPCIÓN** En caso de que el riesgo se materialice el impacto u afectación sería…
		4		MAYOR		Se presentarían 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

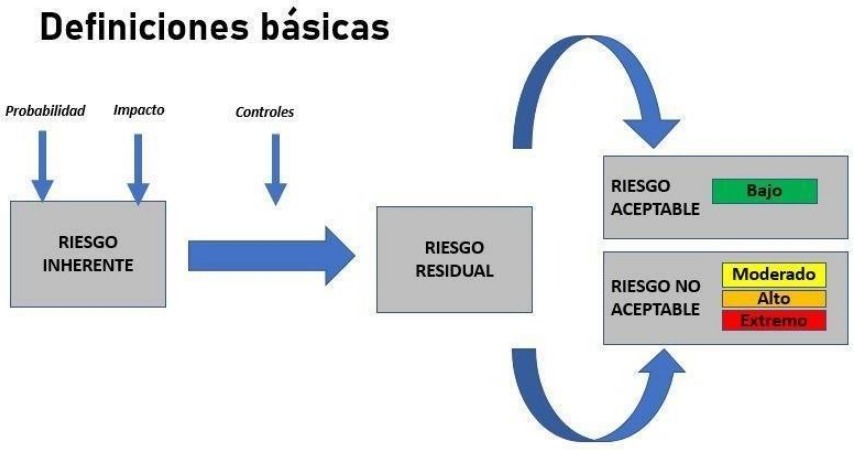


Ilustración. Aceptación de riesgo. Fuente propia

Identificación de los riesgos Idartes

El objetivo de la identificación de riesgos es determinar qué podría suceder que cause una pérdida potencial y llegar a comprender el cómo, dónde y por qué podría ocurrir pérdida. 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 ser asociados 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 la continuidad de los servicios TI u operaciones de la entidad
Análisis
En el Idartes se puede presentar amenazas materializando vulnerabilidades como la pérdida o daño total o parcial de los equipos de cómputo, servidores y equipos activos, lo que claramente impacta en las características de integridad e indisponibilidad de la información en el momento que se necesita para cumplir la operación o funciones propias en la Entidad. También esta no disponibilidad de la información como un activo vital para la gestión institucional, se puede presentar por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones, por fallas en los equipos tecnológicos o redes de comunicación debido a agentes externos, ambientales, intencionales o no intencionales. Así mismo, se puede presentar 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 integrar 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
Probable
Impacto
Moderado
Opción de manejo
Reducir

ID del riesgo
R02
Riesgo

Daño a 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 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
Casi seguro
Impacto
Mayor
Opción de manejo
Evitar

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

Matriz de tratamiento de riesgos						
ID del riesgo	**Escenario**	**Tratamiento**	**Controles**	**Recursos**	**Fecha máxima de aplicación**	**Responsable**
R01	Se presenta fallas de la continuidad de los servicios TI afectando las operaciones de la entidad	Reducir	Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Matriz de activos de información	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente	Controlador de dominio	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Aplicar perímetros de seguridad para proteger áreas que contengan información confidencial o	Minuta de empresa vigilancia	31/12/2021	Oficina Asesora de planeación y tecnologías

Matriz de tratamiento de riesgos						
ID del riesgo	**Escenario**	**Tratamiento**	**Controles**	**Recursos**	**Fecha máxima de aplicación**	**Responsable**
			crítica e instalaciones de manejo de información.			de la información
			Implementar en las áreas seguras una protección mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	Entrega de medios de acceso previa validación de autorización por minuta de guardas	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Aplicar los mecanismos de seguridad a los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	Documento Acuerdo Niveles de Servicio TI	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Aplicar requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Cláusulas en minutas contractuales	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Aplicar procedimiento de control de cambios a los sistemas dentro del ciclo de vida de desarrollo	Documento Procedimiento de Mantenimiento y Desarrollo de Software	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Implementar un plan de contingencia donde idartes pueda establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Documento Plan de contingencia	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
R02	Se evidencian daños a la confidencialidad, integridad y disponibilidad	Reducir	Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización	Documento Plan de Seguridad y Privacidad de la Información	31/12/2021	Oficina Asesora de planeación y tecnologías

Matriz de tratamiento de riesgos						
ID del riesgo	**Escenario**	**Tratamiento**	**Controles**	**Recursos**	**Fecha máxima de aplicación**	**Responsable**
	de la información de la entidad					de la información
			Implementar un proceso formal de registro y de cancelación de cuentas de usuario para habilitar la asignación de los derechos de acceso.	Controlador de dominio	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Restringir de acuerdo con los lineamientos de control de acceso a la información y a las funciones de los sistemas de las aplicaciones	Documento Políticas de Seguridad de la Información	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Documento Formato de Levantamiento de Requerimientos Funcionales	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Implementar controles de detección, de prevención y de recuperación contra códigos maliciosos, y combinarlos con la toma de conciencia apropiada de los usuarios.	Herramientas de seguridad perimetral	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Realizar copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente, de acuerdo con una política de copias de respaldo acordada.	Documento Copia y restauración de la Información	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Documento Incidentes de Seguridad de la Información	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
R03	Se comprueban fallas en los equipos,	Evitar	Ubicar y proteger los equipos para reducir los riesgos de amenazas, peligros ambientales y las	Datacenter Centros de cableado	31/12/2021	Oficina Asesora de planeación y tecnologías

Matriz de tratamiento de riesgos						
ID del riesgo	**Escenario**	**Tratamiento**	**Controles**	**Recursos**	**Fecha máxima de aplicación**	**Responsable**
	sistemas y aplicaciones que respaldan los servicios tecnológicos de la entidad		posibilidades de acceso no autorizado.	Centros de respaldo		de la información
			Proteger los equipos ante fallas de fluido eléctrico y otras interrupciones causadas por daños en los servicios públicos de soporte.	Sistema de Aire Sistema UPS	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Proteger el cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información contra interceptaciones, interferencia o daño.	Cuartos de cableado estructurado y Backbone	31/12/2021	Oficina Asesora de planeación y tecnologías de la información
			Mantener correctamente los equipos para asegurar su disponibilidad e integridad continua.	Documento Plan de Mantenimiento de Equipos	31/12/2021	Oficina Asesora de planeación y tecnologías de la información

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 a la 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

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

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN 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

ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN – ISO
Norma Internacional ISO 27001.
Ginebra, Suiza 2018