
	<b>INSTRUCTIVO DILIGENCIAMIENTO HERRAMIENTA MATRIZ RIESGOS SEGURIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO:</b> E-SGI-SI-I005
		<b>Versión:</b> 01
		<b>Fecha:</b> 28/02/2022
		<b>Página</b> 1 de 8

## INSTRUCTIVO DILIGENCIAMIENTO HERRAMIENTA MATRIZ RIESGOS SEGURIDAD DE LA INFORMACIÓN

### Contenido

1. <b>Objetivo:</b> .....	3
2. <b>Alcance:</b> .....	3
3. <b>Descripción:</b> .....	3
<b>3.1 Matriz de Riesgo:</b> .....	3
4. <b>Indicaciones Diligenciamiento Matriz de Riesgo</b> .....	3
1. <b>ID. Riesgo</b> .....	4
2. <b>Proceso</b> .....	4
3. <b>Activo de Información</b> .....	4
4. <b>Descripción Activo</b> .....	4
5. <b>Identificación Impacto</b> .....	4
6. <b>Vulnerabilidad</b> .....	4
7. <b>Causa Inmediata</b> .....	4
8. <b>Causa Raíz</b> .....	5
9. <b>Descripción del Riesgo</b> .....	5
10. <b>Clasificación del Riesgo</b> .....	5
11. <b>Probabilidad Inherente</b> .....	5
12. <b>Impacto Inherente</b> .....	5
13. <b>Zona de Riesgo Inherente</b> .....	6
14. <b>Número de Control</b> .....	<b>¡Error! Marcador no definido.</b>
15. <b>Descripción del Control</b> .....	6
16. <b>Afectación</b> .....	6
17. <b>Atributos de los Controles</b> .....	6
18. <b>Probabilidad Residual</b> .....	7
19. <b>Impacto Residual</b> .....	7
20. <b>Zona de Riesgo Residual</b> .....	7
21. <b>Tratamiento</b> .....	7
22. <b>Plan de Acción</b> .....	7
23. <b>Responsable</b> .....	7

24.	<b>Fecha Inicio Implementación</b> .....	7
25.	<b>Fecha Seguimiento</b> .....	7
26.	<b>Seguimiento</b> .....	8
27.	<b>Estado</b> .....	8
28.	<b>Observaciones</b> .....	8
5.	<b>Actualización</b> .....	8
6.	<b>Historial de Cambios</b> .....	8

	<b>INSTRUCTIVO DILIGENCIAMIENTO HERRAMIENTA MATRIZ RIESGOS SEGURIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO:</b> E-SGI-SI-I005
		<b>Versión:</b> 01
		<b>Fecha:</b> 28/02/2022
		<b>Página</b> 3 de 8

## INSTRUCTIVO DILIGENCIAMIENTO HERRAMIENTA MATRIZ RIESGOS SEGURIDAD DE LA INFORMACIÓN

### 1. Objetivo:

Identificar las casillas correspondientes a la herramienta Matriz de Riesgo para su correcto diligenciamiento.

### 2. Alcance:

Aplica a los todos aquellos activos de información que se consideren críticos en la entidad y se hayan registrado en la matriz de activos de información

### 3. Descripción:

#### 3.1 Matriz de Riesgo:

La herramienta Matriz de Riesgo está alineada con el **Instructivo Riesgos de Seguridad de la Información en su versión 03**, diseñada en hoja de cálculo, le permitirá consignar la información concerniente de los riesgos detectados en los Activos de Información de la entidad (IDEAM) y su tratamiento basado en controles.

A continuación, encontrará las indicaciones para su diligenciamiento.

### 4. Indicaciones Diligenciamiento Matriz de Riesgo

Estas indicaciones le permitirán diligenciar la Matriz de Riesgo de una forma ordenada, contiene los aspectos más relevantes en la Gestión del Riesgo; La matriz está compuesta de múltiples casillas, las cuales se deberán diligenciar en su totalidad, existen casillas de selección y otras son de texto libre, algunas son automáticas y corresponden a la visualización de resultados, en ningún caso se deben alterar o cambiar su formulación.

