TABLA DE CONTENIDO

INTRODUCCIÓN

La administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las instituciones minimizar pérdidas y maximizar oportunidades.

Todos los colaboradores de la ESE Centro, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

1. OBJETIVO

Definir la metodología para el tratamiento de los riesgos de seguridad y privacidad de la información.

1.1. OBJETIVOS ESPECIFICOS

- Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI
- Calcular el nivel de riesgo
- Establecer el plan de tratamiento de riesgos
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos

2. ALCANCE

Esta política, proporciona la metodología establecida por la Institución para la administración y gestión de los riesgos a nivel de procesos; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

3. DEFINICIONES

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

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).

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.

Control o Medida: Medida que permite reducir o mitigar un riesgo.

4. MARCO LEGAL

Resolución 500 de 2021

5. RESPONSABILIDADES

Evaluación y Mejora

Control Interno

Lideres de Proceso

Funcionarios

6. TALENTO HUMANO REQUERIDO

Control Interno – Profesional Monitoreo de materialización de riesgos

Evaluación y Mejora – Mejora continua

Lideres de proceso – Monitoreo constante para NO materializar el riesgo.

7. MATERIALES, INSUMOS Y EQUIPOS REQUERIDOS

Plan de Seguridad de la Información

Matriz de Riesgos (Almera)

8. MARCO TEORICO

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, corrupción, Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los servicios (riesgos de interrupción) de la Red de Salud del Centro ESE procurando que no se materialicen, atendiendo los lineamientos establecidos en el plan de seguridad y privacidad de la información, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos

9. DESARROLLO DEL PROGRAMA

ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, colaboradores de la ESE Centro y contratistas; por esto, es preciso identificar los actores que intervienen:

- Alta Dirección: aprueban las directrices para la administración del riesgo en la Institución. La gerencia es la responsable del fortalecimiento de la política de administración del riesgo.
- Proceso Administración del Sistema Integrado de Gestión: Genera la metodología para la administración del riesgo de la Institución, coordina, lidera, capacita y asesora en su aplicación.
- Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la institución (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.
- Colaboradores de la ESE Centro y contratistas: ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la

identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la institución.

- Quien haga las veces de Control Interno: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La ESE CENTRO adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la institución se comprometen a:

- Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
- Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la institución para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la gerencia asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, la presente guía forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la institución y que tienen como propósito evitar la materialización del riesgo.

ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

- Contexto estratégico: Determinar los factores externos e internos del riesgo.

- Identificación: identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- Análisis: Calificación y evaluación del riesgo inherente.
- Valoración: identificación y evaluación de controles; incluye la determinación del riesgo residual.
- Manejo: Determinar, si es necesario, acciones para el fortalecimiento de los controles.
- Seguimiento: Evaluación integral de los riesgos.

ANÁLISIS CONTEXTO ESTRATÉGICO

Definir el contexto estratégico contribuye al control de la institución frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la institución actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta primera etapa se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la institución; es la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las causas del riesgo.

DESARROLLO PRÁCTICO - CONTEXTO ESTRATÉGICO

Tomando como referente lo anterior, se debe atender y seguir las siguientes orientaciones:

- Cada responsable de proceso del Sistema Integrado de Gestión deberá identificar a los funcionarios que por su competencia pueden ser considerados claves dentro de cada una de las dependencias que participan en el proceso, serán factores de selección de estos, el conocimiento y nivel de toma de decisiones sobre el proceso.
- Los funcionarios seleccionados deberán ser convocados a una reunión inicial, en donde se presentará el propósito de esta actividad
- Se establecerán los factores internos y externos que afectan el proceso, para esto, se debe realizar una Matriz DOFA para identificación de riesgos.
- Para diligenciar la matriz DOFA, y como parte introductoria se deberá informar a los asistentes: la dependencia a la cual corresponde el proceso y el objetivo (se debe presentar indicando que se hace, cual es el mediante y la finalidad). Con esta información, se identificarán las posibles debilidades como:

- La administración, la estructura organizacional, las funciones y las responsabilidades.
- Las políticas, los objetivos y las estrategias que existen para su realización.
- Las capacidades, entendidas en términos de recursos y de conocimiento (humanos, de capital, tiempo, personas, infraestructura, procesos, sistemas y tecnologías).
- Los sistemas de información y comunicación, flujos de información formales e informales y toma de decisiones.
- Las normas, directrices y modelos adoptados por la institución.
- La forma y el alcance de las relaciones contractuales.

