Alcaldía Mayor de
Cartagena de Indias

Gestión de Riesgos de Seguridad y Privacidad de la Información (GRSPI)

Alcaldía de Cartagena

Séptima mesa de Transformación Digital

“Acompañamiento técnico para el diligenciamiento de la matriz de riesgos SPI”

Noviembre/2025

Alcaldía Mayor de
Cartagena de Indias

Propósito de la sesión

Fortalecer la GRSPI institucional, garantizando la confidencialidad, integridad y disponibilidad de la información distrital.

Metodología de MinTIC para identificar y valorar riesgos.	Guiar el diligenciamiento de la matriz GRSPI institucional.	Promover la cultura de autocontrol digital.

Alcaldía Mayor de
Cartagena de Indias

GRSPI en el marco institucional

01 La Política de Administración de Riesgos Institucional 4.0 articula el MIPG, MECI y MSPI..

02 La OAI es segunda línea de defensa, responsable de implementar el MSPI

03 La GRSPI aplica a todas las dependencias, no solo a TI.

Alcaldía Mayor de
Cartagena de Indias

Marco Normativo -Lineamientos

01 Documento Maestro del Modelo de Seguridad y Privacidad de la Información

02 Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

03 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

04 Guía para la Administración del Riesgo y el diseño de controles en entidades públicas

05 Política de Administración de Riesgos Institucional 4.0

06 GTIGPS01-F007 Formato_Activos_Información V2.xlsx

07 GTIGPS01-F001 Matriz_de_riesgos V2.xlsx

Alcaldía Mayor de
Cartagena de Indias

GRSPI – Conceptos

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente..

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

Integridad: Propiedad de exactitud y completitud.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Alcaldía Mayor de
Cartagena de Indias

Hoja de ruta MinTIC para la GRSPI

Paso 1

- Política de seguridad de la información
  - Formulación de una política alineada con el plan estratégico de T.I

Paso 2

- Identificación Y Gestión de Activos
  - Valoración de Activos
  - Priorización de Activos

Paso 3

Gestión de los Riesgos de Seguridad Digital

- Identificación de amenazas y vulnerabilidades
- Análisis/Valoración del riesgo
- Tratamiento del Riesgo

Fuente: MinTIC – Modelo de Seguridad y Privacidad de la Información (MSPI), Gestión de Activos y Riesgos.
https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Alcaldía Mayor de Cartagena de Indias

GRSPI

Identificación de activos de información	Análisis de riesgos	Evaluación del riesgo	Tratamiento riesgo residual
• Listar los activos por cada proceso • Identificar el dueño de los activos • Clasificar los activos • Clasificar la información • Determinar la criticidad del activo • Identificar si existen Infraestructuras Críticas Cibernéticas	• Identificación de amenazas • Identificación de las vulnerabilidades • Identificación de las consecuencias • Valoración de la probabilidad • Valoración del Impacto	• Identificación de riesgo inherente • Identificación de causas o fallas • Identificación de controles existentes • Valoración de los controles existentes • Evaluar el riesgo después de controles (Riesgo residual)	• Determinar opción de tratamiento (Evitar, aceptar, compartir o mitigar el riesgo) • Establecer plan de tratamiento (Responsable, tiempo e indicador) • Ejecución de los planes de tratamiento definidos

Alcaldía Mayor de
Cartagena de Indias

GRSPI - Identificación de activos de información

	ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS	Código: GTIGPS01-F007
	MACROPROCESO: GESTIÓN TECNOLOGÍA E INFORMÁTICA	Versión: 2.0
	PROCESO/ SUBPROCESO: GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN / SEGURIDAD TÁCTICA Y ESTRATEGICA	Fecha: 27/10/2025
	FORMATO DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	Página: 1 de 1

Dependencia		Macroproces o		Proceso		Tipo de diligenciamiento	
Objetivo Proceso							Fecha

IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN (LEY 594 DE 2000 - LEY 1712 DE 2014- DECRETO 103 DE 2015 - DECRETO 1080 DE 2015 - ISO 27001)

