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

PTRSI

2024

2027

Secretaría General

Equipo de Sistemas

SGI

1 OBJETIVO

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) a los que la Corporación Autónoma Regional del Atlántico – CRA pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.
- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.
- Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), de acuerdo con los contextos establecidos por el MinTIC.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de la CRA.

2 ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), que permita integrar en los procesos de la CRA, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Adicionalmente dar los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la entidad.
El Plan de Tratamiento de Riesgo tendrá en cuenta todos los riesgos en especial los que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por el Sistema de Gestión Integrado, teniendo en cuenta que aquellos que se encuentren en niveles inferiores serán aceptados por la Entidad.

3 MARCO REFERENCIAL

3.1 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE LA CRA

La corporación Autónoma Regional del Atlántico CRA está comprometido con el fortalecimiento de la cultura de la prevención. Por lo tanto, dentro del Sistema de Gestión Integrado de la Entidad, se identifican y se gestionan los riesgos que puedan afectar el cumplimiento de la ley, la misión, los objetivos estratégicos, el manejo eficiente y transparente de los recursos y la satisfacción de los grupos de interés.

El ámbito de aplicación de la presente Política de Administración del Riesgo abarca todos los procesos de la Corporación Autónoma Regional del Atlántico y es aplicable en las etapas de identificación,

valoración, monitoreo y seguimiento tanto de los riesgos asociados a la gestión como los asociados a corrupción.

La Alta Dirección establece los lineamientos y criterios metodológicos, con el fin de minimizar sus efectos adversos, así como orientar la toma de decisiones en la formulación de acciones efectivas tendientes a garantizar la continuidad de la gestión institucional, de tal manera que la gestión del riesgo se constituya en una herramienta de mejoramiento continuo.

En representación de la Alta Dirección, la Secretaría General a través de la Coordinación del Sistema Integrado, y con apoyo de la Oficina de Control Interno, se encargará de liderar el proceso de administración y/o gestión del riesgo dentro de la corporación.

La Corporación adopta la estructura conceptual para la administración de riesgos establecida en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas en su versión vigente, dentro de la cual brindan los criterios pertinentes para identificar y valorar los riesgos de manera consistente, determinar sus consecuencias y desarrollar acciones de mitigación que permitan mantenerlos en un nivel aceptable.

3.2 TÉRMINOS Y DEFINICIONES

- Aceptar el riesgo: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
- Administración de Riesgos: Conjunto de elementos de control que, al interrelacionarse, permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.
- Análisis de riesgo: Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la corporación para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.
- Contexto: Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.
- Contexto externo: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad.
- Contexto interno: Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.
- Controles para el riesgo: Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad o situación no deseable potencial o detectada.

- Evaluación del control: Elemento de control que, basado en un conjunto de mecanismos de verificación y evaluación, determina la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.
- Evaluación del riesgo: Proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
- Evento: Incidente o situación que ocurre en un lugar determinado durante un período de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.
- Identificación del riesgo: Elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.
- Impacto: Consecuencias o daños que puede ocasionar a la corporación la materialización del riesgo, expresado cualitativa o cuantitativamente, siendo una pérdida, lesión, desventaja o ganancia. Puede haber un rango de posibles resultados asociados con un evento.
- Gestión del riesgo fiscal: Son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial)
- Monitorear: Comprobar, Supervisar, observar, o registrar la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles cambios.
- Pérdida: Consecuencia negativa que trae consigo un evento.
- Probabilidad: Grado en el cual es probable que ocurra de un evento, este se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir.
- Proceso de administración de riesgo: Aplicación sistemática de políticas, procedimientos y prácticas de administración a las diferentes etapas de la administración del riesgo.
- Reducción del riesgo: Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia.
- Riesgo: Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.
- Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Riesgo fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- 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: Es aquel al que se enfrenta la corporación en ausencia de acciones o controles para modificar su probabilidad o impacto.

- Riesgo residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo o aplicación de los controles.
- Sistema de Administración de Riesgo: conjunto de elementos del direccionamiento estratégico de una entidad concerniente a la Administración del Riesgo.