	<b>INSTRUCTIVO DILIGENCIAMIENTO HERRAMIENTA MATRIZ RIESGOS SEGURIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO:</b> E-SGI-SI-I005
		<b>Versión:</b> 01
		<b>Fecha:</b> 28/02/2022
		<b>Página</b> 4 de 8

1. **ID. Riesgo** (Identificador de Riesgo):  
En esta casilla se asigna (digita) un número consecutivo a cada riesgo identificado comenzando por el número 1 (uno) en adelante.
  
2. **Proceso** (Selección del Proceso):  
En esta casilla se selecciona el nombre del proceso donde fue identificado el riesgo y donde pertenece el activo de información, para cada proceso, se antepone la letra que identifica la categoría del mismo.  
**E:** estratégicos, **M:** Misionales, **A:** Apoyo: **EV:** Evaluación.
  
3. **Activo de Información** (Selección del Activo de Información):  
En esta casilla se escribe el nombre del activo de información, o el nombre que se le asigna a un grupo de activos de información con características similares.
  
4. **Descripción Activo** (Descripción del Activo de Información):  
Esta casilla permite de forma clara y concisa describir el Activo de Información identificado, se debe indicar brevemente su utilidad y contenido dentro de la entidad.
  
5. **Identificación Impacto** (Identificación de Impacto):  
En esta casilla se debe seleccionar el tipo de Impacto que puede causar para la organización en caso de materialización del riesgo, los tipos de impacto que se pueden seleccionar son los siguientes: **Económica** (afectación económica), **Reputación** (afectación a la reputación), **Económica y Reputación** (afectación conjunta).
  
6. **Vulnerabilidad** (Identificación de la Vulnerabilidad):  
En esta casilla se debe seleccionar la vulnerabilidad que pueda presentar el activo de información, si este presenta más de una vulnerabilidad aún si no la encuentra en el listado, estas se deben consignar en la casilla observaciones.
  
7. **Causa Inmediata** (Causa Inmediata):  
En esta casilla se debe describir brevemente en lenguaje claro y entendible para la mayoría, la razón o razones evidentes que se pueden percibir de: ¿Cómo es posible que se materialice el riesgo en el activo de información?, se debe responder a la pregunta ¿Cómo?

	<b>INSTRUCTIVO DILIGENCIAMIENTO HERRAMIENTA MATRIZ RIESGOS SEGURIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO:</b> E-SGI-SI-I005
		<b>Versión:</b> 01
		<b>Fecha:</b> 28/02/2022
		<b>Página</b> 5 de 8

8. **Causa Raíz** (Causa Raíz):

En esta casilla se debe describir brevemente en lenguaje claro y entendible para la mayoría, la razón principal del: ¿por qué puede presentar el riesgo en el activo de información?, se debe encontrar el punto inicial o causa raíz.

9. **Descripción del Riesgo** (Descripción del Riesgo):

En esta casilla se debe describir el riesgo identificado y que pudiese afectar al activo de información, esta descripción debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso, en la estructura de la descripción del riesgo se deben tener en cuenta las vulnerabilidades, causa inmediata y causa raíz.

10. **Clasificación del Riesgo** (Clasificación del Riesgo):

En esta casilla se debe seleccionar del listado existente, la clasificación que corresponda al riesgo, dentro de las opciones se tiene: i) Daños Activos Físicos, ii) Ejecución y Administración de procesos, iii) Fallas Tecnológicas, iv) Fraude Externo, v) Fraude Interno, vi) Relaciones Laborales, vii) Usuarios, productos y prácticas organizacionales.

11. **Probabilidad Inherente** (Frecuencia con la cual se realiza la actividad):

Para diligenciar esta casilla se debe visualizar la pestaña "PROBABILIDAD", allí se describen las escalas de frecuencia de la actividad con su respectivo valor de probabilidad en escala de porcentaje (%) y color asignado, estas se deben leer atentamente y seleccionar la que corresponda; enseguida se debe regresar a la matriz principal y escoger en la lista desplegable la opción más adecuada según el análisis previo. Las opciones existentes son: Muy Alta, Alta, Media, Baja, Muy Baja, al seleccionar alguna de las opciones, se reflejará en la siguiente celda el valor en porcentaje correspondiente.

