Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2020 2023

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece las actividades requeridas para la gestión de los riesgos de seguridad y privacidad de la información, en función de la implementación de controles que permitan a la entidad disminuir la probabilidad y el impacto de materialización.

Manizales, enero de 2022

Versión	Fecha versión	Observaciones
1	31 de enero de 2022	

CONTENIDO

1. INTRODUCCIÓN

El Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información define las actuaciones de Corpocaldas entorno a la gestión de riesgo enfocada a procesos, que le permite identificar, evaluar, tratar y dar seguimientos a los riesgos de seguridad de la información a los que estén expuestos los activos de información, para prevenir su materialización y/o reducir los impactos negativos en la gestión institucional

Este documento se basa en las recomendaciones técnicas establecidas por el ministerio de las tecnologías de la información y comunicación MinTIC, apoyadas en sugerencias emitidas por el departamento administrativo de la función pública DAFP para la gestión de riesgos, anexas en el modelo de seguridad y privacidad de la información.

1.1 Definiciones

- **Amenaza:** Circunstancia o evento que puede provocar daños en los sistemas de información produciendo pérdidas tangibles o intangibles.
- **Confidencialidad:** Brinda un nivel de seguridad, el cual asegura que la información sea asequible por las personas autorizadas.
- **Disponibilidad:** Permite la disposición, fiabilidad y el acceso oportuno a los datos y servicios a ser usados cuando sea necesario. La falta de disponibilidad causa una interrupción del servicio y afecta directamente la productividad de las organizaciones. Por ello es importante contar con mecanismos y acciones correctivas disponibles (backups, servicios redundantes) que permitan tomar acciones rápidamente.
- **Integridad:** Certeza de que la información y los datos contenidos en el sistema no han sido modificados por entes externos, previniendo cualquier tipo de modificación no autorizada que pueda alterar los datos.
- **Modelo de Seguridad y Privacidad de la Información (MSPI):** reúne el conjunto de lineamientos, políticas, normas, procesos e instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación

del modelo, así como a la implementación de la Estrategia de Gobierno en Línea, establecida en manual GEL.

- **Riesgo:** Grado de exposición de un activo en donde un agente de amenaza pueda tomar ventaja de una vulnerabilidad causando impacto a la organización.
- **Riesgo Inherente:** Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- **Riesgo residual:** El riesgo que permanece tras el tratamiento del riesgo.
- **Vulnerabilidad:** Son Aquellas debilidades que se presentan en los sistemas, lo cual la hace susceptibles de ser afectada, alterada o destruida por alguna circunstancia indeseada afectando su correcto funcionamiento.

2. OBJETIVO

Determinar las acciones de tratamiento de riesgos de seguridad y privacidad de la información, mediante la identificación, análisis, valoración y tratamiento de los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información, para prevenir su materialización y/o reducir los impactos negativos en la gestión institucional

3. ALCANCE

Los requisitos, lineamientos y acciones establecidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son aplicables de forma anualizada a los procesos estratégicos, misionales, de apoyo y de evaluación, por lo cual deberán ser conocidos y cumplidos por todos los funcionarios, contratistas y terceras partes vinculadas a la Entidad que accedan a los activos de información.

4. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.1 Identificación del riesgo

La identificación del riesgo tiene como propósito determinar que podría suceder que cause una pérdida potencial, entendiendo aspectos claves entre ellos el cómo, dónde y por qué puede ocurrir esta pérdida (ISO 27005).

4.2 Identificación de amenazas

Las amenazas comunes puedes ser de diversos tipos, deliberadas (D), accidentales (A) y ambientales (E). Las acciones deliberadas que tienen como objetivo los activos de la información se identifican con la letra D, la A se utiliza para todas aquellas acciones humanas que pueden dañar accidentalmente los activos de la información y la E para aquellos incidentes que no se basan en la intervención humana.

Tipo	Amenazas	Origen
Daño físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
	Interceptación de señales de interferencia comprometedoras	D

Tipo	Amenazas	Origen
Compromiso de la información	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

A demás de las amenazas, se debe prestar atención a las fuentes de amenazas humanas, a continuación, se mencionan en la siguiente tabla:

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.

Fuente de amenaza	Motivación	Acciones amenazantes
Criminal de la computación	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador (por ejemplo, espionaje cibernético). • Acto fraudulento (por ejemplo, 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 (warfare). • Ataques contra el sistema (por ejemplo, negación distribuida del servicio). • Penetración en el sistema. • Manipulación del sistema.
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	• Ventaja de defensa. • Ventaja Política. • Explotación económica. • Hurto de información. • Intrusión en la privacidad personal. • Ingeniería social. • Penetración en el sistema. • Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología).