3.3 METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

Para determinar la metodología para la administración del riesgo adoptada por la corporación, se toma como referencia la establecida por el Departamento Administrativo de la Función Pública, la cual estipula una serie de etapas que se deben desarrollar para realizar una adecuada gestión del riesgo. Para facilitar su aplicación, la corporación ha diseñado una herramienta (mapa de riesgos) que permite realizar la identificación, valoración, el monitoreo y seguimiento a los riesgos.

3.3.1 IDENTIFICACIÓN DEL RIESGO

En esta etapa se deben establecer los eventos o riesgos, las clases o tipos de riesgos, las fuentes que generan el riesgo, sus causas y sus consecuencias.

Para el análisis, los responsables de los procesos junto con su equipo de trabajo realizan la identificación de los riesgos que puedan afectar el desempeño de los procesos considerando:

- El contexto interno y externo (Ver documento *Análisis del Contexto Interno y Externo de la Organización*).
- Las necesidades y expectativas de las partes interesadas (Ver documento *Análisis de partes interesadas*)
- Cuestiones o situaciones de riesgos que afecten el cumplimiento de sus funciones y objetivos institucionales trazados en las líneas estratégicas.

3.3.1.1 REGISTRO DEL RIESGO

Una vez identificados los riesgos, es preciso registrar dentro del formato *Mapa de riesgos* la descripción de cada evento inductor (Riesgo), el tipo de riesgo, fuentes, causas y sus consecuencias potenciales en su estado natural, es decir, sin considerar medidas de mitigación. De esta forma se determina aquéllos que, en caso de ocurrir, pueden significar una pérdida o daño. Estos aspectos se registran en las primeras columnas de la estructura del mapa diseñado para la corporación.

También se puede establecer un inductor de riesgo que tenga relación con varias situaciones consideras significativas.

Por otro lado, es importante destacar que un evento de riesgo puede afectar a más de un área, y, por tanto, dar lugar a múltiples consecuencias, las que a su vez generan más de una actividad de control,

así mismo se pueden registrar en un mismo inductor varias fuentes, causas y tipos de riesgos según clasificación establecida en la presente guía. Entre las clases de riesgos que pueden presentarse están:

- **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
- **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- **Riesgos Operativos:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.
- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
- **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
- **Riesgos de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

3.3.2 ANÁLISIS DEL RIESGO

El análisis del riesgo consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto que puede causar la materialización del riesgo, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE) y la zona de riesgo final (RIESGO RESIDUAL). Esta etapa está compuesta por los procesos Análisis del Riesgo Inherente y Valoración del Riesgo Residual.

3.3.2.1 ANÁLISIS DEL RIESGO INEHERENTE

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE), para ello se deben ejecutar los siguientes paso claves:

3.3.2.1.1 DETERMINAR LA PROBABILIDAD

Se entiende por Probabilidad, la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Factibilidad.

- Bajo el criterio de Frecuencia se analizan el número de eventos en un período determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.
- Bajo el criterio de Factibilidad se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Bajo el criterio de probabilidad, el líder del proceso debe medir el riesgo tomando como referencia las siguientes especificaciones registradas en la tabla No. 01, la cual es adoptada por la corporación para el manejo de sus riesgos y una vez determinado el nivel que mide el inductor evaluado, se registra el número que lo identifica en el mapa diseñado.

Tabla No. 01.

Probabilidad			
Descriptor	**Nivel**	**Descripción**	**Frecuencia**
Casi Seguro	5	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año
Probable	4	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
Posible	3	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
Improbable	2	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
Rara vez	1	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

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

3.3.2.1.2 DETERMINAR EL IMPACTO O CONSECUENCIA

Por Impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo. Se tienen en cuenta las consecuencias potenciales establecidas en la etapa de Identificación del riesgo.

