
	GESTIÓN DIRECTIVA		MODERNIZACIÓN Y ADMINISTRACIÓN DE LOS SISTEMAS DE GESTIÓN	
	FORMATO	MATRIZ DE RIESGOS Y OPORTUNIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: GDI-MAS-FM023	Versión: 001	Fecha de vigencia: 17/01/2022	Página 1 de 8

## MATRIZ DE RIESGOS Y OPORTUNIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Grover Sotelo Lopez Oficial de Seguridad Digital	Kelly Paz Orellana Jefa (e) de la Unidad de Modernización	Kelly Paz Orellana Jefa (e) de la Unidad de Modernización

	GESTIÓN DIRECTIVA		MODERNIZACIÓN Y ADMINISTRACIÓN DE LOS SISTEMAS DE GESTIÓN	
	FORMATO	MATRIZ DE RIESGOS Y OPORTUNIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: GDI-MAS-FM023	Versión: 001	Fecha de vigencia: 17/01/2022	Página 2 de 8

### CONTROL DE CAMBIOS

N°	Ítems	Descripción del cambio (*)
-	-	Versión inicial del documento.




Primera sección: Identificación, análisis y valoración del riesgo

Fecha de revisión:  
Revisado por:

IDENTIFICACION DE RIESGOS														ANALISIS DE RIESGO								VALORACION DEL RIESGO																			
Fecha de Identificación	Proceso donde se identifica el riesgo	Código Riesgo	Descripción del Riesgo	Activo de Información Comprometido	Causa raíz o Amenaza	Vulnerabilidad	Origen de las Amenazas		Riesgo afecta a:					Contexto	Partes Interesadas	Dueño de Riesgo	Consecuencias (Efecto)	Control Actual	Tipo Control	Frecuencia del Control	Automatización del Control	Está documentado y deja evidencia	Diseño del Control	Cumplimiento del Control	Nivel de Efectividad del Control	Probabilidad	Impacto	Valor del Nivel de Riesgo	Nivel de Riesgo	Medidas de Tratamiento	Priorización										
							Internas	Externas	Confidencialidad	Integridad	Disponibilidad	LPDP																													

Segunda sección: Plan de tratamiento y riesgo residual real

TRATAMIENTO DE RIESGOS									RIESGO RESIDUAL REAL											
Nuevo control a Implementar (Anexo A)	Actividades	Responsables	Fecha Inicio	Fecha Fin	Riesgo Residual Objetivo		Nivel de Riesgo	Nivel de Riesgo Residual Objetivo	Fecha de Medición Residual	Tipo Control	Frecuencia del Control	Automatización del Control	Está documentado y deja evidencia	Diseño del Control	Cumplimiento del Control		Nivel de Efectividad del Control	Probabilidad	Impacto	Nivel de Riesgo Residual Real
					Probabilidad	Impacto														

 <p>El regulador del agua potable</p>	GESTIÓN DIRECTIVA		MODERNIZACIÓN Y ADMINISTRACIÓN DE LOS SISTEMAS DE GESTIÓN	
	FORMATO	MATRIZ DE RIESGOS Y OPORTUNIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: GDI-MAS-FM023	Versión: 001	Fecha de vigencia:	Página 5 de 8


## CONTROLES

Tipos de Controles	
<b>Preventivo</b>	Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones. Anticipa eventos no deseados. Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones, Sistemas de claves de acceso, cámaras de seguridad, entre otros.
<b>Detectivo</b>	Son aquellos que no evitan que ocurran las causas del riesgo, sino que los detecta luego de ocurridos. Identifican eventos en el momento de presentarse. Ejemplo: Archivos y procesos que sirvan como pistas de auditoría
<b>Correctivo</b>	Ayudan a la investigación y corrección de las causas del riesgo. Aseguran tomar acciones para revertir un evento no deseado

Cumplimiento de Controles		
<b>Cumplimiento de 0%- 60%</b>	<b>Débil</b>	No hay control. El control no cumple su función, existen evidencias de incumplimientos constantes, hay varios incidentes.
<b>Cumplimiento de 61%- 89%</b>	<b>Moderado</b>	El control cumple parcialmente su función, se han presentado algunos incidentes.
<b>Cumplimiento del 90% a 100%</b>	<b>Fuerte</b>	El control es robusto, cumple plenamente su función, no se han presentado incidentes.