IDENTIFICACIÓN DE RIESGOS

Es la etapa que permite conocer los eventos potenciales, estén o no bajo el control de la institución pública, que ponen en riesgo el logro de su misión, estableciendo las causas y los efectos de su ocurrencia". Adicionalmente, en esta etapa también se realiza la clasificación del riesgo.

En este paso se identifican los riesgos institucionales y por procesos que la institución debe gestionar. Esta identificación se realiza con base en el Contexto Estratégico, definido en el paso anterior.

Componentes de la identificación del riesgo

a. Causas del riesgo

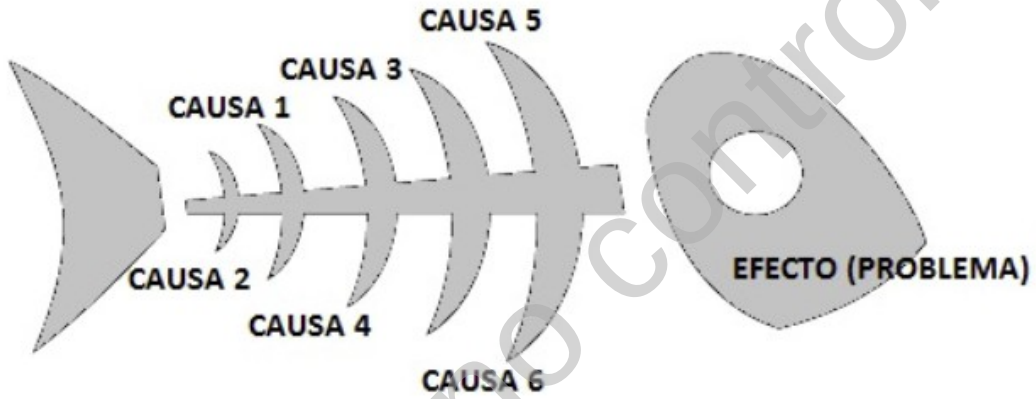
Son las causas, uno de los aspectos a eliminar o mitigar para que el riesgo no se materialice; esto se logra mediante la definición de controles efectivos. Para realizar el análisis de las causas existen varias técnicas que serán analizadas a continuación.

Lluvia de ideas: Usualmente se utiliza la técnica de lluvia de ideas para identificar todo aquello que puede ser considerado dentro del análisis de riesgos y para que esta sea eficaz, se debe considerar que:

1. Debe haber un moderador que tome nota y que organice las exposiciones de todos los participantes, indicando el tiempo que cada cual tiene para presentar sus ideas.
2. Es más importante la cantidad de ideas que la calidad de estas. Todas las ideas son valiosas para el proceso de recopilación de información.
3. No se deben calificar las ideas como buenas o malas, son simplemente puntos de vista que capitalizados pueden brindar alternativas no consideradas.
4. Es importante soportarse en las ideas de los otros. Es decir, agregar valor a las apreciaciones de otros o considerar situaciones a partir de las mismas.
5. El análisis de las ideas se debe realizar al final, por el moderador, quien las organizará y las expondrá a manera de resultado.

6. Todos deben participar de manera equitativa, es importante no fijar la atención en pocos participantes, ni mantenerse en la palabra sin dar la oportunidad a otro de expresar sus ideas.