Para su determinación se utiliza la tabla No. 02, la cual registra los niveles de impactos establecida como política por la corporación, en la que se establecen el impacto desde el punto de vista cuantitativo como cualitativamente. Cada nivel diseñado para calificar de impacto está formado por varias características que distinguen los cinco niveles que lo constituyen.

Para determinar el nivel del impacto, el líder del proceso debe identificar y seleccionar por lo menos unas de las características allí descritas que refleja la consecuencia de la activación de inductor de

riesgo, ya sea cualitativa y/o cuantitativamente, identificar a qué nivel pertenece y registrarlo en la columna de Impacto del evento inductor de riesgo que está siendo evaluado.

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles **"moderado"**, **"mayor"** y **"catastrófico"**, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos. Para su determinación se utiliza la tabla No. 03, la cual establece los criterios para estipular el nivel de impacto.

Tabla N° 2.

Impacto (Consecuencias)			
Descriptor	**Nivel**	**Impacto (consecuencias) Cuantitativo**	**Impacto (consecuencias) Cualitativo**
Catastrófico	5	»Impacto que afecte la ejecución presupuestal en un valor ≥50% »Pérdida de cobertura en la prestación de los servicios de la entidad ≥50% »Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% »Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad	»Interrupción de las operaciones de la Entidad por más de cinco (5) días. »Intervención por parte de un ente de control u otro ente regulador. »Pérdida de Información crítica para la entidad que no se puede recuperar. »Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. »Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados
Mayor	4	»Impacto que afecte la ejecución presupuestal en un valor ≥20% »Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. »Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% »Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	»Interrupción de las operaciones de la Entidad por más de dos (2) días. »Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.. »Sanción por parte del ente de control u otro ente regulador. » Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. » Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos
Moderado	3	»Impacto que afecte la ejecución presupuestal en un valor ≥5% »Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. »Pago de indemnizaciones a terceros por	»Interrupción de las operaciones de la Entidad por un (1) día. »Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de

Impacto (Consecuencias)			
Descriptor	**Nivel**	**Impacto (consecuencias) Cuantitativo**	**Impacto (consecuencias) Cualitativo**
		acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% »Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad	largo alcance para la entidad. »Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. »Reproceso de actividades y aumento de carga operativa. »Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. »Investigaciones penales, fiscales o disciplinarias
Menor	2	»Impacto que afecte la ejecución presupuestal en un valor ≤1% »Pérdida de cobertura en la prestación de los servicios de la entidad ≤5%. »Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≤1% »Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤1%del presupuesto general de la entidad	»Interrupción de las operaciones de la Entidad por algunas horas. »Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. »Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos
Insignificante	1	»Impacto que afecte la ejecución presupuestal en un valor ≤0,5% »Pérdida de cobertura en la prestación de los servicios de la entidad ≤1%. »Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≤0,5% »Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤0,5%del presupuesto general de la entidad	»No hay interrupción de las operaciones de la entidad. »No se generan sanciones económicas o administrativas. »No se afecta la imagen institucional de forma significativa

3.3.2.1.3 ESTIMAR EL NIVEL DEL RIESGO INHERENTE

Para estimar el nivel de riesgo inicial, los valores determinados para la probabilidad y el impacto se cruzan en la siguiente Matriz de Evaluación de Riesgo (denominado sistema de semáforo), con el fin de determinar la zona de riesgo en la cual se ubica el evento inductor identificado, registrando dicha zona en la celda respectiva del mapa.

Este primer análisis del riesgo se denomina Riesgo Inherente y se define como aquél al que se enfrenta la corporación en ausencia de acciones o controles para modificar su probabilidad o impacto.