## ESCALAS DE PROBABILIDADES

OPORTUNIDADES			RIESGOS	
Nivel	Clasificación	Descripción	Clasificación	Descripción
1	No Realizable	La probabilidad que se pueda realizar es muy baja	Raro	Puede ocurrir en circunstancias excepcionales; una vez cada dos años. / No existen condiciones que impliquen riesgo. El control implementado su efectividad es Fuerte.
2	improbable	<b>Podría realizarse.</b> Existen condiciones que hacen que su probabilidad de realización sea baja o de largo plazo.	Improbable	Podría ocurrir una vez cada dos años. / Existen condiciones que hacen lejana la posibilidad de ocurrencia.
3	Posible	<b>Puede ocurrir su realización.</b> Existen condiciones que hacen que pueda ocurrir en el lapso de un año, siendo una probabilidad media que sucede.	Posible	Puede ocurrir una vez al año / Existen condiciones que hacen poco probable en el corto plazo pero que no son suficientes para evitarlo en el largo plazo.
4	Probable	<b>Probablemente se realice.</b> Se puede dar en el corto plazo y no existen condiciones que impidan la ocurrencia.	Probable	Probablemente ocurrirá una vez al mes. / No existen condiciones que impidan la ocurrencia.
5	Realizable	Se puede realizar en la mayoría de las circunstancias. La ocurrencia es inminente.	Muy probable	Ocurrirá en la mayoría de las circunstancias; varias veces al mes. / La ocurrencia es inminente.

 <p><b>Sunass</b> El regulador del agua potable</p>	GESTIÓN DIRECTIVA		MODERNIZACIÓN Y ADMINISTRACIÓN DE LOS SISTEMAS DE GESTIÓN	
	FORMATO	MATRIZ DE RIESGOS Y OPORTUNIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: GDI-MAS-FM023	Versión: 001	Fecha de vigencia:	Página 6 de 8

## ESCALAS DE IMPACTOS

Nivel	OPORTUNIDADES		RIESGOS	
	Clasificación	Descripción	Clasificación	Descripción
1	Muy Bajo	Impacto no significativo, no beneficiaría el logro de objetivos de la compañía o terceros. No impacta en los procesos.	Muy Bajo	Impacto insignificante, no afectaría actividades ni procesos de la organización o terceros.
2	Bajo	Impacto no significativo. Beneficiaría con un margen mínimo el logro de objetivos de la compañía o terceros. El impacto es mínimo en los procesos.	Bajo	Impacto insignificante, afectaría una actividad o proceso no críticos de la organización o terceros.
3	Moderado	Impacto que podría ocasionar un beneficio para el logro de objetivos de la compañía o terceros hasta a un 50%. El impacto es moderado en los procesos.	Moderado	Impacto que podría ocasionar un perjuicio en una actividad o proceso crítico o más de una actividad o proceso no crítico de la organización o terceros.
4	Alto	Impacto que podría ocasionar en beneficio para el logro de objetivos de la compañía o terceros entre 80% a 90%. El impacto es alto en los procesos.	Alto	Impacto que podría ocasionar un perjuicio significativo para la organización o terceros y que podría impedir la ejecución de las actividades de la organización.
5	Muy Alto	Impacto que podría ocasionar un beneficio para el logro de objetivos de la institución entre 91% a 100% y que además genera nuevas oportunidades en el ámbito de tecnología y de negocio	Muy Alto	Impacto que podría ocasionar un perjuicio significativo o catastrófico para la organización, terceros o podría impedir la ejecución de las actividades de la organización, incumplimientos legales, regulatorios, normativos, hay multas y/o sanciones

## MAPAS DE CALOR

MAPA DE CALOR DE RIESGOS						
		1 Muy Bajo	2 Bajo	3 Moderado	4 Alto	5 Muy Alto
PROBABILIDAD	5 Casi Cierto	Bajo	Moderado	Alto	Muy Alto	Muy Alto
	4 Probable	Bajo	Moderado	Alto	Alto	Muy Alto
	3 Posible	Muy Bajo	Bajo	Moderado	Alto	Alto
	2 Improbable	Muy Bajo	Bajo	Bajo	Moderado	Moderado
	1 Raro	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo

