
	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código: P-SSI-012	Versión :04	Fecha de emisión: enero 2026

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

Modelo de Seguridad y Privacidad de la Información

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 2

Contenido

INTRODUCCIÓN.....	3
2. OBJETIVO	3
3. ALCANCE PARA LA ADMINISTRACIÓN DEL RIESGO	3
5. DEFINICIONES	4
6. ORGANIZACIÓN PARA LA GESTIÓN DEL RIESGO	4
6.1 Definición de Roles y Responsabilidades	4
7. IDENTIFICACIÓN DE RIESGOS	9
7.1 Establecimiento del Contexto.....	9
7.2 Identificación, Clasificación y Valoración de Activos	9
7.3 Metodología para el Análisis de Riesgos	10
7.4 Plan de Tratamiento	30
8. MAPA DE RIESGO RESIDUAL	31
9. TRATAMIENTO DEL RIESGO	32
10. SEGUIMIENTO Y REVISIÓN	32
11. REGISTRO E INFORME	32
12. CAPACITACIÓN	32
13. CONTROL DE CAMBIOS.....	33

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, ciberseguridad y protección de datos personales, 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 Seguridad de la Información y Ciberseguridad del Instituto para el Desarrollo de Antioquia - IDEA.

2. OBJETIVO


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

3. 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.

4. NORMATIVIDAD

Ver normograma.

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 4

5. DEFINICIONES

- Ver definiciones en M-SSI-011 Sistema de Administración de Riesgo de Seguridad de la Información y Ciberseguridad - SARSIC

6. ORGANIZACIÓN PARA LA GESTIÓN DEL RIESGO

6.1 Definición de Roles y Responsabilidades


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

6.1.1 Junta Directiva

Adquirir el compromiso de facilitar el cumplimiento de los objetivos para la gestión del Riesgo de Seguridad de la Información, Ciberseguridad y protección de datos personales. Las responsabilidades son las siguientes:

- Realizar seguimiento a la gestión de los riesgos de seguridad de la información, ciberseguridad y protección de datos personales y establecer medidas, teniendo en cuenta el nivel de tolerancia del riesgo.
- Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente el jefe de la Oficina Control de Riesgo.
- Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente la seguridad de la información, ciberseguridad y protección de datos personales.
- Aprobar las modificaciones relacionadas con seguridad de la información, ciberseguridad y protección de datos personales en el Plan de Contingencia y Continuidad del Negocio del IDEA.
- Designar la dependencia o cargo para la ejecución y seguimiento de la gestión del riesgo de seguridad de la información, ciberseguridad y protección de datos personales.

6.1.2 Gerente General

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 5

Responsable por el direccionamiento estratégico e impulso de la Gestión del Riesgo de seguridad de la información, ciberseguridad y protección de datos personales, así como: velar por el cumplimiento de lineamientos, políticas y demás disposiciones relacionadas.

Las responsabilidades son las siguientes:


- Someter a aprobación de la Junta Directiva, el Manual para la Administración de Riesgo en la seguridad de la información, ciberseguridad y protección de datos personales y sus actualizaciones.
- Adquirir un compromiso con la implementación y seguimiento a la gestión del riesgo de la seguridad de la información, ciberseguridad y protección de datos personales.
- Sensibilizar a los miembros del Comité de Gerencia, en la toma de consciencia respecto a la criticidad de los activos de información y su importancia en el desarrollo de la misión de la Instituto.
- Evaluar los informes de seguimiento permanente de las etapas y elementos constitutivos del Manual para la Administración de Riesgo en la Seguridad de la Información y Ciberseguridad.
- Velar porque se implementen estrategias con el fin de establecer el cambio cultural que la gestión de este riesgo implica para el Instituto.
- Disponer de los recursos necesarios para la oportuna gestión del riesgo.

6.1.3 Directivos

Aplicar políticas y lineamientos para la gestión del riesgo de seguridad de la información, ciberseguridad y protección de datos personales en la dependencia a cargo, transmitiendo los objetivos de seguridad para cada uno de los roles que desempeñe.

Las responsabilidades son las siguientes:

- Velar por que sea suministrada la información para el establecimiento de cada uno de los mapas de riesgo en los procesos de seguridad de la información, ciberseguridad y protección de datos personales.
- Identificar y valorar riesgos, controles y planes de acción en cada uno de sus procesos y procedimientos.