MATRIZ DE EVALUACIÓN DE RIESGO

Zonas de Riesgos						
5 Casi seguro	Probabilidad de Ocurrencia	Zona de Riesgo Alta	Zona de Riesgo Alta	Zona de Riesgo Extrema	Zona de Riesgo Extrema	Zona de Riesgo Extrema
4 Probable		Zona de Riesgo Moderada	Zona de Riesgo Alta	Zona de Riesgo Alta	Zona de Riesgo Extrema	Zona de Riesgo Extrema
3 Posible		Zona de Riesgo Baja	Zona de Riesgo Moderada	Zona de Riesgo Alta	Zona de Riesgo Extrema	Zona de Riesgo Extrema
2 Improbable		Zona de Riesgo Baja	Zona de Riesgo Baja	Zona de Riesgo Moderada	Zona de Riesgo Alta	Zona de Riesgo Extrema
1 Rara vez		Zona de Riesgo Baja	Zona de Riesgo Baja	Zona de Riesgo Moderada	Zona de Riesgo Alta	Zona de Riesgo Alta
Riesgo Inherente y Residual		1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
		Impacto				

3.3.2.2 VALORACIÓN DEL RIESGO RESIDUAL

Para la valoración del riesgo residual es necesaria la identificación y registro de las acciones de control de cada uno de los riesgos identificados, para que posteriormente se valore el nivel de control que realmente tienen estas acciones sobre el riesgo. Estas acciones de control deben establecerse en la columna *Controles para el riesgo* del *Mapa de riesgos*. Para la determinación de los controles del riesgo se recomienda considerar las siguientes variables:

- Identificar acciones que actualmente pueden controlar el riesgo.
- Qué busca hacer el control (objetivo).
- Cómo se lleva a cabo el control (procedimiento).
- Cuando se realiza el control (periodicidad).
- Evidencia de la ejecución del control.
- Quién lleva a cabo el control (responsable).
- Tipo de control (manual o automático).

Posteriormente es necesario valorar los controles establecidos, lo cual implica:

a. Determinar su naturaleza: Si se trata de un control preventivo o correctivo.

b. Determinar si los controles están documentados, lo cual determinará las evidencias que van a respaldar la ejecución de este.
c. Determinar si los controles se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo.

Para realizar dicha evaluación, a continuación, se muestra una tabla ilustrativa No. 04, con el fin de orientar el análisis objetivo de los controles y de este modo poder determinar el riesgo residual.

Las calificaciones planteadas para cada aspecto deben ser usadas tal como están expresadas y aplicar el valor asignado a cada aspecto si responde SI; cero (0) si responde NO. Es importante que no se asignen valores intermedios para evitar subjetividad en el análisis.

El responsable del proceso, teniendo en cuenta el inductor de riesgo que es objeto de evaluación, responde cada una de las preguntas descritas en la tabla No. 04 y dependiendo a su respuesta (si / no), va tomando los valores asignados a cada aspecto y al finalizar los suma. El resultado obtenido, se ubica en qué Rango de Calificación de los Controles se encuentra, según la tabla No. 05, el cual va a indicar el número de cuadrantes a disminuir en la Matriz de Evaluación de Riesgo, que dependiendo si el control afecta la probabilidad el número de cuadrantes a disminuir avanza hacia abajo de la matriz y si el control afecta el impacto el número de cuadrantes a disminuir se desplaza hacia la izquierda de la matriz, en este sentido se va a obtener la zona de riesgo final, la cual es registrada en la columna de Riesgo Residual del mapa de riesgo.

No siempre en este proceso, aunque se ejecuten los controles, el riesgo va a disminuir, en ocasiones y dependiendo del resultado obtenido en la evaluación de los controles el riesgo se va a mantener en la misma zona.

Tabla No. 04.

Analisis y Evaluación de los Controles

Sc.	Criterios para la Evaluación (Describa el control determinado para el riesgo identificado)	Evaluación	
		Si	No
A	¿El control previene la materialización del riesgo (afecta probabilidad) ¿El control permite enfrentar la situación en caso de materialización (afecta impacto)?	NA	NA
B	¿Existen manuales, instructivos o procedimientos para el manejo del control?	15	0
C	¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5	0
D	¿El control es automático? (Sistemas o Software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros).	15	0
E	¿El control es manual? (Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros)	10	0
F	¿La frecuencia de ejecución del control y seguimiento es adecuada?	15	0
G	¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10	0
H	¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30	0
	Total	100	0

Tabla No. 05.