Diagrama Causa-efecto (Espina de pescado): es un método que permite visualizar de manera estructurada todas las causas posibles del riesgo mediante el análisis desde los factores generadores de riesgo.



b. Consecuencias

Son los efectos que se generan o pueden generarse con la materialización del riesgo sobre los objetivos de los procesos y de la institución; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Se deben determinar las consecuencias del riesgo en escala ascendente; definiendo cual podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado.

c. Clasificación de los riesgos

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo.

Definición de clases de riesgo

Estratégico: Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la institución por parte de la alta gerencia.

Operativo: Relacionados con el funcionamiento y operatividad de los sistemas de información de la institución: definición de procesos, estructura de la institución, articulación entre dependencias.

Financieros: Relacionados con el manejo de los recursos de la institución: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.

Cumplimiento: Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.

Tecnología: Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión.

Imagen: Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la institución.

ESTRUCTURA ADECUADA DE LA IDENTIFICACIÓN DEL RIESGO

La identificación del riesgo no se puede realizar de manera fragmentada; debe existir una relación total entre las causas identificadas, el riesgo y las consecuencias que podrían presentarse producto de la materialización; para evitar confusiones y definir articuladamente todos los componentes de la identificación del riesgo se establece un método apropiado que consiste en el uso del lenguaje del riesgo para una identificación estructurada en tres partes:

Debido a	**Podría ocurrir**	**Lo que podría generar**
Una o más causa	Riesgo	Uno o más consecuencia

ANÁLISIS DE RIESGOS

El análisis del riesgo busca establecer la probabilidad de ocurrencia de este y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos para tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Institución la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

Calificación del riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

Escala para calificar la probabilidad del riesgo		
Nivel	Concepto	Frecuencia
Raro	El evento puede ocurrir solo en	No se ha presentado en

	circunstancias excepcionales.	los últimos 5 años.
Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
Moderado	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi certeza	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Escala para calificar el impacto del riesgo							
Tipos de efecto o impacto		**a) Estratégico**	**b) Operativo**	**c) Financieros**	**d) Cumplimiento**	**e) Tecnología**	**f) Imagen**
INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la institución	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida financiera no afecta la operación normal de la institución	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida financiera afecta algunos servicios administrativos de la institución	Genera investigaciones disciplinarias, y/o fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
MODERADO	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la Institución	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida financiera afecta considerablemente la prestación del servicio	Genera interrupciones en la prestación del bien o servicio	Afecta varios procesos de la institución	Afecta a todos los servidores de la institución
MAYOR	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas de la institución	Genera intermitencia en el servicio	La pérdida financiera afecta considerablemente el presupuesto de la institución	Genera sanciones	Afecta a toda la institución	Afecta el sector
CATASTRÓFICO	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la institución	Afecta al presupuesto de otras instituciones o a de la del departamento	Genera cierre definitivo de la institución	Afecta al Departamento	Afecta al Departamento, Gobierno, Todos los usuarios de la institución

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (Estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo

con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

PROBABILIDAD	**IMPACTO**				
	Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Moderado	B	M	A	A	E
Probable	M	A	A	E	E
Casi certeza	M	A	E	E	E

Color	**Zona de riesgo**
B	Zona de riesgo baja
M	Zona de riesgo moderada
A	Zona de riesgo alta
E	Zona de riesgo extrema

Con la evaluación del riesgo, previa a la formulación de controles se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina evaluación del riesgo inherente.

Valoración de los riesgos

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

Identificación de controles

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la institución, en la medida

en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan las características mínimas que se deben tener en cuenta para la definición de los controles:

Característica	**Descripción**
Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo
Realizables	Se deben definir controles que la institución o el proceso esté en capacidad de llevar a cabo
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad
Periódicos	Tienen frecuencia de aplicación en el tiempo
Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo
Asignables	tienen responsables definidos para su ejecución

En esta etapa se deben describir todos los controles, existentes y por definir, deben estar orientados a atacar las causas y/o consecuencias (mitigar y/o eliminar) del

riesgo. Una vez se hayan identificado y descrito los controles se debe determinar la clase del control; un control puede ser de tipo preventivo o correctivo.