Fuente de amenaza	Motivación	Acciones amenazantes
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales) por ejemplo, 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 do (por ejemplo, virus, bomba lógica, troyano). • Venta de información personal. • Errores en el sistema (bugs). • Intrusión al sistema. • Sabotaje del sistema. • Acceso no autorizado al sistema.

Fuente. ISO 27005

4.3 Identificación de vulnerabilidades

Las vulnerabilidades son puntos débiles de un activo que pueden ser aprovechadas o explotadas por una o más amenazas, en la siguiente tabla se muestran algunos ejemplos de amenazas de diferentes áreas que pueden ser explotadas por estas vulnerabilidades.

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
Software	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso

	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

4.4 Identificación de riesgos

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

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 con el desarrollo del proceso.
- ✓ ¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo. Mirar si esto se quita lo amarillo, lo fuccia es lo que se está cambiando.

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: “**Integridad, confidencialidad o disponibilidad**”

Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Se debe identificar:

- ✓ Riesgo
- ✓ Activo
- ✓ Descripción del riesgo
- ✓ Amenaza
- ✓ Tipo

- ✓ Causas/Vulnerabilidades
- ✓ Consecuencias

4.5 Valoración de riesgos

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).

4.6 Análisis de riesgos

Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por lo tanto, se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos.

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

Criterios parar calificar la probabilidad

NIVEL	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Análisis del Impacto

Respecto a la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Es importante resaltar que en la versión 2018 de la Guía de administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

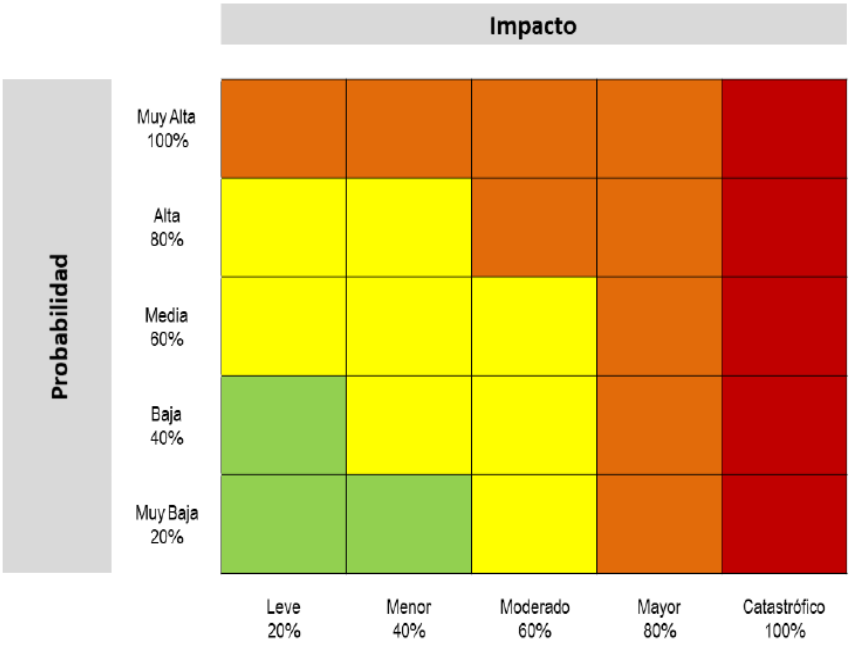
NIVEL	AFECTACIÓN ECONÓMICA	REPUTACIONAL
Leve 20%	Afectación menor a 10 SMLMV . E	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

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

Matriz de calor

Se toma y se ubica la calificación de probabilidad en la fila y la de impacto en la columna correspondiente y se establece el punto de cruce de las dos para definir el riesgo inherente.

se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.



Riesgo Extremo. Reducir el riesgo, evitar y transferir

Riesgo alto. Reducir el riesgo, evitar y transferir

Riesgo moderado. Asumir el riesgo, Reducir el riesgo.

Riesgo bajo. Asumir el riesgo.

5. TRATAMIENTO DEL RIESGO

El tratamiento del riesgo incluye todas las actividades relacionadas para el control de los riegos identificados y valorados. El riesgo puede ser aceptado, reducido, evitado o transferido, por medio de la aplicación de controles de seguridad, de acuerdo de aplicabilidad.

