





SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN			
SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
Código:	Versión :02	Fecha de emisión: 2024	Pagina 1

SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :02	Fecha de emisión: 2024	Pagina 2

INTRODUCCIÓN	3
1. OBJETIVO.....	3
2. ALCANCE PARA LA ADMINISTRACIÓN DEL RIESGO	3
3. NORMATIVIDAD	3
4. DEFINICIONES	4
5. ORGANIZACIÓN PARA LA GESTIÓN DEL RIESGO	7
5.1 Definición de Roles y Responsabilidades	7
6. IDENTIFICACIÓN DE RIESGOS.....	7
6.1 Establecimiento del Contexto	7
6.2 Identificación, Clasificación y Valoración de Activos.....	7
6.3 Metodología para el Análisis de Riesgos	8
6.3.1 Identificación de Vulnerabilidades	9
6.3.2 Identificación de Amenazas.....	13
6.3.3 Descripción de Consecuencias.....	20
6.3.4 Definición de Riesgos.....	20
6.3.5 Probabilidad de ocurrencia.....	20
6.3.6 Nivel de Impacto.....	21
6.3.7 Valoración del Riesgo	22
6.4 Plan de Tratamiento	22
6.4.1 Estrategia de Tratamiento de Riesgo.....	22
6.4.2 Identificación de Controles.....	23
7. MAPA DE RIESGO RESIDUAL.....	24
8. TRATAMIENTO DEL RIESGO	24
9. SEGUIMIENTO Y REVISIÓN.....	24
10. REGISTRO E INFORME.....	24
11. CAPACITACIÓN	25

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :02	Fecha de emisión: 2024	Pagina 3

INTRODUCCIÓN

La información que hace parte del Instituto para el Desarrollo de Antioquia - IDEA es crucial para su correcto desempeño y es primordial para el cumplimiento de sus objetivos. Es necesario que el Instituto tenga un enfoque sistemático para la administración del riesgo en la seguridad de la información y ciberseguridad, siendo adecuado para su entorno y en particular, debería cumplir los lineamientos de toda la gestión del riesgo Institucional.

La administración del riesgo en la seguridad de la información y ciberseguridad debe aplicar a todo el Instituto y debe ser una parte integral de todas las actividades de gestión de seguridad de la información y ciberseguridad que se realicen, analizando siempre lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo.

Esta guía está basada en las normas técnicas NTC-ISO 27005, ISO 31000 y en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas de la Función Pública, y forma parte del Sistema de Gestión de Ciberseguridad y Seguridad de la Información del IDEA.

1. OBJETIVO


Establecer un marco de administración de riesgos de seguridad de la información y ciberseguridad, que permita identificar las amenazas y vulnerabilidad que puedan afectar la confidencialidad, integridad y disponibilidad de la información del Instituto.

2. ALCANCE PARA LA ADMINISTRACIÓN DEL RIESGO

La administración del riesgo de seguridad de la información y ciberseguridad es aplicable a todos los procesos y activos de información del IDEA.


3. NORMATIVIDAD

Ver normograma.


	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
			Pagina 4

4. DEFINICIONES


- **ACTIVO DE INFORMACIÓN:** Es toda la información misional, operativa y administrativa que el Instituto recibe o produce y que es considerada de alta validez. Incluye la información impresa, escrita, transmitida o almacenada en cualquier medio electrónico, equipo de cómputo, software, hardware y datos contenidos en registros, archivos, bases de datos, videos e imágenes.
- **AMENAZAS:** Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización
- **APETITO AL RIESGO:** Magnitud y tipo de riesgo que una organización está dispuesta a aceptar
- **CAUSA:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **CIBERAMENAZA:** Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.
- **CIBERATAQUE:** Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.
- **CIBERESPACIO:** Entorno complejo resultante de la interacción de personas, software y servicios en internet a través de dispositivos tecnológicos conectados a dichas red, el cual no existe en ninguna forma física.
- **CIBERIESGO:** Posible resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.
- **CIBERSEGURIDAD:** Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio
- **CSIRT (Computer Security Incident Response Team) :** Equipo responsable del desarrollo de medidas preventivas y de respuesta a incidentes informáticos.
- **CONSECUENCIA:** Los efectos o situaciones resultantes de la materialización del riesgo que impacta en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **CONTEXTO EXTERNO:** Ambiente externo en el cual la organización busca alcanzar sus objetivos.