Evaluación de los controles

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad de la siguiente manera:

¿El control está documentado, incluye el responsable y la frecuencia de aplicación?	¿El control se está aplicando?	¿El control es efectivo (¿sirve o cumple su función?

La evaluación se debe aplicar a cada control definido para el riesgo, determinando si se cumple o no el factor, según corresponda.

Manejo de riesgos

Una vez determinada la zona donde está ubicado el riesgo, y dependiendo de las opciones de manejo, se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados. Las acciones que se definan para el manejo del riesgo deben contemplar:

- Corregir las fallas identificadas en los controles según la evaluación realizada a cada uno.
- Reforzar o fortalecer los controles existentes.

Si la evaluación del riesgo residual, lo ubica en la zona baja no se deben formular acciones de manejo, el manejo estará únicamente enfocado en garantizar que los controles previamente establecidos operan de manera adecuada. Los riesgos ubicados en las zonas moderada, alta o extrema exigen realizar acciones que fortalezcan los puntos débiles identificados en la evaluación de los controles.

Seguimiento de riesgos

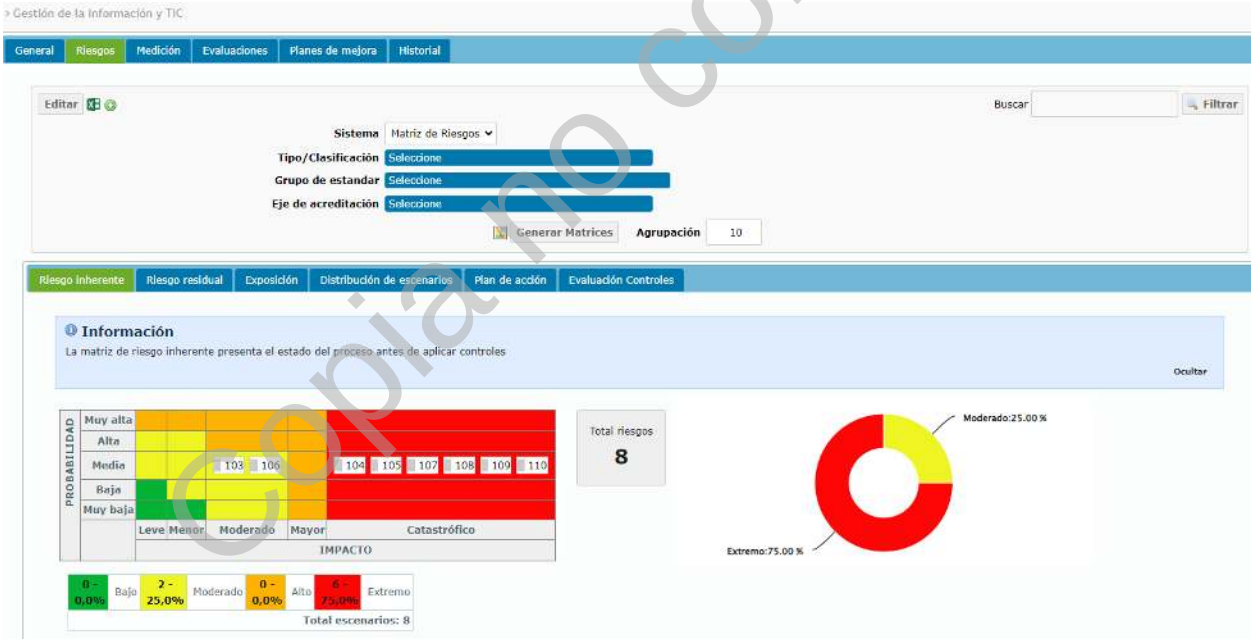
Cada cuatro meses Control Interno realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
- Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.
- • Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la institución.