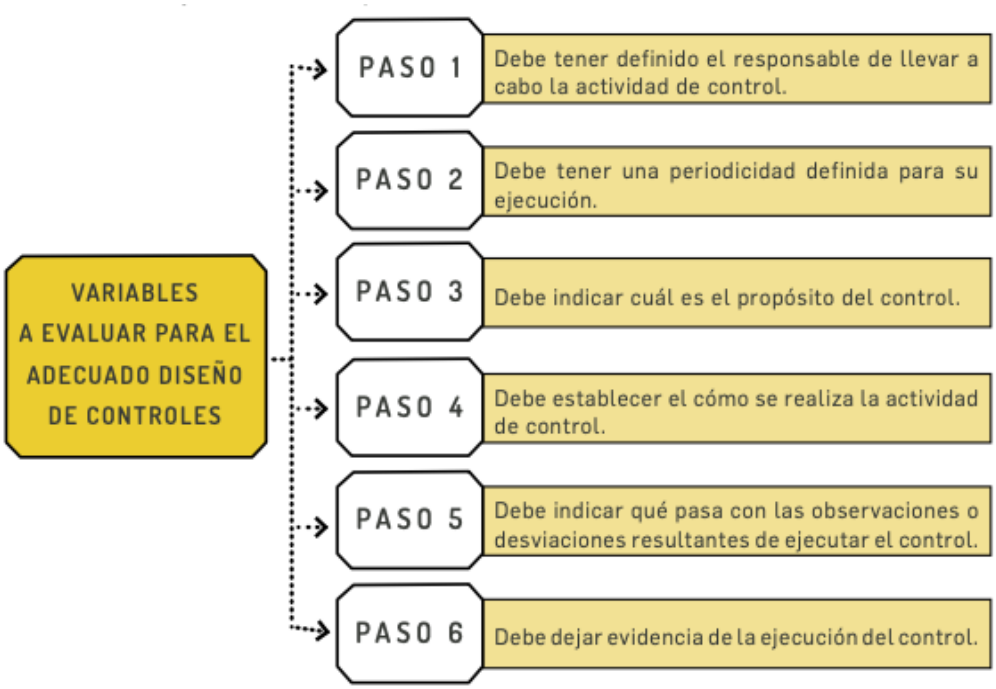
5.1 EVALUACIÓN DEL RIESGO

La evaluación del riesgo es una actividad de suma importancia para el tratamiento del riesgo, ya que es la acción previa y posterior al establecimiento de los respectivos controles que evitarán o reducirán el riesgo identificado.

Es de resaltar que a la hora de implementar las actividades que definirán los controles, se debe considerar un correcto diseño en estas, ya que su éxito dependerá exclusivamente de este y de una implementación clara.

5.2 Diseño de controles

CORPOCALDAS debe garantizar el desarrollo de controles que sean eficientes y logren el objetivo de disminuir el impacto o la probabilidad del riesgo que va a controlar, para ello, a continuación, se enumeran un conjunto de pasos definidos en la guía del DAFP, que permiten diseñar controles adecuados.



PASO 1: Tener definido el responsable de llevar a cabo el control.

Las actividades del control deben tener un responsable, quién debe poseer la autoridad, los conocimientos y las habilidades para ejecutar en control dentro de los procesos, además es importante segregar las responsabilidades en diferentes individuos, con el fin de disminuir los riesgos de error o de actuaciones irregulares o fraudulentas

PASO 2: Tener una periodicidad definida.

Se debe establecer una periodicidad específica para la ejecución del control, se pueden establecer tiempos (diario, mensual, trimestral, anual u otro que se defina según la necesidad). Un indicador que ayuda a establecer si la periodicidad del control está bien establecida, es si al ejecutarse dicho control según su periodicidad ayuda a prevenir o detectar de manera oportuna el riesgo.

PASO 3: Indicar cuál es el propósito del control.

El o los controles que se definan, deben tener un propósito que indique para qué se realiza y que conlleve a mitigar las causas que propician el riesgo (verificar, validar, conciliar, comparar, revisar y cotejar) o detectar la materialización del riesgo.

Es importante destacar que es mejor pensar primero en tener controles preventivos que controles detectivos.

PASO 4: Establecer el cómo se realiza la actividad de control.

Es necesario que el control tenga facilidad de ser evaluado, para esto es indispensable saber cómo se realizan las actividades establecidas en él. La fuente de la información de donde provienen los elementos de entrada del control deben ser confiables, un mecanismo recomendado para la evaluación es la utilización de listas de chequeo.

PASO 5: Indicar qué pasa con las observaciones o desviaciones al ejecutar el control.

El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones

PASO 6: Dejar evidencia de la ejecución del control.

Las ejecuciones de los controles deben dejar evidencia, tanto por procesos de auditoría o ya sea por el ciclo básico del control que tiene dentro de sus fases la verificación y evaluación del control, lo que hace que sea necesario que cada control ejecutado cuente con un registro.

5.3 Valoración de controles

En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

5.4 Estructura para la descripción del control

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.

Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

5.5 Tipología de controles y procesos

A través del ciclo de los procesos es posible establecer cuándo se activa un control y , por lo tanto, establecer su tipología con mayor precisión.