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :02	Fecha de emisión: 2024	Pagina 5

- **CONTEXTO INTERNO:** Ambiente interno en el cual la organización buscar alcanzar sus objetivos
- **CONTROL:** Medida que modifica al riesgo. Medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- **ESTABLECIMIENTO DEL CONTEXTO:** Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo.
- **EVALUACIÓN DEL CONTROL:** Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces
- **EVALUACIÓN DEL RIESGO:** Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles.
- **FRECUENCIA:** Medición del número de ocurrencias por unidad de tiempo.
- **GESTIÓN DEL RIESGO:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo
- **GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL:** Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.
- **IDENTIFICACIÓN DEL RIESGO:** Proceso para encontrar, reconocer y describir el riesgo
- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones.

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :02	Fecha de emisión: 2024	Pagina 6

- **IMPACTO:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **MAPA DE RIESGOS:** Documento con la información resultante de la gestión del riesgo
- **NIVEL DE RIESGO:** Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad
- **PROBABILIDAD:** Posibilidad de ocurrencia del riesgo, puede ser medida con criterios de frecuencia o factibilidad.
- **REDUCCIÓN DEL RIESGO:** Acciones que se toman para disminuir la probabilidad, las consecuencias negativas o ambas, asociadas a un riesgo.
- **RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN:** una amenaza determinada explote la vulnerabilidad de un activo pudiendo causar un daño.
- **RIESGO INHERENTE:** Es aquel riesgo al que se enfrenta la entidad en ausencia de controles o acciones que mitiguen la probabilidad o el impacto.
- **RIESGO RESIDUAL:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.
- **TRATAMIENTO DEL RIESGO:** Proceso para modificar el riesgo
- **TOLERANCIA AL RIESGO:** Son los niveles aceptables de desviación relativa a la consecución de objetivos.
- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.
- **VALORACIÓN DEL RIESGO:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo
- **VULNERABILIDAD:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :02	Fecha de emisión: 2024	Pagina 7

5. ORGANIZACIÓN PARA LA GESTIÓN DEL RIESGO

5.1 Definición de Roles y Responsabilidades

Se describen todos los roles y responsabilidades de la Junta Directiva, Gerente General, Directivos, Oficina Gestión del Riesgos, Dirección de Sistemas, Control Interno, Comité de Seguridad de la Información y Ciberseguridad, Servidores Públicos y Contratistas.

6. IDENTIFICACIÓN DE RIESGOS

En esta etapa se deben establecer las fuentes o factores de riesgo, las vulnerabilidades, las amenazas, los eventos o riesgos, y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas (NTC ISO31000, Numeral 2.15).

6.1 Establecimiento del Contexto


Es la definición de los parámetros internos y externos que tomaran en consideración para la administración del riesgo, esto ayuda en la identificación de las causas de los riesgos.

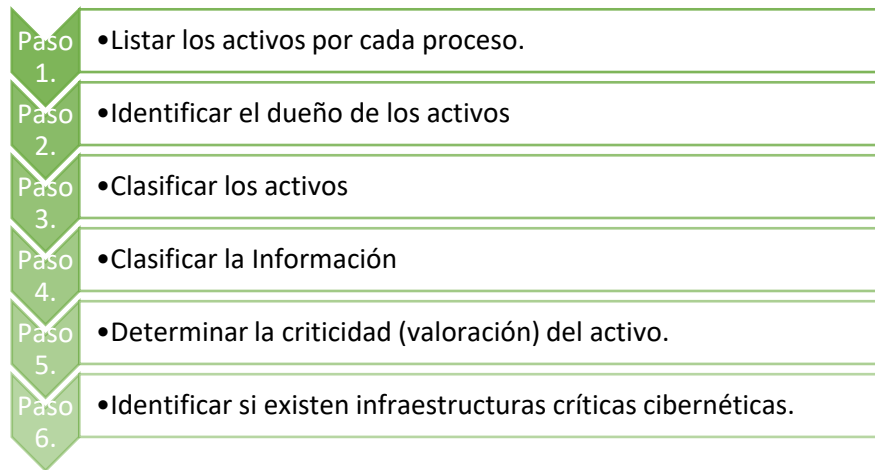
En la medida en que se vayan presentando cambios en el contexto, se pueden presentar nuevos eventos o riesgos que deben ser atendidos como parte del proceso.

Se puede tener en cuenta el análisis situacional y las herramientas utilizadas para establecer el PEI, enfocándose en la seguridad de los activos de información.