Rangos de Calificación de los Controles	Dependiendo si el control afecta probabilidad o impacto desplaza en la matriz de evaluación del riesgo así: EN PROBABILIDAD AVANZA HACIA ABAJO EN IMPACTO AVANZA HACIA LA IZQUIERDA
	Cuadrantes a disminuir
Entre 0-50	0
Entre 51-75	1
Entre 76-100	2

3.3.3 ACCIONES EN CASO DE MATERIALIZACIÓN DEL RIESGO

A pesar de establecer e implementar controles para prevenir la materialización del riesgo, se tiene cierta posibilidad de que esta pueda suceder, por esta razón, es necesario definir acciones en caso de materialización del riesgo que busquen mitigar o contener las consecuencias negativas del evento. Estas acciones deben quedar registradas en la columna *Acciones en caso de materialización* del *Mapa de riesgos.*

En caso de materialización del riesgo, el personal responsable de estas acciones debe implementarlas de acuerdo con lo establecido en el *Mapa de riesgos* asegurando en todo momento las evidencias y registros que den soporte.

Es recomendable que posterior a un evento de materialización del riesgo, el personal responsable de gestionar los riesgos identificados realice un análisis de la situación que le permita determinar en que fallaron los controles del riesgo y como fue la eficacia de las acciones establecidas en caso de materialización. De este análisis puede identificarse, entre otros elementos, lo siguiente:

- Deficiencias en el diseño o implementación de los controles, tanto en los controles del riesgo como en las acciones en caso de materialización.
- Necesidad de diseñar y establecer nuevos controles.
- Necesidad de documentar acciones que actualmente se implementan para controlar los riesgos.
- Necesidad de implementar cambios dentro de los procesos de la entidad.

Estas cuestiones identificadas deben gestionarse de acuerdo con los procedimientos establecidos dentro del Sistema de Gestión Integral de la Entidad, por ejemplo:

- En caso de requerir un cambio en los procesos, se debe proceder de acuerdo con el procedimiento de Gestión del Cambio del SGI.
- Si se presentan desviaciones en la implementación de los controles se sugiere la definición de una acción correctiva de acuerdo con el procedimiento para gestionar las acciones correctivas establecido en el SGI.

Las acciones tomadas posterior al análisis de la materialización del riesgo deben ser soportadas y evidenciadas adecuadamente.

3.3.4 ARTICULACIÓN CON EL SISTEMA DE GESTIÓN Y OTROS

Teniendo en cuenta que los procesos operan como un sistema, se debe determinar y registrar con qué indicador establecido en el proceso guarda relación el inductor de riesgo identificado y en el caso de no existir, colocar no aplica (N.A.) o contemplar la posibilidad de su creación.

Por otra parte, se deben registrar los documentos establecidos en el sistema de gestión de la corporación que guardan relación con el inductor de riesgo identificado, en el caso de existir, en caso contrario, colocar no aplica (N.A.)

3.3.5 ELABORACIÓN DEL MAPA DE RIESGO

El mapa de riesgos es una representación gráfica y final de la probabilidad e impacto de uno o más riesgos identificados por la alta dirección y responsables de cada proceso de la corporación como factores que afectan o pueden incidir negativamente en el logro de los objetivos.