MAPA DE RIESGOS

Una vez se tenga toda la información relacionada en los numerales anteriores, se documentará la información en el formato Mapa de riesgos de la Institución.

Los responsables de procesos y sus equipos de trabajo deben garantizar que la información de los riesgos sea adecuada, coherente, pertinente y vigente. Cualquier ajuste que se deba realizar de esta información, debe ser informado. La herramienta donde se pueden visualizar los riesgos es Almera.



Fuente: Sistema de Gestión Integral Almera

Su tratamiento se aplica en plataforma.

PROCESO DE BUENAS PRACTICAS DE SEGURIDAD PARA MANEJO TRANSACCIONAL

a) Riesgos originados por incidentes de delito informático

Los riesgos originados por incidentes de delito informático pueden ser variados y tienen el potencial de afectar a las entidades públicas. Es por esto tan importante conocerlos e implementar medidas de seguridad robustas, educando al personal sobre prácticas de seguridad y estableciendo prácticas regulares de seguridad, para mitigar estos riesgos.

A continuación, una descripción de las principales modalidades de delito informático identificados:

1. Fraude electrónico: Es la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, donde se influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema. (Referencia Código Penal, Ley N° 1273 de 2009).

2. Phishing: Fraude tradicionalmente cometido a través de internet, que pretende conseguir datos confidenciales de usuarios, tales como identificación o claves de acceso a cuentas de diversos sistemas. Una variante del Phishing, pero por teléfono se conoce como Vishing.

3. Pharming: Modalidad de estafa online (en línea) mediante la manipulación de los servidores DNS (Domine Name Server) para re-direccionar el nombre de un dominio, visitado habitualmente por el usuario, a una página web idéntica a la original, que ha sido creada para obtener datos confidenciales de usuarios como identificación o claves de acceso a cuentas de diversos sistemas.

4. Phreaking: Hacking orientado a la telefonía y estrechamente vinculado con la electrónica aplicada a los sistemas telefónicos.

5. Humanware: El factor humano que interviene en un sistema. Se refiere a las personas involucradas como usuarios, desarrolladores de aplicaciones, administradores, operadores, entre otros.

b) Buenas prácticas de Entidades Públicas en el componente de Tecnología Seguridad y Ciberseguridad de la Información:

Con el fin de mitigar la exposición a los riesgos derivados de las modalidades de delito informático mencionados, presentamos un compendio de buenas prácticas para Entidades Públicas.

1. La seguridad de la información debe acompañarse de medidas complementarias, tanto en seguridad física como en estandarización de procesos, siguiendo un modelo de tipificación de los riesgos, asociado al modelo de madurez en seguridad de la información.

2. Implementar seguridad lógica y física en los equipos donde se realizan los giros de tesorería.

3. Protección física de la CPU de pagos y de su cableado para evitar cualquier manipulación de Hardware.

4. Licenciamiento del sistema operativo con estándares de seguridad.

5. Des-habilitación de puertos USB y unidades de CD/DVD.

6. IP fija registrada en el portal bancario, lo cual no permite realizar transacciones desde otro lugar.

7. Políticas de seguridad Active Directory desde el servidor principal.

8. Restricciones de Páginas de Correo, Redes Sociales, Generación de Historial de navegación, Archivos Temporales en los puntos de acceso a los portales bancarios.

9. Acceso a portales bancarios restringidos a los horarios semanales laborales. Lunes a Viernes de 8:00 am a 6:00 pm.

10. Cifrado de Archivos del sistema para impedir que terceros los puedan visualizar por fuera de la maquina principal.

11. Autenticación del usuario vía contraseña de Windows y su posterior Login al dominio del portal bancario con usuario y contraseña respectivos (token).

12. Empleo de herramientas de antivirus, antimalware, entre otras que identifiquen comportamientos inusuales en el equipo.