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 6


- Impulsar y promover la cultura de la gestión del riesgo de seguridad de la información, ciberseguridad y protección de datos personales del personal a su cargo, así como en los procesos y actividades que se ejecuten.
- Participar en el control y mitigación de los riesgos a los cuales se encuentran expuestos sus procesos.
- Mantener actualizados los procedimientos y mapas de riesgos, propendiendo el control y la mitigación de los riesgos presentes en sus procesos.
- Ejecutar de manera oportuna los planes de acción que se establezcan para la mitigación de riesgos.

6.1.4 Gerencia de Gestión de Riesgos

Definir los instrumentos, metodologías y procedimientos que usará el Instituto para una correcta gestión del riesgo de seguridad de la información, ciberseguridad y protección de datos personales.

Las responsabilidades son las siguientes:

- Establecer una metodología del riesgo, para que el Instituto administre y mida efectivamente los riesgos de seguridad de la información, ciberseguridad y protección de datos personales acorde con los lineamientos y mejores prácticas que considere convenientes.
- Asesorar y acompañar a los líderes de proceso en la administración y gestión de riesgo para su identificación, análisis, evaluación y tratamiento.
- Reportar al menos 2 veces al año la junta directiva y a la alta dirección, los resultados de la gestión de los riesgos, especialmente la evaluación que se haga de la confidencialidad, integridad y disponibilidad de la información, identificación de ciberamenazas, resultados de la evaluación de efectividad de los programas de ciberseguridad y propuestas de mejora en materia de ciberseguridad.
- Establecer los principios y lineamientos para promover una cultura para la gestión del riesgo, que incluya actividades de difusión, capacitación y concientización para todos los funcionarios y contratistas.
- Realizar seguimiento a los planes de acción y/o planes de mejoramiento identificados.

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 7

- Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.
- Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.

6.1.5 Dirección de TI

Liderar la gestión de los riesgos de seguridad sobre la gestión de tecnología de la información (TI) del Instituto.

Las responsabilidades son las siguientes:


- Identificar y valorar los posibles riesgos tecnológicos que puedan afectar la confidencialidad, integridad y disponibilidad de la plataforma tecnológica.
- Realizar pruebas de vulnerabilidad sobre los diferentes servicios y sistemas de información tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad informática.
- Realizar pruebas al Plan de Continuidad del Negocio que simulen la materialización de ataques cibernéticos.
- Asegurar la capacitación y entrenamiento continuo del personal de sistemas en temas de seguridad informática y ciberseguridad.
- Participar en el proceso de gestión de incidentes, informando a la Oficina de Gestión del Riesgo todos los eventos o incidentes que puedan afectar la disponibilidad, integridad y confidencialidad de la información Institucional.

6.1.6 Control Interno

Evaluar la efectividad de las políticas y lineamientos del sistema de gestión de riesgos de seguridad de la información, ciberseguridad y protección de datos personales, a través del proceso de auditorías internas.

Las responsabilidades son las siguientes:

- Brindar elementos para la evaluación sobre procesos de administración del riesgo.
- Determinar si la evaluación de los riesgos es correcta.
- Evaluar los procesos de gestión del riesgo.

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 8


- Evaluar los reportes de riesgos.

6.1.7 Comité de Seguridad de la Información y Ciberseguridad

- Coordinar la implementación del Modelo de Seguridad de la Información y Ciberseguridad.
- Coordinar e impulsar el desarrollo de proyectos de seguridad de la información, ciberseguridad y protección de datos personales.
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Aprobar el uso de metodologías y procesos para la seguridad de la información.
- Revisar los diagnósticos del estado de la seguridad de la información.
- Participar en la formulación y evaluación de planes para mitigar y/o eliminar riesgos.
- Realizar revisiones al Modelo de Seguridad de la Información y Ciberseguridad por lo menos una (1) vez al año y definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información y la ciberseguridad dentro del Instituto para el Desarrollo de Antioquia.
- Revisar por lo menos una (1) vez al año la Política de Seguridad de la Información y Ciberseguridad y participar de la actualización en caso de ser necesario.
- Verificar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad dentro del Instituto.
- Las demás funciones inherentes a la naturaleza del comité.

6.1.8 Servidores Públicos y Contratistas

- Reportar oportunamente los eventos de riesgo de seguridad de la información y ciberseguridad que ocurran en el transcurso diario de sus actividades, según lo indicado en el Modelo de Seguridad de la Información y Ciberseguridad.
- Adoptar una cultura de autocontrol y mitigación de riesgo seguridad de la información y ciberseguridad en todas las actividades diarias.
- Participar activamente en las capacitaciones que se brinden en materia de riesgo de seguridad de la información y ciberseguridad en el Instituto.