6.2 Identificación, Clasificación y Valoración de Activos

El proceso de identificación, clasificación y valoración de activos de información se realiza de acuerdo a la “Guía para la Gestión de Activos de Información” la cual forma parte del Sistema de Gestión de Ciberseguridad y Seguridad de la Información del IDEA:

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
			Pagina 8



6.3 Metodología para el Análisis de Riesgos

El propósito de la identificación del riesgo es determinar que podría suceder que cause una pérdida potencial, las preguntas claves para la identificación del riesgo permiten determinar:

¿QUÉ PUEDE SUCEDER?

Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER?


Establecer las causas a partir de los factores determinados en el contexto

¿CUÁNDO PUEDE SUCEDER?

Determinar de acuerdo al desarrollo del proceso

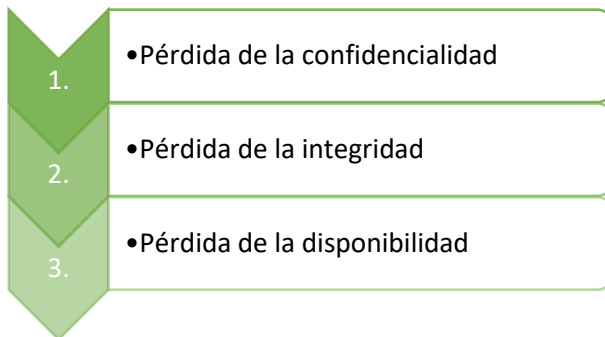
¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?

Determinar los posibles efectos por la materialización del riesgo

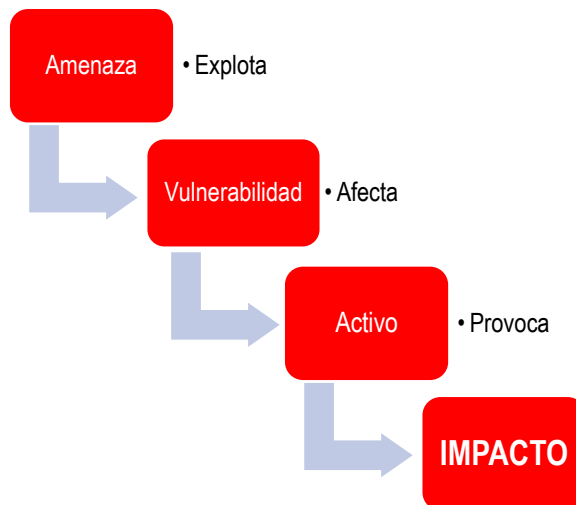
	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
			Pagina 9

Nota: En la descripción del riesgo se deben tener en cuenta las respuestas a las preguntas arriba mencionadas.

Se identificarán los siguientes tres (3) riesgos inherentes:




El siguiente diagrama muestra las relaciones entre conceptos:



6.3.1 Identificación de Vulnerabilidades

Acorde a los activos seleccionados para realizar el análisis de riesgo definidos según su criticidad (alto – medio), se realiza la identificación de vulnerabilidades. Estas son las fallas o debilidades que tiene un activo. Cuando la amenaza encuentra la vulnerabilidad surge el riesgo. La Vulnerabilidad se asemeja a la causa.

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
			Pagina 10

control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Conviene anotar que un control implementado de manera incorrecta o que funcione mal, o un control que utiliza de modo incorrecto podría por sí solo constituir una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente en el cual funcione.

Esto son algunos ejemplos de vulnerabilidades que se pueden tener en cuenta:

TIPO DE ACTIVO	VULNERABILIDAD
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Almacenamiento sin protección
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de terminación de sesión cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Ausencia de registros de auditoría
	Software ampliamente distribuido
	En términos de tiempo utilización de datos errados en los programas de aplicación
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas



SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN
SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC


Código:

Versión :02


Fecha de emisión:
2024

Pagina 11

	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descargue y uso no controlado de software
	Ausencia de copias de respaldo
	Ausencia de protección física de la edificación, puertas y ventanas
	Fallas en la producción de informes de gestión
Personal	Ausencia de personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia en seguridad
	Ausencia de mecanismos de monitoreo
	Trabajo no supervisado de personal externo o de limpieza
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de fallas
	Ausencia de identificación y autenticación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :02	Fecha de emisión: 2024	Pagina 12