13. Conexiones VPN seguras para transferencia de archivos y ordenes de transacciones de cara a los portales bancarios.

14. Cambios dinámicos y periódicos de contraseñas seguras.

15. Controles de acceso de celulares a las áreas de Tesorería.

16. Sistemas de monitoreo y grabación de las zonas transaccionales.

17. Implementación de políticas, procesos y procedimientos para estandarizar la gestión de la tesorería.

18. La estandarización de los canales transaccionales, a través de soluciones bancarias que cumplan con los lineamientos legales y garanticen la trazabilidad de la información y el manejo seguro de los recursos públicos.

19. La implementación de procesos que permiten el manejo adecuado de la información pública en lo relacionado con el cumplimiento de los protocolos de integridad y reserva de datos y las políticas de Habeas Data.

20. Hacer uso del portal transaccional, ingresando directamente a la página web dispuesta por la entidad, digitando completamente la dirección dentro del navegador y no mediante enlaces o accesos directos.

21. Hacer uso de la aplicación móvil que se encuentra registrada y disponible desde las tiendas oficiales, y no mediante archivos de instalación no autorizados.

22. No compartir sus credenciales y tokens, e implementar la configuración de contraseñas seguras.

23. Mantener actualizado el sistema operativo, el antivirus y las aplicaciones instaladas en los equipos.

24. Se recomienda no habilitar bluetooth y conexiones Wi-Fi en lugares desconocidos para realizar transacciones o consultas.

25. Evitar hacer descargas de enlaces compartidos y desconocidos.

26. Mostrar enmascarados los productos de los clientes como cuentas de ahorros, cuentas corrientes, tarjetas débito, tarjetas crédito y créditos.

27. Establecer campañas de sensibilización a los usuarios sobre el uso de la tecnología, protección al consumidor, buenas prácticas de seguridad y prevención de fraude

c) Algunos de los principales riesgos asociados a las Entidades Públicas:

Adicional a los incidentes de delito informático, las entidades públicas están expuestas a diferentes eventos de riesgo. Es importante que se implementen medidas de seguridad sólidas, que permitan la elaboración de evaluaciones de riesgos periódicas y el establecimiento de planes de respuesta a incidentes para mitigar estos riesgos y protejan los recursos públicos, la información sensible y los servicios esenciales que proporcionan a los ciudadanos.

A continuación, una descripción de los principales riesgos:

1. Fraude Interno: Se refiere a actividades fraudulentas o engañosas realizadas por personas dentro de la entidad, ya sea de manera actual o pasada. Este tipo de fraude puede involucrar a empleados, gerentes o incluso a personas en posiciones de liderazgo y confianza dentro de la entidad.

2. Riesgo Legal: Se refiere a la posibilidad de que la entidad o sus empleados se enfrenten a consecuencias negativas como resultado de acciones legales, incumplimientos de leyes, regulaciones o disputas legales. Este tipo de riesgo puede surgir de diversas áreas y situaciones, y su impacto puede variar desde multas financieras hasta daños en la reputación o incluso implicaciones penales para las personas o las entidades.

3. Fraude externo: Se refiere a actividades fraudulentas o engañosas llevadas a cabo por individuos o entidades externas a la entidad (individuos, grupos organizados o incluso otras entidades o empresas).

4. Fallas tecnológicas: Se genera por fallos en los sistemas de cómputo, en el hardware o en el software de la entidad.

5. Ejecución y gestión de procesos: Se refiere a la posibilidad de que los procedimientos y actividades administrativas no se lleven a cabo de manera eficiente, efectiva o conforme a las normativas establecidas. Típicamente se genera por un incorrecto procesamiento de las transacciones, o por un deficiente monitoreo y gestión de los presupuestos públicos.

d) Buenas prácticas de Entidades Públicas en el componente de seguridad de la información para el manejo de sus productos financieros:

1. Implementar procedimientos internos para los trámites de apertura, cancelación y/o cambio de firmas de cuentas bancarias necesarias para el manejo de los recursos propios y especiales, con el fin de mantener el adecuado registro, control y conciliación de las cuentas en los tiempos establecidos legalmente.