12. **Impacto Inherente** (Criterios de Impacto):

Para diligenciar esta casilla se debe visualizar la pestaña "IMPACTO", allí se describen las escalas de impacto a la Información, Afectación Económica y Afectación Reputación, con su respectivo valor de impacto en escala de porcentaje (%) y color asignado, estas se deben leer atentamente y seleccionar la que corresponda; enseguida se debe regresar a la matriz principal y escoger en la lista desplegable la opción más adecuada según el análisis previo. Las opciones existentes son: Catastrófico, Mayor, Moderado, menor, Leve, al seleccionar alguna de las opciones, se reflejará en la siguiente celda el valor en porcentaje correspondiente.

	<b>INSTRUCTIVO DILIGENCIAMIENTO HERRAMIENTA MATRIZ RIESGOS SEGURIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO:</b> E-SGI-SI-I005
		<b>Versión:</b> 01
		<b>Fecha:</b> 28/02/2022
		<b>Página</b> 6 de 8

13. **Zona de Riesgo Inherente** (Zona de Riesgo Inherente)

Esta casilla hace alusión a la zona dentro del mapa de calor donde se encuentra ubicado el Riesgo Inherente, para ello se debe tener información precisa acerca de la Probabilidad Inherente y el Impacto Inherente calculado anteriormente, enseguida se verifica la pestaña Mapa de Calor (Zona) y de forma matricial se ubican los puntos correspondientes, determinando así la Zona de Riesgo Inherente, esta se calcula automáticamente y sus valores pueden ser: Extremo, Moderado Alto Bajo, según la ubicación previa.

14. **Dominios** (Norma ISO 27002 Controles)

En esta casilla se debe seleccionar el Dominio del control que se va a aplicar, de esta manera se cargará en la siguiente columna (**Numero de Control/Descripción del Control**) el control correspondiente dentro de la celda.

15. **Numero de Control/Descripción del Control** (Descripción del Control)

En esta casilla se debe seleccionar el control que se van a aplicar para el tratamiento del riesgo identificado, puede consultar la norma ISO/IEC 27002:2013 la cual consta de 14 Dominios, 35 Objetivos de Control y 114 Controles, los cuales se pueden aplicar.

En caso que existan controles que no son tomados de la norma, igualmente se deberán registrar manualmente agregando una fila adicional.

16. **Afectación** (Afectación)

**Probabilidad:** En esta casilla se seleccionará, si el control tratará la Probabilidad.

**Impacto:** En esta casilla se seleccionará, si el control tratará el Impacto.

17. **Atributos de los Controles** (Atributos de los Controles)

**Tipo:** En esta casilla se debe seleccionar si el control es: Preventivo, Correctivo, Detectivo.

**Implementación:** En esta casilla se debe seleccionar si el control se ejecuta en modo automático o manual.

**Documentado:** En esta casilla se debe seleccionar si el control esta Documentado o Sin Documentar.


**Frecuencia:** En esta casilla se debe especificar si el control tiene una frecuencia continua o si por el contrario es aleatoria.

**Evidencia:** En esta casilla se debe seleccionar si el control contará con registro o si por el contrario no contará con el mismo (sin registro).

	<b>INSTRUCTIVO DILIGENCIAMIENTO HERRAMIENTA MATRIZ RIESGOS SEGURIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO:</b> E-SGI-SI-I005
		<b>Versión:</b> 01
		<b>Fecha:</b> 28/02/2022
		<b>Página</b> 7 de 8

**Calificación:** En esta casilla se visualizará la calificación obtenida según los atributos configurados anteriormente.