MAPA DE CALOR DE OPORTUNIDADES						
		1 Muy Bajo	2 Bajo	3 Moderado	4 Alto	5 Muy Alto
PROBABILIDAD	5 Realizable	Baja	Moderada	Alta	Muy Alta	Muy Alta
	4 Probable	Baja	Moderada	Alta	Alta	Muy Alta
	3 Posible	Muy Baja	Baja	Moderada	Alta	Alta
	2 Improbable	Muy Baja	Baja	Baja	Moderada	Moderada
	1 No Realizable	Muy Baja	Muy Baja	Muy Baja	Baja	Baja

 <p>El regulador del agua potable</p>	GESTIÓN DIRECTIVA		MODERNIZACIÓN Y ADMINISTRACIÓN DE LOS SISTEMAS DE GESTIÓN	
	FORMATO	MATRIZ DE RIESGOS Y OPORTUNIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: GDI-MAS-FM023	Versión: 001	Fecha de vigencia:	Página 7 de 8

## ESTRATEGIAS DE TRATAMIENTO

ESTRATEGIAS PARA EL TRATAMIENTO - RIESGOS	
Estrategia	Descripción
Reducir	El nivel del riesgo se debería reducir mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable.
Aceptar	Significa asumir un riesgo y las consecuencias que este traiga en el momento que se presente. Los riesgos <b>se aceptan cuando la frecuencia es baja e impacto leve, y no pones en peligro la estabilidad de la organización</b>
Retener	Es posible que existan algunos riesgos para los cuales la organización no puede identificar controles o el costo del control sobrepasa la potencial pérdida si ocurriese el riesgo. En estos casos se puede tomar la decisión de retener el riesgo y vivir con las consecuencias, si ocurriera.
Evitar	Se debería evitar la actividad o la acción que da origen al riesgo particular.
Compartir	El riesgo se debería transferir o compartir a otra de las partes que pueda manejar de manera más eficaz el riesgo particular dependiendo de la valoración del riesgo.

ESTRATEGIAS PARA EL TRATAMIENTO - OPORTUNIDADES	
Estrategia	Descripción
Explotar	Aumenta la posibilidad de la oportunidad, potenciándola
Compartir	Compartir un riesgo positivo con terceros aumenta la capacidad que salga adelante.
No Implementar	Aceptar que viene una oportunidad, cuando se presente veremos cómo abordarla. Por ahora no representa un beneficio para la organización

	GESTIÓN DIRECTIVA		MODERNIZACIÓN Y ADMINISTRACIÓN DE LOS SISTEMAS DE GESTIÓN	
	FORMATO	MATRIZ DE RIESGOS Y OPORTUNIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: GDI-MAS-FM023	Versión: 001	Fecha de vigencia:	Página 8 de 8

## ANEXO- ASPECTOS RELEVANTES PARA LA APLICACIÓN DEL FORMATO

### 1. EVALUACIÓN DE RIESGOS Y OPORTUNIDADES

- Se identifican los riesgos de seguridad de la información para los activos con nivel de criticidad: Crítico y Alto.
- En base a las buenas prácticas de gestión de riesgos se ha establecido cinco niveles de evaluación de riesgos y oportunidades, los cuales son: Muy Bajo, Bajo, Moderado, Alto y Muy Alto. Tanto para la probabilidad como para determinar el impacto.

### 2. SOBRE LOS NIVELES Y CRITERIOS DE ACEPTACION DE RIESGOS

De acuerdo con el análisis de la Matriz de Contexto y la Matriz de Necesidades y Expectativas de las Partes Interesadas del SGSI, se ha establecido que se aceptan aquellos riesgos de nivel "Muy Bajo", "Bajo" y "Moderado", y no se aceptan los riesgos de nivel "Alto" y "Muy Alto" los cuales deben ser tratados.

### 3. NIVELES Y CRITERIOS DE ACEPTACION DE OPORTUNIDADES

En el caso de las Oportunidades se ha establecido que no se aceptan los niveles "Muy Baja", "Baja" y "Moderada", y se aceptan las Oportunidades de nivel "Alta" y "Muy Alta" las cuales deben ser tratadas.

### 4. DETERMINACION DEL NIVEL DE RIESGOS Y OPORTUNIDADES

- El nivel del riesgo es la combinación de la probabilidad y el impacto, es decir  $NR = P * I$
- El nivel de la Oportunidad es la combinación de la probabilidad y el impacto, es decir  $NO = P * I$