2. Implementar procedimientos internos para apertura y custodia de Títulos Valores con Entidades Financieras.

3. Implementar procedimientos internos para la custodia de chequeras de las cuentas corrientes dadas por las Entidades Financieras.

4. Utilizar canales electrónicos autorizados para efectuar los pagos a los beneficiarios finales (Contratistas, Proveedores y funcionarios de la entidad por

concepto de salarios y prestaciones sociales, descuentos de las nóminas, embargos judiciales, impuestos, servicios públicos y transferencias, Aportes de Salud y Pensión, entre otros, donde se le brinda el pago directo a la cuenta bancaria previamente definida y autorizada).

5. Utilizar medios y canales electrónicos para la reducción de los costos de manejo del efectivo y de chequeras (ahorro de tiempo y mayor seguridad), mejorando la transparencia en las transacciones y el control de los flujos de fondos.

6. Implementar un sistema de administración de cuentas corrientes y cuentas de ahorro, discriminadas por cada uno de los conceptos que se tienen (recursos de libre destinación, recursos de destinación específica, recursos especiales, recursos del crédito, recursos de dividendos).

7. Implementar las medidas de control y seguridad internos con el fin de garantizar el acceso a los canales transaccionales, emisión de órdenes de pago, traslados y demás operaciones bancarias, únicamente al funcionario facultado por los manuales de funciones internos de la Entidad.

8. Implementar estándares de calidad, seguridad e idoneidad para la contratación de terceros encargados de la revisión y mantenimiento de equipos e instalación de software o hardware que soportan la transaccionalidad con las entidades financieras.

9. Definir las competencias, roles y responsabilidades mínimos que debe cumplir el funcionario público designado por la entidad para el manejo de las transacciones, por los diferentes canales dispuestos por la Entidad Financiera.

10. Garantizar que la totalidad de los pagos que realicen las entidades públicas se realicen con pago a cuenta.

11. Sobre los procesos de apertura de cuentas, actualización de información y de nuevos administradores, se debe crear una capa de control en las plataformas de Tecnologías de Información TI, para que el intercambio de información se realice garantizando los principios de seguridad de la información.

12. Adoptar protocolos que mitiguen el lavado de activos, en línea con las políticas de SARLAFT (Sistema de Administración del Riesgo de Lavado de Activos y Financiación al Terrorismo).

13. Adoptar protocolos para la mitigación de riesgos relacionados con malas prácticas como sobornos y condicionamientos contractuales (ABAC).

10. SEGUIMIENTO Y EVALUACIÓN

Nombre del Indicador	Fórmula
Tratamiento de eventos relacionados en marco de seguridad y privacidad de la información Definición: El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.	(Número de anomalías cerradas / Número total de anomalías encontradas) * 100

11. ANEXOS

No aplica

12. DOCUMENTOS RELACIONADOS

GTI-PL-005 Plan de Seguridad y Privacidad de la información

GTI-M-002 Políticas y estándares de seguridad informática para los usuarios

CONTROL DE CAMBIOS Y REVISIONES				
Revisión	**Fecha**	**Versión Anterior**	**Versión Actual**	**Cambio Realizado**
01	11/01/2024	01	02	Se actualiza formato del plan de tratamiento de riesgos de seguridad de la información 2024 - 2027
02	31/12/2024	02	03	Se adiciona buenas prácticas de seguridad para la parte bancaria

Elaboró:	Revisó:	Aprobó:
Marneilde Londoño Ricaurte Líder de Gestión de Tecnologías y la Información	Marneilde Londoño Ricaurte Líder de Gestión de Tecnologías y la Información	Natali Mosquera Narváez Gerente General