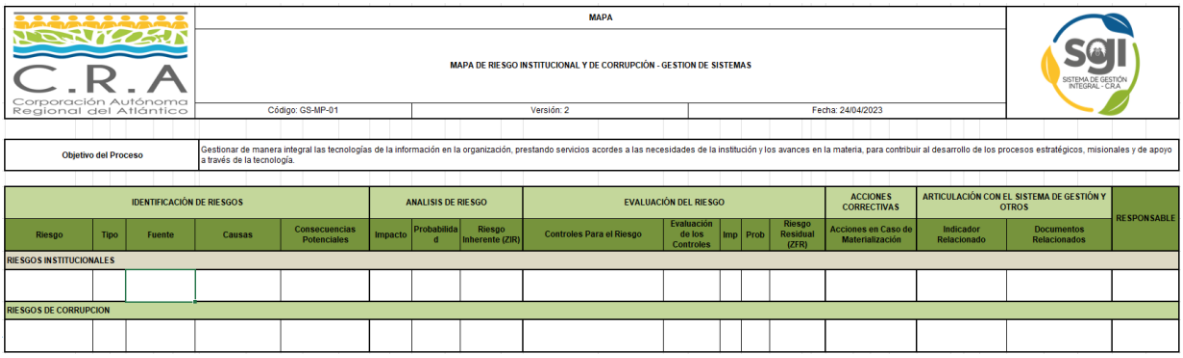
Como producto final del proceso de identificación y valoración de los riesgos se obtiene el Mapa Institucional de Riesgos, el cual contiene los riesgos identificados para cada uno de los procesos, los cuales pueden afectar el logro de sus objetivos.

3.3.6 ALINEACIÓN CON LAS POLÍTICAS DE LUCHA CONTRA LA CORRUPCIÓN Y DE EFICIENCIA ADMINISTRATIVA

En aras de disminuir los niveles de corrupción en todos los ámbitos. La Secretaría de Transparencia de la Presidencia de la República en cumplimiento del artículo 73 de la Ley 1474 de 2011, diseñó una metodología para que todas las entidades determinen su Plan Anticorrupción y de Atención al ciudadano, la cual contempla como uno de sus componentes el levantamiento de los mapas de riesgos asociados a posibles hechos de corrupción.

Entendiendo que los riesgos de corrupción se convierten en una tipología de riesgos que debe ser controlada por la corporación, éstos deben incorporarse en el mapa de riesgos del proceso o institucional, sobre el cual se han identificado, de modo tal que el responsable o líder del mismo pueda realizar el seguimiento correspondiente, en conjunto con los riesgos de gestión propios del proceso, evitando que se generen mapas separados de gestión y de corrupción, lo que promueve que el responsable tenga una mirada integral de todos los riesgos que pueden llegar a afectar el desarrollo de su proceso.

En virtud de lo anterior, en la Corporación Autónoma Regional del Atlántico C.R.A., se diseñó un formato de mapa de riesgo, denominado en el sistema de calidad con el nombre Mapa de Riesgo Institucional y de Corrupción bajo el Código: XX-MP-01, en donde se incorporan los dos tipos de riesgos, el cual se puede observar en la imagen siguiente:



	MAPA	
C.R.A Corporación Autónoma Regional del Atlántico	MAPA DE RIESGO INSTITUCIONAL Y DE CORRUPCIÓN - GESTION DE SISTEMAS	SGI SISTEMA DE GESTIÓN INTEGRAL - CRA
	Código: GS-MP-01 / Versión: 2 / Fecha: 24/04/2023	

Objetivo del Proceso	Gestionar de manera integral las tecnologías de la información en la organización, prestando servicios acordes a las necesidades de la institución y los avances en la materia, para contribuir al desarrollo de los procesos estratégicos, misionales y de apoyo a través de la tecnología.

IDENTIFICACIÓN DE RIESGOS					ANALISIS DE RIESGO			EVALUACIÓN DEL RIESGO					ACCIONES CORRECTIVAS	ARTICULACIÓN CON EL SISTEMA DE GESTIÓN Y OTROS		RESPONSABLE
Riesgo	Tipo	Fuente	Causas	Consecuencias Potenciales	Impacto	Probabilidad	Riesgo Inherente (ZIR)	Controles Para el Riesgo	Evaluación de los Controles	Imp	Prob	Riesgo Residual (ZFR)	Acciones en Caso de Materialización	Indicador Relacionado	Documentos Relacionados	
RIESGOS INSTITUCIONALES																
RIESGOS DE CORRUPCION																

A demás de la presente guía y en aras de ser más didáctico el proceso de diligenciamiento del mapa de riesgo, al final de dicho formato, se encuentran descritas las pautas establecidas en la presente guía que servirá de apoyo en el momento de su elaboración.