SubProceso	Identificador	Código SGD	Tipo	Serie documental	Subserie documental	Nombre	Descripción	Nombre del responsable de la producción de la información	Fecha de generación de la información	Nombre del responsable de la información (Custodio del	Fecha de ingreso del activo al archivo	Soporte de registro	Medio de conservación	Formato	Idion

GTIGPS01-F007 Formato_Activos_Información V2.xlsx

Alcaldía Mayor de
Cartagena de Indias

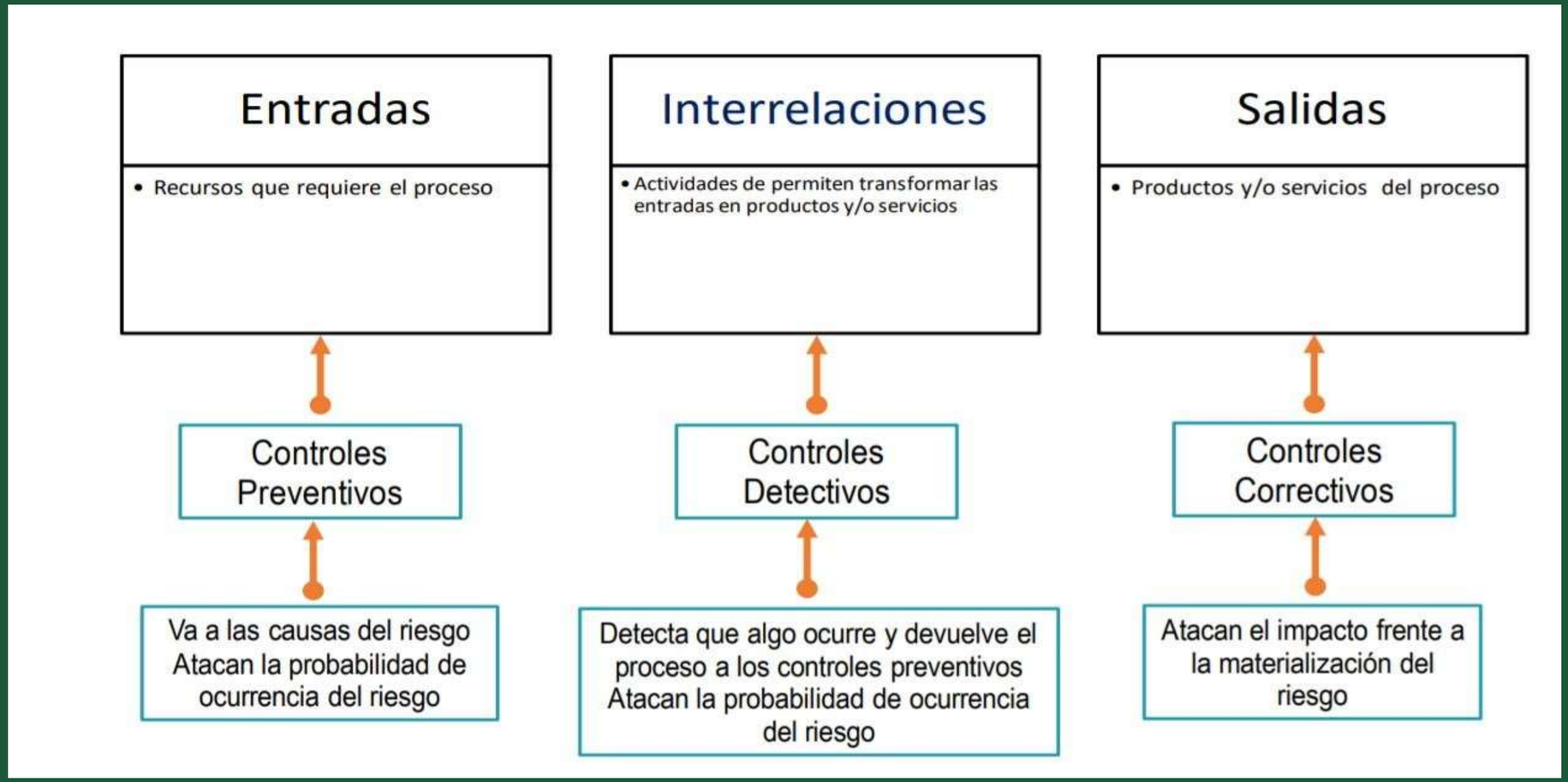
Matriz de GRSPI

	ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS									Código: GTIGPS01-F001
	MACROPROCESO: GESTIÓN TECNOLOGÍA E INFORMÁTICA									Versión: 2.0
	PROCESO/ SUBRPOCESO: GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN / SEGURIDAD TÁCTICA Y ESTRATEGICA									Fecha: 27/10/2025
	MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN									Páginas: 2 de 2
		Descripción del control								
Activo	Amenazas (Causa Inmediata)	Control Anexo A	Descripción del control	Responsable	Fecha de Implementación	Seguimiento	Estado	de segunda línea de defensa o quien haga sus veces	de la Oficina de Control Interno o quien haga sus veces	Estado
0										
0										
0										
0										
0										
0										
0										
0										
0										

