GESTIÓN DE RIESGOS PARA LA IMPLEMENTACIÓN DE UN SGSI

1. INTRODUCCIÓN

El SGSI (Sistema de Gestión de Seguridad de la Información) es la generación e implementación de una estrategia para el tratamiento de los riesgos de seguridad de los activos informáticos y activos de información, con la finalidad de resguardar, proteger, asegurar y garantizar su confidencialidad, integridad y disponibilidad.

Se inicia considerando y clasificando todos los activos informáticos y activos de información a partir de su importancia y criticidad y los riesgos de pérdida, destrucción, alteración y accesos no autorizados a los que se encuentran expuestos, tales como desaparición o robo de activos físicos, (computadoras y/o tablets), eliminación no autorizada de información en sistemas y bases de datos, copia, consulta y/o eliminación no autorizada de documentos en red y/o computadoras, ataques a sitios web para indisponibilidad de información pública, destrucción de documentos físicos por derrame de líquidos, fallas no controladas en sistemas informáticos, etc.

El SGSI conlleva la implementación de políticas, normas, procedimientos y controles para garantizar el resguardo y la seguridad de la información a partir de un **Análisis de Riesgos**, el cual debe incluir como base ***¿Qué información se debe proteger? ¿Cuál es la probabilidad de la amenaza a los activos?, evaluación del riesgo, definición e implementación de los debidos procedimientos y controles para el resguardo y la seguridad de los activos y la revisión continua y mejora del proceso periódicamente***.

El paso inicial para poder conformar e implementar el SGSI es el Análisis de Riesgos ya que será la base para evaluar cada activo (informático y de información) y poder determinar lo que se hará con el riesgo identificado.

En atención a lo anterior, para la elaboración del presente procedimiento, se han tomado como guías metodológicas, la norma técnica ISO 31000 e ISO 27005 que incluye los principios y directrices correspondientes a la gestión de riesgo de la información y que, en adelante, servirá de orientación para los procesos y actividades correspondientes.

La gestión de riesgo de la información obedece a una actuación permanente de prevención, para asegurar en todo momento el cumplimiento de objetivos y facilitar la toma de decisiones.

2. OBJETIVO

Brindar los lineamientos y las actividades requeridas para la administración del riesgo de la información, a partir de una metodología para la identificación, análisis y valoración del riesgo que contribuya a identificar e implementar planes de acción para mitigar los riesgos que tengan impacto sobre el cumplimiento de los objetivos de una organización.

3. GLOSARIO DE TÉRMINOS

Activo	Cualquier recurso de la institución necesario para el desempeño de sus actividades diarias y cuya disponibilidad o deterioro suponen un costo, servicios web, redes, hardware, información física o digital, entre otros.
Análisis de riesgo	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Amenazas	Circunstancia desfavorable que puede ocurrir y que cuando sucede tienen consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.
Causa	Todos aquellos factores internos y externos que solos o combinados con otros, pueden materializar el riesgo.
Confidencialidad	Se refiere a que la información no esté disponible, ni sea revelada a individuos, entidades o procesos no autorizados.
Consecuencia	Los efectos o situaciones resultantes de la materialización del riesgo que impacta en el proceso, activo, institución y partes interesadas.
Disponibilidad	Hace referencia a que el usuario accede a la información cuando se requiera.
Evento	Presencia o cambio de un conjunto particular de circunstancias.
Gestión del riesgo	Proceso efectuado por la alta gerencia y por todo el personal de la institución para un aseguramiento razonable al logro de los objetivos.
Identificación del riesgo	Proceso para encontrar, reconocer y describir el riesgo.
Impacto	Consecuencias que pueden ocasionar al área o dependencia la materialización del riesgo.

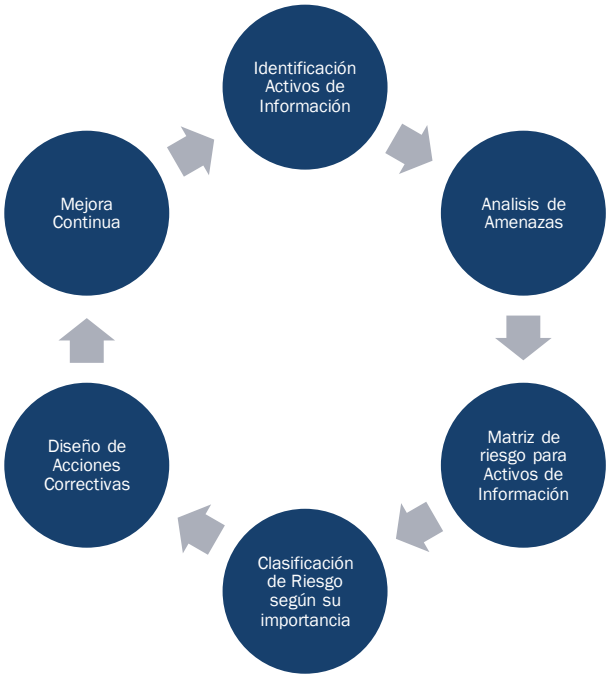
Integridad	Se refiere a la exactitud y completitud de la información, permitiendo que la información publicada sea precisa, coherente y compleja.
Probabilidad	Es la posibilidad de ocurrencia de un riesgo. Esta pude ser medida con criterios de frecuencia o factibilidad.
Riesgo inherente	Es aquel al que se enfrenta el área o dependencia en ausencia de acciones para modificar su probabilidad o impacto.
Riesgo residual	Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
Vulnerabilidad	Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de uno o más amenazas contra los activos.