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 9

7. 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, pruebas de vulnerabilidades, incidentes materializados, opiniones informadas y expertas y las necesidades de las partes involucradas (NTC ISO31000, Numeral 2.15).

7.1 Establecimiento del Contexto

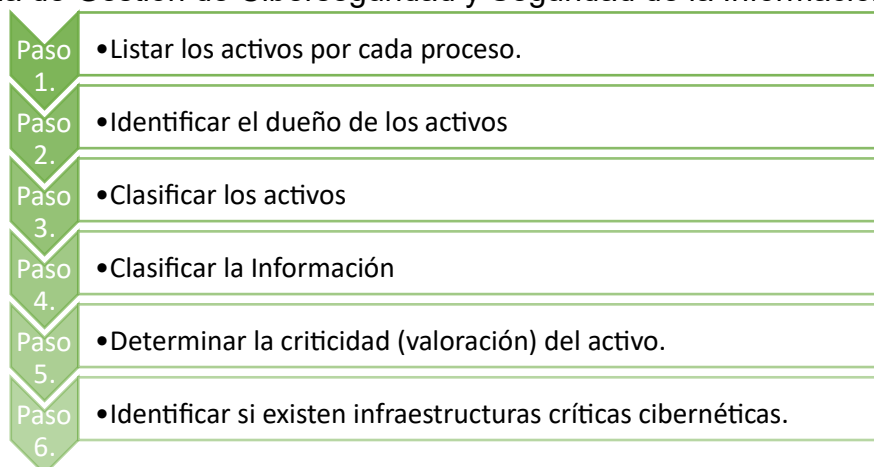
Es la definición de los parámetros internos y externos que toman en consideración para la administración del riesgo, esto ayuda en la identificación de las causas de los riesgos.


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.

7.2 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 Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :03	Fecha de emisión: 2025
			Pagina 10

7.3 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

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

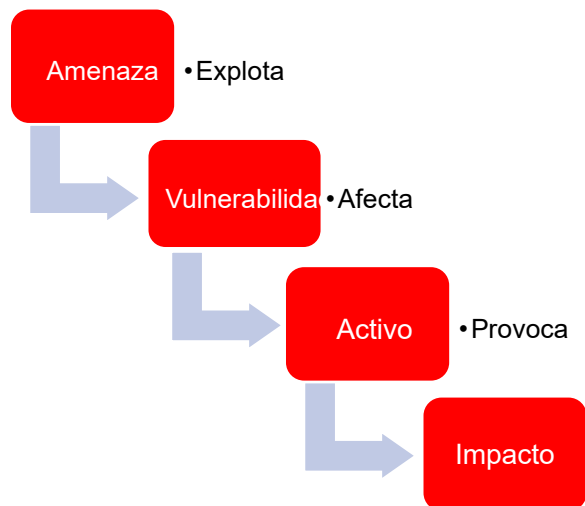
Se identificarán los siguientes tres (3) riesgos inherentes:

1. • Pérdida de la confidencialidad
2. • Pérdida de la integridad
3. • Pérdida de la disponibilidad

“Tomado del Manual de Sistema de Administración de Riesgo de Seguridad de la Información y Ciberseguridad - SARSIC”

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :03	Fecha de emisión: 2025
		Pagina 11	

El siguiente diagrama muestra las relaciones entre conceptos:



“Tomado del SARSIC”

7.3.1 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 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:



**SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

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

Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 12

TABLA DE VULNERABILIDADES COMUNES

Categoría

Descripción de Amenaza

Hardware

Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento

Insuficientes planes de sustitución periódica de los equipos

Susceptibilidad a la humedad, el polvo y la suciedad

Sensibilidad a la radiación electromagnética

Insuficiente control de los cambios de configuración

Susceptibilidad a las variaciones de tensión

Susceptibilidad a las variaciones de temperatura

Almacenamiento sin protección

Falta de cuidado en la eliminación

Copia incontrolada

Software

Ausencia o insuficiencia de pruebas de software

Defectos conocidos en el software

Ausencia de "cierre de sesión" al abandonar el puesto de trabajo

Eliminación o reutilización de los medios de almacenamiento sin un borrado adecuado