GTIGPS01-F001 Matriz de riesgos V2.xlsx

Alcaldía Mayor de
Cartagena de Indias

GRSPI - Tipología de controles



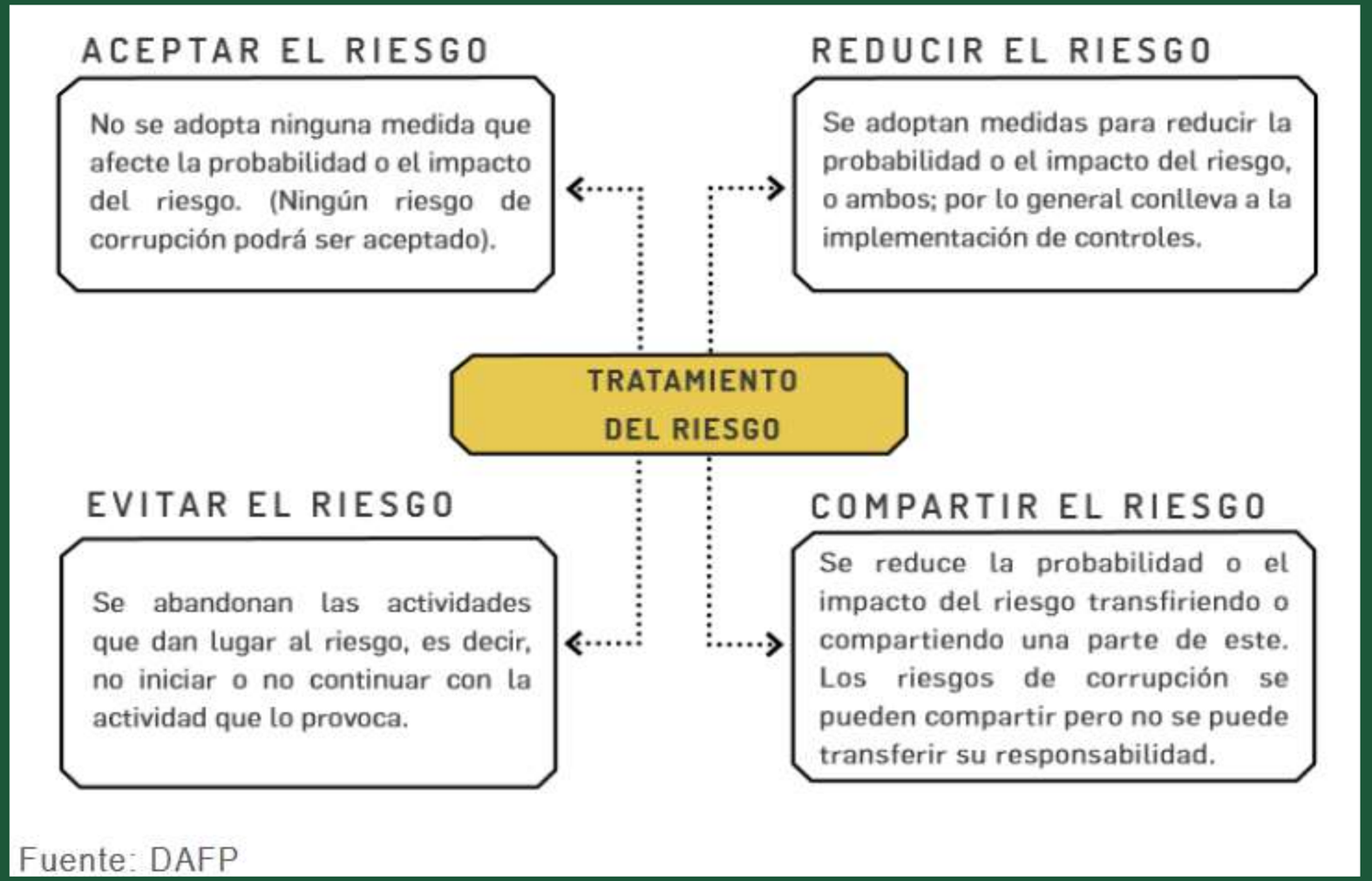
Alcaldía Mayor de Cartagena de Indias

GRSPI - Análisis y evaluación de controles

Características			Descripción
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.
		Sin registro	El control no deja registro de la ejecución del control.

Alcaldía Mayor de
Cartagena de Indias

GRSPI - Tratamiento del riesgo



Fuente: DAFP

Alcaldía Mayor de
Cartagena de Indias

GRSPI – Identificación del riesgo

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Alcaldía Mayor de
Cartagena de Indias

GRSPI – Identificación del riesgo

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

Seleccionar las vulnerabilidades asociadas a la amenaza identificada

Alcaldía Mayor de
Cartagena de Indias

GRSPI – Identificación del riesgo

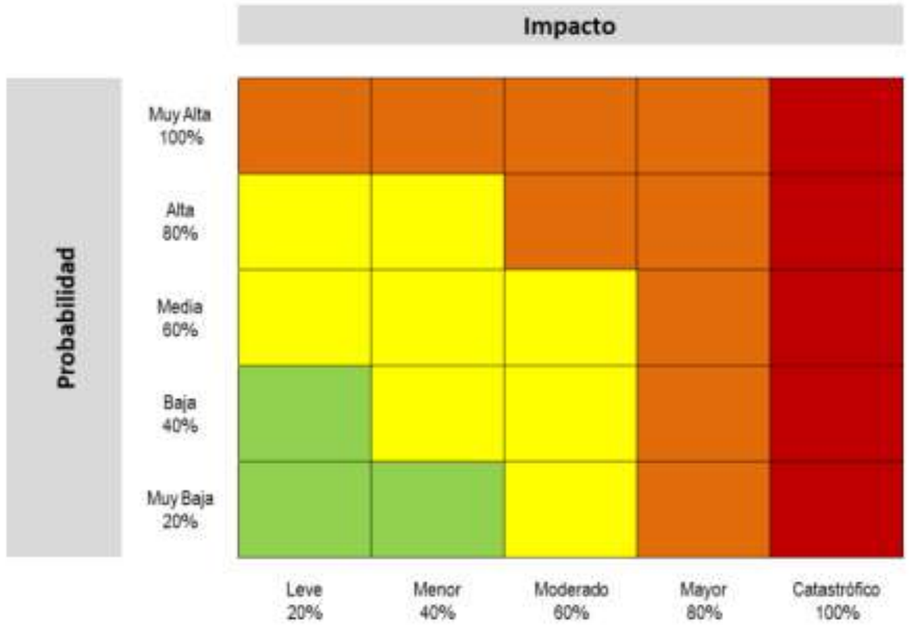
Activo	Riesgo	Descripción del riesgo	Amenaza	Tipo	Causa/ Vulnerabilidades	Consecuencias
Bases de datos de nómina	Pérdida de la integridad	Pérdida de datos por modificación, alteración y eliminación de información de la base de datos de nómina de entidad.	Falsificación de permisos	Información	**1.**Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario **2.**Gestión deficiente de las contraseñas **3.**Tablas de contraseñas sin protección	Pérdida de Dinero, Retraso en el pago de nómina, Demandas por incumpliendo de salarios, Plan tortuga funcionarios, Generación de desconfianza a los ciudadanos.
Servidor de base de datos	Pérdida de confidencialidad	Acceso no autorizado al servidor	Error de uso	Hardware	Ausencia de un eficiente control de cambios en la configuración	Ausencia de un eficiente control de cambios en la configuración Explotación de vulnerabilidades por falta de actualizaciones se seguridad y hardening
Servidor aplicación de impuestos	Pérdida de confidencialidad	Acceso no autorizado al servidor, donde se encuentran los datos de los contribuyentes para el pago de impuestos.	**Uso no autorizado del equipo** **Falsificación de derechos**	Hardware	**1.** Conexiones de red pública sin protección **2.** Arquitectura insegura de la red **3.** Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	**1.** Desconfianza ciudadanos, robo de información, cifrado de información (Ramsonware) **2.** Robo de información, activación de malware, escalamiento de privilegios, modificación y eliminación de datos.
Servidor Portal Web	Pérdida de disponibilidad	Servidor fuera de servicio, impidiendo que los usuarios autorizados no tengan acceso para descargar el recibo de pago de impuestos.	Saturación del sistema de información	Hardware	**1.** Arquitectura insegura de la red **2.** Ausencia de mecanismos de monitoreo	Impedir la descarga de los formatos de pago de impuestos