	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
	Conexiones de red pública sin protección
Lugar	Uso inadecuado o descuido del control de acceso físico a las edificaciones y los recintos
	Ubicación en área susceptible de inundación
	Red energética inestable
	Ausencia de protección física de la edificación (puertas y ventanas)
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de proceso formal para la revisión de los derechos de acceso
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información
	Ausencia de auditorias
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de reportes de fallas en los registros de administradores y operadores
	Respuesta inadecuada de mantenimiento del servicio
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos
	Ausencia de procedimientos de control de cambios
	Ausencia de procedimiento formal para la documentación del MSPI
	Ausencia de procedimiento formal para la supervisión del registro del MSPI
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información
	Ausencia de planes de continuidad

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
			Página 13

	Ausencia de políticas sobre el uso de correo electrónico
	Ausencia de procedimientos para introducción del software en los sistemas operativos
	Ausencia de registros en bitácoras
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información
	Ausencia de política formal sobre la utilización de computadores portátiles
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de política sobre limpieza de escritorio y pantalla
	Ausencia de autorización de los recursos de procesamiento de información
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad
	Ausencia de revisiones regulares por parte de la gerencia
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales


Tabla 1. Fuente: ISO/IEC 27005:2009

6.3.2 Identificación de Amenazas

Acorde a los activos seleccionados para realizar el análisis de riesgo definidos según su criticidad (alto – medio), se realiza la identificación de amenazas.

Las amenazas tienen el potencial de causar daños a activos tales como información, procesos y sistemas. Pueden ser de origen natural o humano o podrían ser accidentales o deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización.

Algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
			Pagina 14

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos:

Deliberadas (D), fortuito (F) o ambientales (A).

D: acciones deliberadas que tienen como objeto los activos de la información

F: Acciones humanas que pueden dañar accidentalmente los activos de información

A: los incidentes que no se basa en acciones humanas.


TABLA DE AMENAZAS COMUNES		
TIPO	AMENAZA	ORIGEN
Daño Físico	Fuego	D, F, A
	Agua	D, F, A
	Destrucción del equipo o medios	D, F, A
	Polvo, corrosión, congelamiento	D, F, A
Eventos Naturales	Fenómenos Climáticos	A
	Fenómenos Sísmicos	A
	Inundación	A
Pérdida de los servicios esenciales	Fallas en el sistema de suministro de agua	D, F, A
	Fallas en el sistema de suministro de aire acondicionado	D, F, A
	Pérdida en el suministro de energía	D, F, A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debido a la radiación	Radiación electromagnética	D, F, A
Compromiso de la información	Intercepción de señales de interferencia comprometida	D
	Espionaje Remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F

Acciones autorizadas	no	Uso no autorizado del equipo	D
		Copia fraudulenta del software	D,
		Uso del software falso o copiado	D, F
		Corrupción de datos	D
		Procesamiento ilegal de datos	D
Compromiso de las funciones	de las	Error en el uso	D, F
		Abuso de derechos	D, F
		Falsificación de derechos	D
		Incumplimiento en la disponibilidad del personal	D, F

Tabla 2 Fuente: ISO/IEC 27005:2009

Fuentes de amenazas humanas, con o sin intención, proveedores y piratas informáticos:

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto. Ego. Rebelión. Estatus. Dinero.	Piratería. Ingeniería Social. Intrusión, accesos forzados al sistema. Acceso no autorizado al sistema.
Criminal de la Computación	Destrucción de la información. Divulgación ilegal de la información. Ganancia monetaria. Alteración no autorizada de los datos.	Crimen por computador (espionaje cibernético). Acto fraudulento (repetición, personificación, interceptación). Soborno de la información. Suplantación de identidad. Intrusión en el sistema.
Terrorismo	Chantaje. Destrucción. Explotación. Venganza. Ganancia política. Cubrimiento de los medios de comunicación.	Bomba/terrorismo. Guerra de la información. Ataques contra el sistema (negación distribuida del servicio). Penetración en el sistema. Manipulación en el sistema.
Espionaje industrial (inteligencia, empresas, gobiernos, extranjeros, otros intereses gubernamentales)	Ventaja competitiva. Espionaje económico.	Ventaja de defensa. Ventaja política. Explotación económica. Hurto de información. Intrusión en privacidad personal. Ingeniería Social. Penetración en el sistema. Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionadas con la tecnología).
	Curiosidad.	Asalto a un empleado.