18. **Probabilidad Residual** (Probabilidad Residual)  
En esta casilla se visualiza el estado de la probabilidad residual (Muy Baja, Baja, Media, Alta, Muy Alta) con identificación de color asignado, verificando si el control afecta o no este componente.
19. **Impacto Residual** (Impacto Residual)  
En esta casilla se visualiza el Impacto Residual (Catastrófico, Mayor, Moderado, Menor, Leve) correspondiente al análisis realizado, verificando si el control afecta o no este componente.
20. **Zona de Riesgo Residual** (Zona de Riesgo Residual)  
Esta casilla hace alusión a la zona dentro del mapa de calor donde se encuentra ubicado el Riesgo Residual, para ello se debe tener información precisa acerca de la Probabilidad Residual y el Impacto Residual calculado anteriormente, enseguida verifique la zona de Riesgo donde se encuentra ubicado el riesgo residual seleccionando la **casilla de color azul** donde se describe la zona a ubicar, luego presione el botón **“Verificar Zona”**, diríjase a la pestaña **“Matriz de Calor (Zona)”**, allí podrá observar en **color azul claro**, la zona donde está ubicado el riesgo calculado actualmente luego de la aplicación de controles, como resultado puede obtener: Zona de Riesgo (Extremo, Moderado, Alto, Bajo), según la ubicación.
21. **Tratamiento** (Tratamiento)  
Esta casilla hace alusión a la zona dentro de la Matriz Opciones de Riesgo donde se ubicará el Riesgo Residual, para ello se debe ir a la pestaña donde se encuentra la Matriz Opciones de Riesgo y ubicar la misma posición matricial del Riesgo Residual, de manera tal, que pueda visualizar las opciones de tratamiento y escoger una para ser modificada en la casilla tratamiento (Aceptar, Reducir o Mitigar, Transferir o Compartir, Evitar o Eliminar).
22. **Plan de Acción** (Plan de Acción)  
En esta casilla se debe describir las acciones y/o actividades que se deben llevar a cabo para la ejecución del control o controles.
23. **Responsable** (Responsable)  
En esta casilla se debe asignar el responsable o responsables de la ejecución del control, indicando su nombre y cargo dentro de la entidad.
24. **Fecha Inicio Implementación** (Fecha Inicio Implementación)  
En esta casilla se debe consignar la fecha de inicio de implementación del control, el formato fecha se establece como DD/MM/AA.
25. **Fecha Seguimiento** (Fecha Seguimiento)  
En esta casilla se consignarán las fechas de seguimiento al control o controles, el formato fecha se establece como DD/MM/AA.

	<b>INSTRUCTIVO DILIGENCIAMIENTO HERRAMIENTA MATRIZ RIESGOS SEGURIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO:</b> E-SGI-SI-I005
		<b>Versión:</b> 01
		<b>Fecha:</b> 28/02/2022
		<b>Página</b> 8 de 8

**26. Seguimiento** (Seguimiento)

En esta casilla se deberán relacionar las evidencias del seguimiento, estas pueden ser (informes, reportes, checklist, entre otros), que se establezcan para su mejora continua.

**27. Estado** (Estado)

En esta casilla se debe consignar la escala de porcentaje entre (0% - 100%), el avance o estado en la implementación del control.

**28. Observaciones** (Observaciones)

En esta casilla se deben consignar todas aquellas observaciones que se consideren importantes, acerca del riesgo, control, vulnerabilidades y demás que sean de interés.

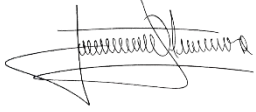


**5. Actualización**

La Matriz de Riesgo se debe actualizar constantemente verificando el estado de los controles y nuevos riesgos asociados.

<b>ELABORADO POR:</b>	Guillermo Otálora Luna
-----------------------	------------------------

**6. Historial de Cambios**

VERSIÓN	FECHA	DESCRIPCIÓN
01	28/02/2022	Creación del Documento

<b>ELABORÓ</b>  <b>Guillermo Otálora Luna</b> Oficial Seguridad Información	<b>REVISÓ</b>  <b>Eduardo Emilio Ramírez</b> Coordinador GAESI	<b>APROBÓ</b>  <b>Alicia Barón Leguizamón</b> Jefe Oficina de Informática
---	--	---