4. METODOLOGÍA

Para la gestión de riesgo se debe seguir la siguiente metodología:

- Identificar los activos informáticos y activos de información
- En esta etapa recopilamos información sobre los procesos y las amenazas a las que está expuesta los activos de información y/o activo informático de área o de la dependencia analizada.
- Cada activo de información identificado debe de ser evaluado en la matriz de riesgo. Para cada riesgo enumerado en la lista de amenazas, debemos asignar una calificación de uno a cinco, para el eje de probabilidad, así como para el de impacto. Obtendremos, así, una calificación de los riesgos según el punto de intersección de ambos ejes, que corresponderá a un tipo de riesgo más o menos elevado.
- Realizada la evaluación de cada activo de información, se clasifican según su importancia. Ahora podemos obtener una lista de riesgos categorizada según su importancia, por orden de gravedad y urgencia de resolución. Realizar una separación entre lo que es relevante para la seguridad de la información y lo que no lo es.
- Tomar acciones para evitar, prevenir, mitigar, compartir o tolerar un riesgo. Después de identificar y asignar un valor numérico de importancia a las vulnerabilidades encontradas, definimos esa acción definitiva. Se realiza un diseño de las acciones correctivas que se van a implementar dentro del área o dependencia analizada.

- Evaluar los resultados de las acciones propuestas, verificar la aparición de nuevas vulnerabilidades y corroborar el nivel de importancia de las amenazas, ya que algunas de ellas pueden dejar de serlo o reducir su nivel de impacto.



La gestión de riesgo debe incluir todos los riesgos a los que este expuesto el activo, independientemente de su origen.

Se debe hacer como mínimo una evaluación anual de riesgos, debido a que el contexto cambia o puede haber nueva información sobre el riesgo, la eficacia del control establecido también debe ser monitoreada y documentada.

4.1. CRITERIOS DE GESTIÓN DE RIESGOS

A continuación, se establecen los criterios con los que se va a analizar y evaluar la importancia de los riesgos de información en el área y dependencias de la CC.

4.1.1. CRITERIOS PARA DETERMINAR LA PROBABILIDAD

Para medir la probabilidad de que un determinado evento ocurra se empleará la siguiente escala:

NIVEL DE PROBABILIDAD		DESCRIPCIÓN	FRECUENCIA
1	**Raro**	La amenaza no ha ocurrido en el último año	Ocurrencia = 0 al año
2	**Improbable**	La amenaza no ha ocurrido en los últimos 6 meses.	Ocurrencia = 0 en los últimos 6 meses
3	**Posible**	La amenaza no ha ocurrido en los últimos 3 meses.	Ocurrencia = 0 en los últimos 3 meses
4	**Probable**	La amenaza ha ocurrido una sola vez en el último mes.	Ocurrencia = 1 al mes
5	**Casi Seguro**	La amenaza ha ocurrido más de una vez en el último mes.	Ocurrencia > 1 al mes

4.1.2. CRITERIO PARA DETERMINAR LAS CONSECUENCIAS (IMPACTO)

Para medir los efectos de la ocurrencia de un evento determinado sobre los objetivos de la Organización, activo o proceso, se emplearán las siguientes escalas:

NIVEL	VALOR	DESCRIPCIÓN
Insignificante	**1**	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre el área o dependencia.
Menor	**2**	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre el área o dependencia.
Moderado	**3**	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre el área o dependencia.
Mayor	**4**	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre el área o dependencia.
Catastrófico	**5**	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre el área o dependencia.

La tabla anterior da una referencia general para cuantificar las consecuencias, pero se pueden desarrollar criterios específicos dependiendo de la clase de análisis de riesgo analizado.

4.1.3. MATRIZ DE EVALUACIÓN DE RIESGO – NIVEL DE RIESGO

De acuerdo a la cuantificación de la probabilidad de ocurrencia de un evento y el grado de severidad de sus consecuencias en los objetivos institucionales, activos o procesos, se establece el nivel de riesgo, el cual es producto de la aplicación de la siguiente fórmula:

$$\boldsymbol{Nivel\ de\ riesgo = Probabilidad\ x\ impacto}$$

Este valor numérico, deberá por tanto ubicarse en una de las casillas de la siguiente matriz para visualizar su zona de riesgo o severidad.