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
		Pagina 16	

Intrusos (empleados con entrenamiento deficientes, descontentos, malintencionados, negligentes, deshonestos o despedidos).	Ego. Inteligencia. Ganancia monetaria. Venganza. Errores y omisiones no intencionales (error en el ingreso de los datos, error de programación).	Chantaje. Observar información reservada. Uso inadecuado del computador Fraude y hurto. Soborno de información. Ingreso de datos falsos o corruptos. Interceptación. Código malicioso (virus, bomba lógica, troyano). Venta de información personal. Errores en el sistema (bugs). Intrusión al sistema. Sabotaje del sistema. Acceso no autorizado al sistema.
--	--	---

Tabla 3. Fuente: ISO/IEC 27005:2009

Para que una vulnerabilidad pueda causar daño es necesario que una amenaza pueda explotar esa debilidad. La siguiente tabla muestra algunas amenazas que pueden explotar unas vulnerabilidades:

TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Almacenamiento sin protección	Hurtos medios o documentos
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos
	Falta de cuidado en la disposición final	Hurtos medios o documentos
Software	Copia no controlada	Hurtos medios o documentos
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos



SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN
SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC

Código:

Versión :02

Fecha de emisión:
2024

Pagina 17

	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de terminación de sesión cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de registros de auditoría	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autenticación de usuarios	Falsificación de derechos
	Contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Falsificación de derechos
	Software nuevo o inmaduro	Falsificación de derechos
	Especificaciones incompletas o no claras para los desarrolladores	Falsificación de derechos
	Ausencia de control de cambios eficaz	Falsificación de derechos
	Descargue y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
Personal	Ausencia de personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios



SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN
SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC

Código:

Versión :02

Fecha de emisión:
2024

Pagina 18

	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia en seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado de personal externo o de limpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autenticación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorías	Abuso de los derechos



SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN
SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC


Código:

Versión :02

Fecha de emisión:
2024

Pagina 19

Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información
Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
Ausencia de planes de continuidad	Falla del equipo
Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
Ausencia de registros en bitácoras	Error en el uso
Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
		Pagina 20	

	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falsificado o copiado

6.3.3 Descripción de Consecuencias

Después de realizar la identificación de amenazas y vulnerabilidades, se identifican las posibles consecuencias de la materialización de una amenaza sobre una vulnerabilidad.

6.3.4 Definición de Riesgos


Acorde a la identificación de vulnerabilidades y amenazas sobre los activos seleccionados objeto del análisis de riesgos, se establecen los riesgos de seguridad a los cuales se encuentra expuesta los activos de información.

Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

6.3.5 Probabilidad de ocurrencia

Se mide en términos de la factibilidad o frecuencia con el riesgo se podría llegar a materializar, teniendo en cuenta la presencia y exposición ante factores internos y externos.

Bajo el criterio de FRECUENCIA se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :02	Fecha de emisión: 2024	Pagina 21

Bajo el criterio de FACTIBILIDAD se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

6.3.6 Nivel de Impacto

Por impacto se entienden las consecuencias que puede ocasionar al Instituto la materialización del riesgo y será determinado por un criterio cualitativo y/o cuantitativo.

Para medir el nivel de gravedad o impacto de los riesgos operativos en la entidad se han definido las siguientes variables de afectación:

- Continuidad del Negocio: tiempo de investigación y reparación
- Operativo: reprocesos
- Reputacional: Afectación de la imagen y/o reputacional
- Legal: sanciones, multas y fallos sin generar erogación presupuestal a la entidad.
- Financiero
- Seguridad de la Información


Se define como variable para la medición del impacto financiero el Patrimonio Técnico ya que, al considerar los activos ponderados por nivel de riesgo, representa los recursos de que dispone el Instituto para solventar un evento de riesgo que se materialice.

Se realizó un análisis estadístico para determinar los rangos que permitan medir los niveles de impacto.

Se tomaron los promedios mensuales del patrimonio técnico de los últimos 5 años, se calcula el promedio y posteriormente se determinan los rangos correspondientes a cada nivel de riesgo.

Para determinar el porcentaje que establezca el nivel máximo de impacto, se tomó como referencia el coeficiente de variación del promedio de los datos por año (coeficiente de la desviación estándar sobre el promedio del patrimonio técnico).

Se tienen en cuenta la teoría de la distribución de frecuencias normal y el teorema de limite central (cerca del 68% de los datos estarán dentro de una desviación estándar de la media, 95% estarán dentro de 2 desviaciones estándar y 99,7% estarán dentro de 3 desviaciones estándar), para definir cuantas desviaciones estándar usar para calcular el coeficiente de variación.