Configuración insuficiente de los registros con fines de auditoría

Asignación incorrecta de los derechos de acceso

Software ampliamente distribuido

Aplicación de programas de aplicación a los datos erróneos en términos de tiempo

Interfaz de usuario complicada



**SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

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

Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 13

	Insuficiente o falta de documentación
	Configuración incorrecta de los parámetros
	Fechas incorrectas
	Mecanismos de identificación y autenticación insuficientes (por ejemplo, para la autenticación de los usuarios)
	Tablas de contraseñas desprotegidas
	Mala gestión de las contraseñas
	Servicios innecesarios habilitados
	Software inmaduro o nuevo
	Especificaciones poco claras o incompletas para los desarrolladores
	Control de cambios ineficaz
	Descarga y uso incontrolado de software
	Falta de copias de seguridad o copias incompletas
	Falta de elaboración de informes de gestión
Red	Mecanismos insuficientes para la prueba de envío o recepción de un mensaje
	Líneas de comunicación desprotegidas
	Tráfico sensible desprotegido
	Cableado conjunto deficiente
	Punto único de fallo
	Ineficacia o falta de mecanismos de identificación y autenticación del emisor y el receptor
	Arquitectura de red insegura
	Transferencia de contraseñas en claro



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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

Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 14

	Gestión inadecuada de la red (resiliencia del enrutamiento)
	Conexiones de red pública no protegidas
Personal	Ausencia de personal
	Procedimientos de contratación inadecuados
	Formación insuficiente en materia de seguridad
	Uso incorrecto del software y el hardware
	Escasa concienciación en materia de seguridad
	Insuficiencia o falta de mecanismos de supervisión
	Trabajo no supervisado por personal externo o de limpieza
	Ineficacia o falta de políticas para el uso correcto de los medios de telecomunicación y mensajería
Sitio	Uso inadecuado o descuidado del control de acceso físico a edificios y salas
	Ubicación en una zona susceptible de inundación
	Red eléctrica inestable
	Insuficiente protección física del edificio, puertas y ventanas
Organización	No se ha desarrollado un procedimiento formal para el registro y la cancelación de usuarios, o su aplicación es ineficaz.
	No se ha desarrollado un proceso formal para la revisión de los derechos de acceso (supervisión), o su aplicación es ineficaz.
	Disposiciones insuficientes (relativas a la seguridad) en los contratos con clientes y/o terceros
	No se ha desarrollado un procedimiento de supervisión de las instalaciones de procesamiento de la información, o su aplicación es ineficaz.
	No se realizan auditorías (supervisión) de forma regular
	No se han desarrollado procedimientos de identificación y evaluación de riesgos, o su aplicación es ineficaz.
Organización	No se han desarrollado procedimientos de identificación y evaluación de riesgos, o su aplicación es ineficaz.



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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

Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 15

Insuficiencia o falta de informes de fallos registrados en los registros de los administradores y operadores

Respuesta inadecuada del servicio de mantenimiento

Acuerdo de nivel de servicio insuficiente o inexistente

No se ha desarrollado un procedimiento de control de cambios, o su aplicación es ineficaz

No se ha desarrollado un procedimiento formal para el control de la documentación del SGSI, o su aplicación es ineficaz.

No se ha desarrollado un procedimiento formal para la supervisión de los registros del SGSI, o su aplicación es ineficaz.

No se ha desarrollado un proceso formal para la autorización de la información

disponible al público, o su implementación es ineficaz.

Asignación inadecuada de las responsabilidades de seguridad de la información

No existen planes de continuidad, o son incompletos, o están obsoletos

No se ha desarrollado una política de uso del correo electrónico, o su aplicación es ineficaz.

No se han elaborado procedimientos para la introducción de programas informáticos en los sistemas operativos, o su aplicación es ineficaz.

No se han desarrollado procedimientos para el manejo de información clasificada, o su aplicación es ineficaz.

Las responsabilidades de seguridad de la información no están presentes en las descripciones de los puestos de trabajo

Insuficiencia o falta de disposiciones (relativas a la seguridad de la información) en los contratos con los empleados

El proceso disciplinario en caso de incidente de seguridad de la información no está definido, o no funciona correctamente

No se ha desarrollado una política formal sobre el uso de ordenadores móviles, o su aplicación es ineficaz


Insuficiente control de los activos fuera de las instalaciones

Insuficiente o falta de política de "escritorio y pantalla limpios".

Autorización de las instalaciones de procesamiento de la información no implementada o que no funciona correctamente

Mecanismos de supervisión de las violaciones de la seguridad no aplicados adecuadamente

Procedimientos de notificación de deficiencias de seguridad no desarrollados, o su aplicación es ineficaz

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :03	Fecha de emisión: 2025
		Pagina 16	

	No se han desarrollado procedimientos de cumplimiento de las disposiciones en materia de derechos intelectuales, o su aplicación es ineficaz
--	--

Tabla 1. Fuente: ISO/IEC 27005:2022

7.3.2 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.

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), Accidentales (A) o Ambientales (E).