PROBABILIDAD		IMPACTO				
		Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
Casi Seguro	5	5	10	15	20	25
Probable	4	4	8	12	16	20
Posible	3	3	6	9	12	15
Raro	2	2	4	6	8	10
Improbable	1	1	2	3	4	5

PROBABILIDAD		IMPACTO				
		Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
Raro	5	A	A	E	E	E
Improbable	4	M	A	A	E	E
Posible	3	B	M	A	E	E
Probable	2	MB	B	M	A	E
Casi Seguro	1	MB	MB	M	A	A

ZONA DE RIESGO	
	Aceptable (MB)

	Tolerable (B)
	Moderado (M)
	Importante (A)
	Inaceptable (E)

4.1.4. EVALUACIÓN DEL RIESGO – OPCIONES DE TRATAMIENTO

A continuación, se relacionan las opciones de manejo/tratamiento sugeridos de acuerdo al nivel de riesgo establecido:

NIVELES DE RIESGO	RESPUESTA A LOS RIESGOS	DESCRIPCIÓN
ACEPTABLE	**Asumir el riesgo**	El nivel de riesgo es Aceptable y se encuentra controlado en el área o dependencia. Los riesgos en este nivel se deben revisar periódicamente.
TOLERABLE	**Asumir el riesgo**	El nivel de riesgo es Tolerable y se encuentra controlado en el área o dependencia. Los riesgos en este nivel se deben revisar periódicamente.
MODERADO	**Asumir el riesgo**	El nivel de riesgo es Moderado de acuerdo a los criterios de aceptación del área o dependencia. Los riesgos en este nivel deben ser monitoreados para identificar oportunamente los cambios en su valoración.
IMPORTANTE	**Mitigar el riesgo, Evitar, Compartir**	El nivel del riesgo es Importante, por lo que es necesario implementar controles en el área o dependencia para mitigar, evitar o compartir el riesgo y llevar a niveles aceptables.
INACEPTABLE	**Mitigar el riesgo, Evitar, Compartir**	El nivel del riesgo es **Inaceptable**, por lo que es necesario implementar controles en el área o dependencia para mitigar, evitar o compartir el riesgo y llevar a niveles aceptables.

4.2. PRIORIZAR LOS RIESGOS SOBRE LOS ACTIVOS

El riesgo nos muestra el grado de exposición frente a las amenazas evaluadas, es posible distinguir entre riesgos muy bajo, bajo, moderado, alto y extremo. Cada nivel nos indicará la prioridad de las acciones requeridas para su tratamiento.

RIESGO	PRIORIDAD	TIEMPO DE EJECUCIÓN DE ACCIONES
ACEPTABLE	**MUY BAJA**	De 12 a 16 Meses
TOLERABLE	**BAJA**	De 7 a 12 Meses
MODERADO	**MEDIA**	De 4 a 7 meses
IMPORTANTE	**ALTA**	De 0 a 4 meses
INACEPTABLE	**MUY ALTA**	Inmediata

4.2.1. GESTIÓN DE RIESGO EN LOS ACTIVOS

En esta etapa se deben estructurar los criterios para la toma de decisiones respecto al tratamiento de los riesgos, estableciendo las guías de acción necesarias para coordinar y administrar los eventos que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos informáticos y activos de información.

4.2.1.1. Toma de decisiones

- Si el riesgo se ubica en una zona **ACEPTABLE,** permite a la organización aceptarlo, es decir el riesgo se encuentra en un nivel que puede asumirse sin necesidad inmediata de tomar otras medidas de control.
- Si el riesgo se ubica en la zona **INACEPTABLE**, es necesario eliminar, en un período corto de tiempo, la actividad que genera el riesgo, para garantizar la continuidad de las operaciones de la institución.
- Si el riesgo se encuentra en cualquiera de las otras zonas (TOLERABLE, MODERADO, IMPORTANTE), se deben tomar medidas para llevar los riesgos a la zona ACEPTABLE, con la implementación de controles que disminuya el riesgo.

4.3. PLAN DE TRATAMIENTO DE LOS RIESGOS

Una vez seleccionados los controles que serán implementados para la mitigación de riesgos, es necesario elaborar un plan de acciones que garantice un efectivo despliegue o ejecución de los mismos.

El plan de tratamiento para la mitigación de los riesgos será elaborado en conjunto con el equipo de seguridad o de gestión de riesgos, comité de Seguridad de la Información, el área y/o dependencia específica.

4.4. SEGUIMIENTO Y REVISIÓN

Puesto que los riesgos no son estáticos, y las amenazas, vulnerabilidades, probabilidad de ocurrencia y consecuencias pueden cambiar, es necesario realizar el monitoreo para la detección de los cambios en el transcurso del tiempo. Se debe evaluar, por lo tanto, el desempeño o grado de seguridad de la información y la eficacia del SGSI. El equipo de Seguridad de la Información será la encargada de determinar los periodos de cuando se llevarán a cabo el seguimiento y la medición y/o cuando las autoridades superiores lo indiquen, así como determinar los métodos a aplicar para una mejor continua.

5. PROCEDIMIENTO PARA LA GESTIÓN DEL RIESGO