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
			Pagina 22

Se define considerar (2) dos desviaciones estándar, es decir que teniendo en cuenta los datos utilizados para el análisis el nivel máximo de impacto es a partir de un 9% del patrimonio técnico.

Para determinar los intervalos entre los niveles Leve y Extremo, se realiza un análisis con los líderes de procesos para definir según la naturaleza de las operaciones, hasta que valor podría ubicarse cada nivel de impacto.

Para establecer las escalas de las otras variables de calificación del impacto (Legal, Reputación, Seguridad de la Información, Operativo, Continuidad del Negocio), se consultó la opinión del experto técnico de los procesos asociados a estos factores según el caso.

6.3.7 Valoración del Riesgo

El riesgo inherente es el nivel de exposición presente en ausencia de controles, no se toman en cuenta los controles existentes en el Instituto.

La valoración de los riesgos en términos de probabilidad e impacto de ocurrencia se obtiene de aplicar la siguiente ecuación:

$\text{Riesgo Inherente} = \text{Probabilidad} * \text{Impacto}$
--

6.4 Plan de Tratamiento

Se debe definir un plan de tratamiento y gestión de los riesgos asociados a los activos de información, el cual tendrá como alcance diseñar y documentar las acciones de mejora que permitan controlar y disminuir los riesgos de seguridad a los que están expuestos los activos de información.

6.4.1 Estrategia de Tratamiento de Riesgo

Con la valoración de los riesgos de seguridad identificados, se define la estrategia del tratamiento para cada uno de los riesgos acorde a los objetivos del Instituto y la importancia del activo de información para la continuidad del negocio, permitiendo así determinar las acciones a realizar en cada uno de los riesgos identificados.

Los siguientes parámetros se tendrán en cuenta para el tratamiento del riesgo:

ESTRATEGIA DE TRATAMIENTO DEL RIESGO	DESCRIPCIÓN
---	--------------------

Evitar	Se abandona las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. Este tratamiento es el menos arriesgado y menos costoso, pero es un obstáculo para el desarrollo de las actividades de la entidad.
Reducir o mitigar	Se adoptan medidas para reducir la probabilidad o el impacto del riesgo o ambas, conlleva la implementación de controles. Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este. Para reducir o mitigar los riesgos de seguridad se deben implementar como mínimo los controles del Anexo A de la ISO/IEC 27001:2013.
Transferir o compartir	se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Esta transferencia se hace a través de seguros o tercerización mediante un acuerdo contractual.
Asumir o Aceptar	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. No es necesario poner controles, el riesgo solo se monitorea.

Ilustración 1. Parámetros para el tratamiento del Riesgo

Riesgo después de medida de tratamiento




Ilustración 2. Riesgo después de Medida de Tratamiento.

6.4.2 Identificación de Controles

6.4.2.1 Controles Actuales

Por cada riesgo inherente identificado, se deben establecer los controles asociados. Así mismo, se determinan las cualidades y características de cada control, que tienen la posibilidad de disminuir el nivel de riesgo, desplazarlas a una zona de riesgo menor a la inherente y determinar si definitivamente es aceptable o no.

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :02	Fecha de emisión: 2024
			Pagina 24

Si la opción de tratamiento es “Reducir el riesgo”, la identificación de controles se apoyará en el anexo A de la norma ISO 27001:2013 o establecer otros controles que considere pertinentes y que sean efectivos y eficaces [\(ver Anexo\)](#).

Cada control debe tener un responsable de su ejecución, la frecuencia de aplicación, como se ejecuta, evidencia de aplicación y excepciones.

7. MAPA DE RIESGO RESIDUAL

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).

8. TRATAMIENTO DEL RIESGO

El tratamiento del riesgo consiste en seleccionar e implementar opciones para abordar el riesgo. La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos, esfuerzo o desventajas de la implementación.


9. SEGUIMIENTO Y REVISIÓN

El seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas

El seguimiento y la revisión deberían tener lugar en todas etapas del proceso. El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

10. REGISTRO E INFORME

La gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados.

	SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :02	Fecha de emisión: 2024	Pagina 25

11. CAPACITACIÓN

El Plan de Capacitación se llevará de acuerdo al “Plan de Sensibilización para la Seguridad de la Información y Ciberseguridad” el cual forma parte del “Sistema de Gestión de Ciberseguridad y Seguridad de la Información”.