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 COMUNE 3		
Categoría	Descripción de Amenaza	Tipo de fuente de riesgo
Amenazas Físicas	Fuego	A,D,E
	Agua	A,D,E
	Contaminación, radiación nociva	A,D,E
	Accidente grave	A,D,E
	Explosión	A,D,E
	Polvo, corrosión, congelación	A,D,E
	Fenómeno climático	E



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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

Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 17

		Fenómeno sísmico	E
		Fenómeno volcánico	E
		Fenómeno meteorológico	E
Amenazas Naturales		Inundación	E
		Fenómeno pandémico/epidémico	E
Fallos en las infraestructuras		Fallo de un sistema de suministro	A,D
		Fallo del sistema de refrigeración o ventilación	A,D
		Pérdida de suministro eléctrico	A,D,E
		Fallo de una red de telecomunicaciones	A,D,E
		Fallo del equipo de telecomunicaciones	A,D
		Radiación electromagnética	A,D,E
		Radiación térmica	A,D,E
		Pulsos electromagnéticos	A,D,E
Fallos técnicos		Fallo del dispositivo o del sistema	A
		Saturación del sistema de información	A,D
		Violación de la mantenibilidad del sistema de información	A,D
		Ataque terrorista, sabotaje	D
		Ingeniería social	D
		Interceptación de la radiación de un dispositivo	D
		Espionaje remoto	D
		Espionaje	D
		Robo de medios o documentos	D
		Robo de equipos	D



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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


Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 18

Acciones Humanas	Robo de identidad o credenciales digitales	D
	Recuperación de soportes reciclados o desechados	D
	Divulgación de información	A, D
	Introducción de datos de fuentes no fiables	A, D
	Manipulación del hardware	D
	Manipulación del software	A, D
	Explotación por medio de la comunicación basada en la web	D
	Ataque de repetición, ataque de hombre en el medio	D
	Tratamiento no autorizado de datos personales	A, D
	Entrada no autorizada a las instalaciones	D
	Uso no autorizado de dispositivos	D
Acciones humanas	Uso incorrecto de los dispositivos	A, D
	Deterioro de dispositivos o soportes	A, D
	Copia fraudulenta de software	D
	Uso de software falsificado o copiado	A, D
	Corrupción de datos	D
	Tratamiento ilegal de datos	D
	Envío o distribución de malware	A, D, E
	Detección de posiciones	D
Compromiso de funciones o servicios	Error de uso	A
	Abuso de derechos o permisos	A, D
	Falsificación de derechos o permisos	D
	Denegación de acciones	D


	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :03	Fecha de emisión: 2025
Pagina 19			

Amenazas para la organización	Falta de personal	A, E
	Falta de recursos	A, E
	Fallo de los proveedores de servicios	A, E
	Violación de leyes o reglamentos	A, D

Tabla 2 Fuente: ISO/IEC 27005:2022

✓ 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) DDoS Penetración en el sistema Manipulación en el sistema
	Ventaja competitiva	Ventaja de defensa

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 20

Espionaje industrial (inteligencia, empresas, gobiernos, extranjeros, otros intereses gubernamentales)	Espionaje económico	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)
Intrusos (empleados con entrenamiento deficientes, descontentos, malintencionados, negligentes, deshonestos o despedidos).	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (error en el ingreso de los datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema (bugs) Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema

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/instalación defectuosa de los medios de almacenamiento	Violación de la mantenibilidad del sistema de información



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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

Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 21

	Insuficientes planes de sustitución periódica de los equipos	Deterioro de dispositivos o soportes
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelación
	Sensibilidad a la radiación electromagnética	Pulsos electromagnéticos
	Insuficiente control de los cambios de configuración	Error de Uso
	Susceptibilidad a las variaciones de Tensión	Pérdida de suministro eléctrico
	Susceptibilidad a las variaciones de temperatura	Fenómeno meteorológico
	Almacenamiento sin protección	Robo medios o documentos
	Falta de cuidado en la Eliminación	Robo medios o documentos
	Copia incontrolada	Robo medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de derechos o permisos
	Defectos conocidos en el software	Abuso de derechos o permisos
	Ausencia de "cierre de sesión" al abandonar el puesto de trabajo	Abuso de derechos o permisos
	Eliminación o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de derechos o permisos
	Configuración insuficiente de los registros con fines de auditoría	Abuso de derechos o permisos
	Asignación incorrecta de los derechos de acceso	Abuso de derechos o permisos
	Software ampliamente distribuido	Corrupción de datos
	Aplicación de programas de aplicación a los datos erróneos en términos de tiempo	Corrupción de datos
	Interfaz de usuario complicada	Error de Uso
	Insuficiente o falta de documentación	Error de Uso
	Configuración incorrecta de los parámetros	Error de Uso
	Fechas incorrectas	Error de Uso
	Mecanismos de identificación y autenticación insuficientes (por ejemplo, para la autenticación de los usuarios)	Falsificación de derechos o permisos