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

5.6 Análisis y evaluación de controles

Atributos: A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la	25%

			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*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.	-

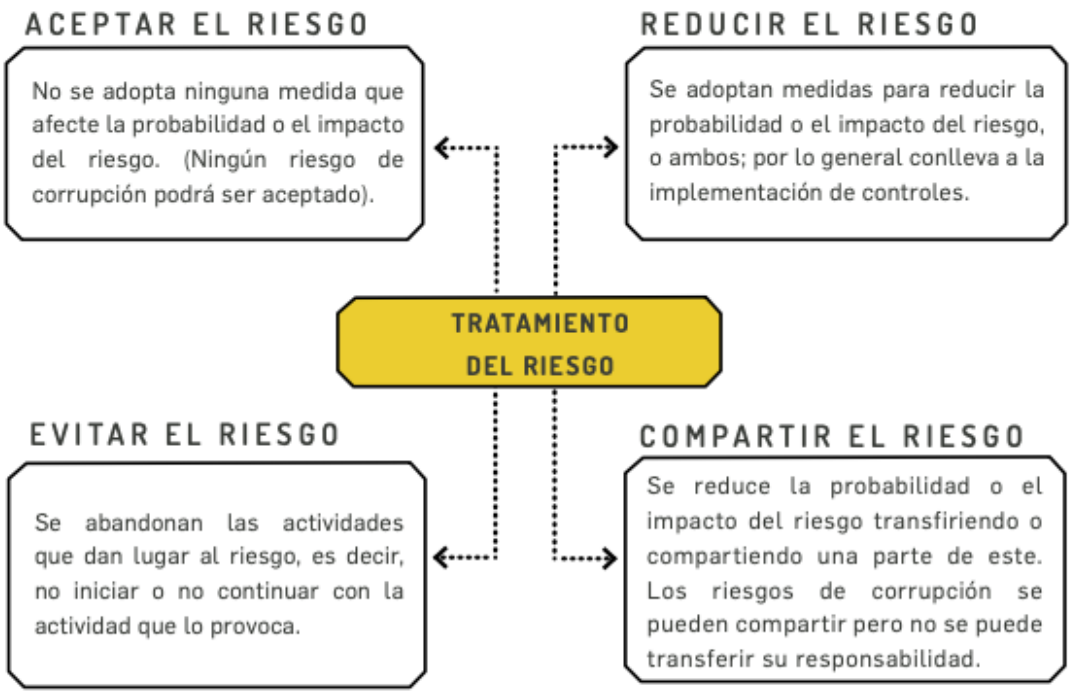
5.7 Criterios del Tratamiento del riesgo

El tratamiento de riesgo es la estrategia utilizada para la mitigación de los riesgos identificados en una organización. Los diferentes riesgos pueden generar retos para la entidad, ya que se pueden presentar casos donde la respuesta a un riesgo genere otro (riesgo residual) que supere los niveles de aceptación, lo que ocasionará que sea hará un rediseño del control que trataba a dicho riesgo. Uno de los aspectos más importantes de la entidad en tema de riesgos, es buscar mitigar los actos asociados a hechos de corrupción (riesgos), ante esto siempre la respuesta será evitar, compartir o reducir el riesgo.

El tratamiento o la respuesta al riesgo se enmarca en las siguientes categorías:

- Aceptar el riesgo.
- Reducir el riesgo.
- Compartir el riesgo.
- Evitar el riesgo.

En la siguiente imagen se observa en detalle las categorías del riesgo.



6. HOJA DE RUTA

Actividad	Fecha Inicio	Fecha Fin	Responsable
Definir y aprobar política de seguridad de la información	15/03/2022	15/05/2022	Subdirección de Planificación Ambiental y Equipo MSPI Comité de Gestión y Desempeño
Desarrollar y/o actualizar el inventario de activos de información	1/04/2022	30/08/2022	Subdirección de Planificación Ambiental y Equipo MSPI
Elaborar procedimientos gestión de Riesgos de seguridad de la información	15/03/2022	15/08/2022	Subdirección de Planificación Ambiental y Equipo MSPI
Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información	15/03/2022	15/08/2022	Subdirección de Planificación Ambiental y Equipo MSPI
Definir herramienta del análisis de Riesgo de seguridad de la Información para la implementación del riesgo	15/03/2022	15/08/2022	Subdirección de planificación Ambiental y Equipo MSPI
Ejecutar Plan de riesgos de seguridad y privacidad de la información	1/08/2022	15/10/2022	Subdirección de planificación Ambiental y Equipo MSPI
Definición e inicio de ejecución de plan de concientización, educación y formación en seguridad y privacidad de la información	1/10/2022	15/12/2022	Subdirección de planificación Ambiental y Equipo MSPI Comunicaciones