Alcaldía Mayor de
Cartagena de Indias

GRSPI – Valoración del riesgo

RIESGO	ACTIVO	AMENAZA	VULNERABILI-DAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confiden-cialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Extremo	
Alto	
Moderado	
Bajo	



La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Alcaldía Mayor de
Cartagena de Indias

GRSPI – Riesgo antes y después de controles

Riesgos antes de controles

- Se identifican los riesgos inherentes o subyacentes que puedan afectar el cumplimento de los objetivos estratégicos y de proceso

Causa o fallas

- Se identifican las causas o fallas que puedan dar origen a la materialización del riesgo

Controles

- Para cada cauda se identifica el control o controles

Riesgo después de controles

- Evaluar si los controles están bien diseñados para mitigar el riesgo y si estos se encuentran como fueron diseñados

Alcaldía Mayor de
Cartagena de Indias

GRSPI – Matriz de riesgo de seguridad

1. Es un prerrequisito tener la **MATRIZ DE ACTIVOS** previamente estructurada. Recuerda que tanto el ejercicio de identificación de activos como de gestión de riesgos se realiza a nivel de cada proceso dentro de la entidad.

2. Una vez las entidades han realizado la identificación, clasificación y valoración de los activos, deberán realizar un análisis de los posibles riesgos que pueden afectar a estos activos.

3. Se debería construir una matriz de activos y una de riesgos **por cada proceso de la entidad.**

4. En esta matriz se identificarán cuáles son las vulnerabilidades (o debilidades) en seguridad que puede tener cada activo o grupo de activos y también se identificarán cuáles son las posibles amenazas que podrían aprovechar nuestras debilidades para afectar la seguridad de los activos.

5. La gestión de riesgos de seguridad se realiza siguiendo lo establecido en la **"Guía de Administración de Riesgos de DAFP – Diciembre 2020". Leer esta guía para complementar los fundamentos para usar la matriz.**

Alcaldía Mayor de
Cartagena de Indias

GRSPI – Recomendaciones

Se puede realizar análisis de riesgos tanto por activos individuales como por grupos que tengan características similares, con el objetivo de no hacer demasiado extensivo el ejercicio.

Si hay activos que se diferencien por su alta criticidad, se recomienda analizarlos **por separado**.

El responsable de seguridad de la información debe acompañar en la aplicación de la metodología y apoyar en las sesiones, sin embargo, cada proceso es el responsable de realizar el diligenciamiento, establecimiento de controles y el seguimiento correspondiente.

Establecer controles que sean realizables a plazos razonables.

Alcaldía Mayor de
Cartagena de Indias

Muchas gracias