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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

Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 22

Tablas de Contraseñas desprotegidas	Falsificación de derechos o permisos
Mala gestión de contraseñas	Falsificación de derechos o permisos
Servicios innecesarios habilitados	Falsificación de derechos o permisos

	Software inmaduro o nuevo	Falsificación de derechos o permisos
	Especificaciones poco claras o incompletas para los desarrolladores	Falsificación de derechos o permisos
	Control de cambios ineficaz	Falsificación de derechos o permisos
	Descarga y uso incontrolado de software	Uso de software falsificado o copiado
	Falta de copias de seguridad o copias incompletas	Uso de software falsificado o copiado
	Faltas de elaboración de informes de gestión	Uso no autorizado de dispositivos
Personal	Ausencia de personal	Falta de personal
	Procedimientos de contratación inadecuados	Deterioro de dispositivos o soportes
	Formación insuficiente en materia de seguridad	Error de uso
	Uso incorrecto del software y el hardware	Error de uso
	Escasa concienciación en materia de seguridad	Error de uso
	Insuficiencia o falta de mecanismos de supervisión	Tratamiento no autorizado de datos personales
	Trabajo no supervisado por personal externo o de limpieza	Robo de medios o documentos.
	Ineficacia o falta de políticas para el uso correcto de los medios de telecomunicación y mensajería	Uso no autorizado de dispositivos
Red	Mecanismos insuficientes para la prueba de envío o recepción de un mensaje	Denegación de acciones
	Líneas de comunicación desprotegidas	Espionaje
	Tráfico sensible desprotegido	Espionaje
	Cableado conjunto deficiente	Fallo del dispositivo o del sistema
	Punto único de fallo	Fallo del dispositivo o del sistema



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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

Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 23

	Ineficacia o falta de mecanismos de identificación y autenticación del emisor y receptor	Robo de identidad o credenciales digitales
	Arquitectura de red insegura	Espionaje remoto
	Transferencia de contraseña en claro	Espionaje remoto
	Gestión inadecuada de la red (resiliencia del enrutamiento)	Saturación del sistema de información

	Conexiones de red pública no protegidas	Uso no autorizado de dispositivos
Sitio	Uso inadecuado o descuidado del control de acceso físico a edificios y salas	Fallo de los proveedores de servicios
	Ubicación en una zona susceptible de inundación	Inundación
	Red eléctrica inestable	Pérdida de suministro eléctrico
	Insuficiente protección física del edificio, puertas y ventanas	Fallo de los proveedores de servicios
Organización	No se ha desarrollado un procedimiento formal para el registro y la cancelación de usuarios, o su aplicación es ineficaz.	Robo de identidad o credenciales digitales
	No se ha desarrollado un proceso formal para la revisión de los derechos de acceso (supervisión), o su aplicación es ineficaz.	Robo de identidad o credenciales digitales
	Disposiciones insuficientes (relativas a la seguridad) en los contratos con clientes y/o terceros	Robo de identidad o credenciales digitales
	No se ha desarrollado un procedimiento de supervisión de las instalaciones de procesamiento de la información, o su aplicación es ineficaz.	Robo de identidad o credenciales digitales
	No se realizan auditorías (supervisión) de forma regular	Robo de identidad o credenciales digitales



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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

Código:

Versión :03

**Fecha de emisión:
2025**

Pagina 24

No se han desarrollado procedimientos de identificación y evaluación de riesgos, o su aplicación es ineficaz.	Robo de identidad o credenciales digitales
Insuficiencia o falta de informes de fallos registrados en los registros de los administradores y operadores	Robo de identidad o credenciales digitales
Respuesta inadecuada al servicio de mantenimiento	Fallo de los proveedores de servicios
Acuerdo de nivel de servicio insuficiente o inexistente	Fallo de los proveedores de servicios
No se ha desarrollado un procedimiento de control de cambios, o su aplicación es ineficaz	Fallo de los proveedores de servicios