3.3.7 SEGUIMIENTO, REVISIÓN Y ACTUALIZACIÓN DE LOS MAPAS DE RIESGO

3.3.7.1 SEGUIMIENTO DE LOS RIESGOS

Los mecanismos de seguimiento a los riesgos de cada proceso deben asegurar que las acciones establecidas en los mapas de riesgos se están implementado adecuadamente.

El seguimiento de los riesgos tanto institucionales como de corrupción, los cuales se encuentran incorporados en el mismo *Mapa de riesgos*, en primer lugar, es responsabilidad de los líderes de los procesos, quienes son los encargados de realizar las acciones asociadas a los controles establecidos para cada uno de los riesgos identificados en su proceso.

Durante la aplicación de las acciones de seguimiento cada líder de proceso debe mantener la documentación respectiva de todas las actividades realizadas, para garantizar de forma razonable que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplirán.

3.3.7.2 REVISIÓN DE LOS MAPAS DE RIESGO

La Coordinación del Sistema de Gestión Integral de la Corporación, en representación de la Secretaria General, en el marco de la *Revisión por Dirección* implementará la revisión a los mapas de riesgos de los procesos, con el fin de verificar la aplicación de los controles existentes que mitigan los inductores de riesgos identificados.

De igual forma, en el marco del *Plan Anual de Auditoría* y la implementación de las auditorías internas de control, la oficina de Control Interno de la Corporación realiza revisión a los riesgos que han sido consolidados en el *Mapa de riesgo* de los procesos, con el fin de evaluar el diseño, efectividad e idoneidad de los controles y determinar si se han materializado o no.

3.3.7.3 ACTUALIZACIÓN DE LOS MAPAS DE RIESGO

Los mapas de riesgos establecidos en cada proceso están sujetos a cambios en pro de la mejora continua, los cuales, deberán ser solicitados por los líderes de proceso y consignarse en el control de cambio del *Mapa de riesgos* correspondiente.

4 METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones antes descritas y la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Versión 5* (2020):

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	SGI, TIC y Gestión Documental	feb-24	dic-24
	Sensibilización	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	SGI y TIC	mar-24	may-24
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	SGI, TIC y Gestión Documental	mar-24	jul-24
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	SGI, TIC y Gestión Documental	mar-24	jul-24
	Aceptación de Riesgos	Aceptación, aprobación riesgos identificados y planes	SGI, TIC y Gestión	may-24	jul-24

	Identificados	de tratamiento	Documental		
	Publicación	Publicación mapas de riesgos relacionados con la seguridad y privacidad de la información	SGI y TIC	jun-24	ago-24
	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos identificados (verificación de evidencias)	SGI, TIC y Gestión Documental	ene-24	dic-24
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento	SGI, TIC y Gestión Documental	ene-24	dic-24
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones presentadas.	SGI, TIC y Gestión Documental	jul-24	dic-24
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	SGI	ene-23	dic-23

Los controles seleccionados de los riesgos de Seguridad y Privacidad de la Información serán confrontados con los estándares ISO 27001 versión 2022 y Modelo de Privacidad y Seguridad de la Información, a fin de determinar la brecha existente.

4.1 DESARROLLO METODOLÓGICO

4.1.1 Establecimiento del contexto

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción). A partir del contexto es posible establecer las posibles causas de los riesgos a identificar. De esta forma para la definición del contexto se seguirán las metodologías dispuestas en la entidad para lograr establecer las posibles causas y determinar la identificación de los riesgos.

4.1.2 Identificación del riesgo

Para la identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de

información, y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos.

La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (Incidente), por lo que es preciso identificar:

- El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad).
- El proceso dueño del riesgo, activo de información afectado.
- Amenazas, vulnerabilidades y consecuencias.

Para la identificación se pueden abarcar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.

4.1.3 Valoración del riesgo

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) se realizará acorde a la metodología establecida en el documento GM-GI-01 Guía para la gestión de riesgos.