No se ha desarrollado un procedimiento formal para el control de la documentación del SGSI, o su aplicación es ineficaz.	Corrupción de datos
No se ha desarrollado un procedimiento formal para la supervisión de los registros del SGSI, o su aplicación es ineficaz.	Corrupción de datos
No se ha desarrollado un proceso formal para la autorización de la información disponible al público, o su implementación es ineficaz.	Tratamiento ilegal de datos
Asignación inadecuada de las responsabilidades de seguridad de la información	Denegación de acciones
No existen planes de continuidad, o son incompletos, o están obsoletos	Fallo del dispositivo o del sistema
No se ha desarrollado una política de uso del correo electrónico, o su aplicación es ineficaz.	Error de uso
No se han elaborado procedimientos para la introducción de programas informáticos en los sistemas operativos, o su aplicación es ineficaz	Error de uso



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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

Código:

Versión :03


**Fecha de emisión:
2025**

Pagina 25

	No se han desarrollado procedimientos para el manejo de información clasificada, o su aplicación es ineficaz.	Error de uso
	Las responsabilidades de seguridad de la información no están presentes en las descripciones de los puestos de trabajo.	Error de uso
	Insuficiencia o faltade disposiciones (relativas a la seguridad de la información) en los contratos con los empleados.	Robo de equipos
	El proceso disciplinario en caso de incidente de seguridad de la información no está definido, o no funciona correctamente.	Uso incorrecto de los dispositivos
	No se ha desarrollado una política formal sobre el uso de ordenadores móviles, o su aplicación es ineficaz	Robo de equipos
	Insuficiente control de los activos fuera de las instalaciones	Robo de equipos
	Insuficiente o falta de política de "escritorio y pantalla limpios".	Robo de medios o documentos
	Autorización de las instalaciones de procesamiento de la información no implementada o que no funciona correctamente	Robo de medios o documentos
	Mecanismos de supervisión de las violaciones de la seguridad no aplicados adecuadamente	Robo de medios o documentos
	Procedimientos de notificación de deficiencias de seguridad no desarrollados, o su aplicación es ineficaz	Uso no autorizado de dispositivos
	No se han desarrollado procedimientos de cumplimiento de las disposiciones en materia de derechos intelectuales, o su aplicación es ineficaz.	Uso de software falsificado o copiado

7.3.3 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.

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :03	Fecha de emisión: 2025
		Pagina 26	

7.3.4 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).

7.3.5 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.

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.

Se establece la siguiente escala cualitativa:


ESCALA	RANGO DE PROBABILIDAD	DESCRIPCIÓN / POSIBILIDAD	FRECUENCIA DE OCURRENCIA
1	Muy baja	Puede ocurrir en circunstancias excepcionales	Ocurre una o dos veces al año
2	Baja	Insignificante posibilidad que el evento ocurra	Ocurre tres a cuatro veces al año
3	Media	Alguna posibilidad que el evento ocurra	Ocurre cinco a ocho veces al año
4	Alta	Posiblemente ocurra todas las veces	Ocurre nueve a doce veces al año
5	Muy Alta	Ocurre la mayoría de las veces	Ocurre más de doce veces al año

7.3.6 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

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :03	Fecha de emisión: 2025
			Pagina 27

- 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
- Datos personales

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 límite 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.

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.



SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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


Código:

Versión :03

Fecha de emisión:
2025

Página 28

Nivel de impacto		Rangos % del promedio del Patrimonio Técnico		Legal	Reputación	Seguridad de la información (Incidentes)	Operativo	Continuidad del negocio
		Min	Max					
1	Leve	0	< 0,004%	Recomendaciones menores por parte de entes de control y vigilancia (internos y/o externos). No se generan multas, sanciones de entes de control o demandas por incumplimientos legales, normativos o contractuales ni investigaciones disciplinarias internas, se generan quejas y reclamos de clientes internos o externos.	Afectación mínima a la imagen y/o reputación institucional.	Sin afectación a la disponibilidad, confidencialidad, integridad	Afectación mínima en el desempeño o del proceso	Afectaciones mínimas que no generan interrupción a la operación
2	Menor	0,004%	0,02%	Se generan medidas cautelares, controles de advertencia y actuaciones administrativas de proceso sancionatorios de los entes de control y vigilancia.	Afectación baja a la imagen y/o reputación institucional ante un cliente o servidor público.	Afectación a la disponibilidad, confidencialidad, integridad de la información que puede remediarse con facilidad.	Afectación en el desempeño o del proceso que puede ser atendida de forma inmediata	Afecta la operación de la Entidad, causando retrasos menores de hasta 2 horas
3	Moderado	0,02%	1,99%	Se generan sanciones, multas y fallos sin generar erogación presupuestal a la entidad.	Afectación a la imagen y/o reputación institucional que podría impactar directamente nuestra relación con clientes y aliados, y se logra intervenir antes de llegar a afectar el desempeño del Instituto. Difusión de información negativa en medios de comunicación y redes sociales	Afectación a la disponibilidad, confidencialidad, integridad de la información que impide el desarrollo de algunos procesos, pero se logra remediar antes de generar perjuicios a terceros.	Afectación en el desempeño o del proceso que puede requerir reprocesos internos y que puedan generar impactos en otros procesos no críticos.	Afecta la operación de la Entidad, causando retrasos de 2 horas hasta 1 día.
4	Mayor	1,99%	9,0%	Se generan sanciones, multas y fallos que si generan erogación presupuestal a la entidad.	Afectación a la imagen y/o reputación institucional en el contexto local y nacional que podría impactar directa y	Afectación a la disponibilidad, confidencialidad, integridad de la información de un activo crítico que impide el desarrollo de procesos	Afectación en el desempeño o del proceso que genera una alerta de incumplimi	Afecta la operación de la Entidad, causando retrasos mayores de 1 a 4 días

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 29


					negativamente e nuestra relación con clientes y aliados, trayendo como consecuencia un efecto negativo en nuestro negocio. Con difusión en los medios de comunicación por varios días de información negativa	críticos y que puede generar perjuicios a la entidad o a terceros	entos potenciales y que puedan generar impactos en otros procesos críticos.	
5	Extremo	> 9%		Se genera una intervención por parte de los entes de control que interrumpan la operación y la sostenibilidad de la entidad.	Afectación grave a la imagen y/o reputación institucional en los contextos local, regional, nacional e internacional, trayendo como consecuencia reacciones negativas en nuestros grupos de interés. Que genere recordación negativa de forma prolongada en los medios de comunicación	Afectación total a la disponibilidad, confidencialidad, integridad, de la información de un activo crítico, lo que impide la operación general de la entidad y el cumplimiento de los compromisos pactados con los diferentes grupos de interés	Afectación grave en el desempeño o del proceso que requiere modificaciones y/o reprocesos sustanciales, lo que afecta la prestación del servicio y genere una afectación masiva en todos los procesos.	Afecta la operación de la Entidad, causando retrasos mayores a 4 días.

7.3.7 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:

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

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 30

7.4 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.


7.4.1 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 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 27001:2022.
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

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :03	Fecha de emisión: 2025
		Pagina 31	

Riesgo después de medida de tratamiento

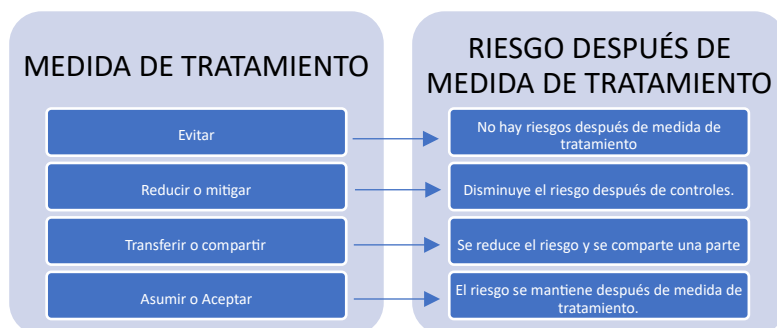


Ilustración 2. Riesgo después de Medida de Tratamiento. "Tomado del SARSIC"

7.4.2 Identificación de Controles

7.4.2.1 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.

Si la opción de tratamiento es "Reducir el riesgo", la identificación de controles se apoyará en el anexo A de la norma ISO 27001:2022 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.

8. 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).

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC		
	Código:	Versión :03	Fecha de emisión: 2025
		Pagina 32	

Extremo	
Alto	
Moderado	
Bajo	

9. 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.

10. 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.

11. REGISTRO E INFORME

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

12. 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”.

	SISTEMA DE GESTIÓN DE Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 32

13. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de Cambios
3	Enero de 2025	Versión 3, que reemplaza lo definido en la versión 2. Se actualizó el documento alineando a la norma ISO 27005/2022.
4	Enero de 2026	Versión 4, que reemplaza lo definido en la versión 3. Se actualizó el documento alineando a la norma ISO 27005/2022.

Elaboró:	Yaritza Shirley Montoya Bolívar	Contratista	Dirección de Ciberseguridad y seguridad de la Información.
Revisó:	Alexander Restrepo Zuluaga	Director	Dirección de Ciberseguridad y Seguridad de la Información.
Aprobó:	Alexander Restrepo Zuluaga	Director	Dirección de Ciberseguridad y Seguridad de la Información.