Es así como en mesas de trabajo con los procesos se analiza el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades e identificando los controles para mitigarlas. A estos controles se le identifican las variables a evaluar para el adecuado diseño de controles como son: responsable, periodicidad, propósito, cómo se realiza la actividad de control, observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo.

Para los riesgos de interrupción, se indica que los controles identificados pueden ser transversales, partiendo del criterio denominado custodio del activo, puesto que cuando dicho custodio es un proceso diferente al proceso que identifica el riesgo o es un tercero, estos controles y planes de tratamiento deben establecerse de manera conjunta. El proceso donde se identifica el riesgo aporta los niveles de probabilidad, impacto y riesgo inherente que genera la posible indisponibilidad del activo

4.1.4 Definición y aprobación de mapas de riesgos y planes de tratamiento.

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción), los líderes de los procesos deberán emitir un memorando de la aprobación de los mapas de riesgos. De igual forma en este memorando aprobarán los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

4.1.5 Materialización

En el caso de materializarse un riesgo, este debe ser tratado de acuerdo con lo establecido en el documento GM-GI-01 Guía para la gestión de riesgos. Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en el mapa de riesgos.

4.2 Oportunidad de Mejora

La CRA no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

5 RECURSOS

La CRA, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), dispone de los siguientes recursos:

<table>
<tr><th>RECURSOS</th><th colspan="4">VARIABLE</th></tr>
<tr><td>Humanos</td><td colspan="4">• Profesional Especializado de Secretaría General – SGI
• Profesional Especializado de Secretaría General - TIC
• Profesional Especializado de Secretaría General - Gestión Documental
• Jefe de Oficina de Control Interno
• Líderes de procesos</td></tr>
<tr><td>Técnicos</td><td colspan="4">GM-GI-01 Guía para la gestión de riesgos
Herramienta para la gestión de riesgos (Matriz de Riesgos)</td></tr>
<tr><td>Logísticos</td><td colspan="4">Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.</td></tr>
<tr><td rowspan="3">Financieros</td><td colspan="4">Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías en Seguridad y Privacidad de la Información</td></tr>
<tr><td>Plan</td><td>Iniciativa</td><td>Proyecto</td><td>Presupuesto</td></tr>
<tr><td>Plan Estratégico de Tecnologías de la Información – PETI 2024 – 2027</td><td rowspan="2">Asegurarse de que las operaciones de Tecnologías de la Información cumplan con la legislación vigente, las normativas aplicables y la política de Gobierno Digital.</td><td>Implementación y certificación en ISO 27001</td><td>$400.000.000</td></tr>
<tr><td>Plan Estratégico de Seguridad y Privacidad de la Información – PETI 2024 – 2027</td><td>Implementación del Modelo de Seguridad y Privacidad de la Información</td><td>$75.000.000</td></tr>
</table>

6 PRESUPUESTO PARA LA IMPLEMENTACIÓN DE CONTROLES

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) identificados en la entidad, corresponderá al dueño del riesgo (líder del proceso), quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento.

7 MEDICIÓN

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los Servicios (riesgos de interrupción) aprobados por los procesos, así como de sus controles y planes de tratamiento, se realiza por parte del equipo la Secretaría General, liderados por el Profesional Especializado de SGI y apoyado por los Profesionales Especializados de TIC y Gestión Documental, teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando los resultados de los seguimientos realizados así como el cargue de los soportes correspondientes a los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de sus planes de tratamiento y controles, el equipo antes mencionado realizará la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el nivel de implementación de los controles de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los Servicios (riesgos de interrupción).

La medición se realiza con un indicador que está orientado principalmente a determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados en los sistemas de gestión de la entidad.

8 APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección y el comité de gestión y desempeño institucional, con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ		**REVISÓ**	**APROBÓ**
Nombre: José Lima Cargo: Profesional Especializado – Secretaría General – TIC	Nombre: Juan Calderón Cargo: Profesional Especializado – Secretaría General – SGI	Nombre: Pedro Cepeda Cargo: Secretario General	Nombre: Jesús León Cargo: Director General Fecha: