PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - PTRSI

OFICINA ASESORA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN
SECRETARÍA GENERAL

1. OBJETIVO

Fortalecer la gestión integral de los riesgos asociados a la Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios de la Corporación Autónoma Regional del Atlántico – CRA, mediante la definición, aplicación y apropiación de lineamientos, buenas prácticas y controles alineados con los requisitos legales, reglamentarios y normativos, con el propósito de proteger la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información, garantizar la continuidad institucional y contribuir al cumplimiento de la misionalidad de la entidad.

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, 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 los riesgos que superen el apetito del riesgo definido por la entidad, es decir, los que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por la Guía para la Gestión Integral del Riesgo en Entidades Públicas en su versión vigente, teniendo en cuenta que aquellos que se encuentren en niveles inferiores serán aceptados por la Entidad.

3. MARCO REFERENCIAL

3.1 POLÍTICA DE GESTIÓN DE RIESGOS DE LA CRA

La Corporación Autónoma Regional del Atlántico CRA está comprometida 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 Gestión 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 integridad pública.

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 gestión del riesgo dentro de la corporación.

La Corporación adopta la estructura conceptual para la gestión de riesgos establecida en la Guía para la gestión integral del riesgo en entidades pública 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 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con la Guía para la gestión integral del riesgo en entidades públicas – versión 7, del DAFP, para gestionar los riesgos de seguridad de la información, en primer lugar, se debe tener en cuenta que la política de seguridad digital de la información se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales y cultura digital.

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2022 y la Guía para la gestión integral del riesgo en entidades pública en su versión vigente.

3.3 APETITO DEL RIESGO

La C.R.A. establece como apetito de riesgo los niveles bajo y moderado identificados en el mapa de riesgos y oportunidades de cada proceso, por considerarse aceptables para el cumplimiento de sus objetivos institucionales. Por su parte, los riesgos clasificados en niveles alto y extremo deberán ser gestionados mediante la formulación e implementación del plan de tratamiento, a través de los cuales la entidad definirá las acciones necesarias para reducir, evitar, transferir o, cuando corresponda y esté debidamente justificado, aceptar dichos riesgos.

4. TÉRMINOS Y DEFINICIONES

- Aceptar el riesgo: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

- Activo de la información: Cualquier elemento que tiene valor para una organización y que contiene, procesa o soporta información, por lo que debe ser protegido.

- Gestión 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.

- Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- 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.

- Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

- Causa inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- Causa raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

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

- Corrupción: Todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero.

- Consecuencia: Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- 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.

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

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

- 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.

- 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.

- Fraude: Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.

- Frecuencia: Número de veces al año en el cual se realiza la actividad que conlleva al riesgo.

- 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)

- 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.

- 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.

- Integridad: Propiedad de exactitud y completitud.
- Monitorear: Comprobar, Supervisar, observar, o registrar la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles cambios.
- Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- 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.
- Punto de riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.
- 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 integridad pública: posibilidad de que, por acción u omisión, un servidor público o particular que ejerza funciones públicas utilice indebidamente sus facultades, recursos, información o posición para obtener un beneficio propio o favorecer a un tercero.

- 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.

- Soborno: Ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar.

- Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

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

5. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

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

5.1 IDENTIFICACIÓN Y VALORACIÓN DEL RIESGO

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:

Para la identificación de los riesgos se debe considerar por lo menos los siguientes insumos:

- El contexto interno y externo de la Corporación Autónoma Regional del Atlántico (Ver documento *Análisis del Contexto Interno y Externo de la Organización*).
- Las necesidades y expectativas de las partes interesadas de la C.R.A (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.

El mapa de riesgos y oportunidades será el instrumento institucional con el que contarán los procesos del Sistema de Gestión Integral de la C.R.A para la identificación de los siguientes riesgos:

- Riesgos institucionales.
- Riesgos de integridad pública.
- Riesgos fiscales.
- Riesgos de seguridad y privacidad de la información.

La valoración de los riesgos identificados se consolidará en el mismo instrumento, mapa de riesgos y oportunidades, siguiendo los establecido en la Guía CG-GI-01 Gestión de Riesgos y Oportunidades que adopta los lineamientos de la Guía para la gestión integral del riesgo en entidades pública emitida por el Departamento Administrativo de la Función Pública.

6. SEGUIMIENTO, REVISIÓN Y ACTUALIZACIÓN DE LOS MAPAS DE RIESGOS Y OPORTUNIDADES

6.1 SEGUIMIENTO DE LOS RIESGOS

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

El seguimiento de los riesgos y oportunidades, en primera instancia es responsabilidad de los líderes de los procesos, quienes son los encargados de gestionar las acciones asociadas a los controles y actividades 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 los riesgos no se materialicen y las oportunidades se consoliden, y por ende que los objetivos del proceso se cumplan.

6.2 REVISIÓN DE LOS MAPAS DE RIESGOS Y OPORTUNIDADES

La Corporación Autónoma Regional del Atlántico, en concordancia con el Modelo Integrado de Planeación y Gestión MIPG adoptado por la Resolución 0000038 de 2024, establece la operatividad de la gestión del riesgo basado en las líneas de defensa requerido por la Guía para la gestión integral del riesgo en entidades públicas en su versión vigente, tal como se muestra en la siguiente figura:

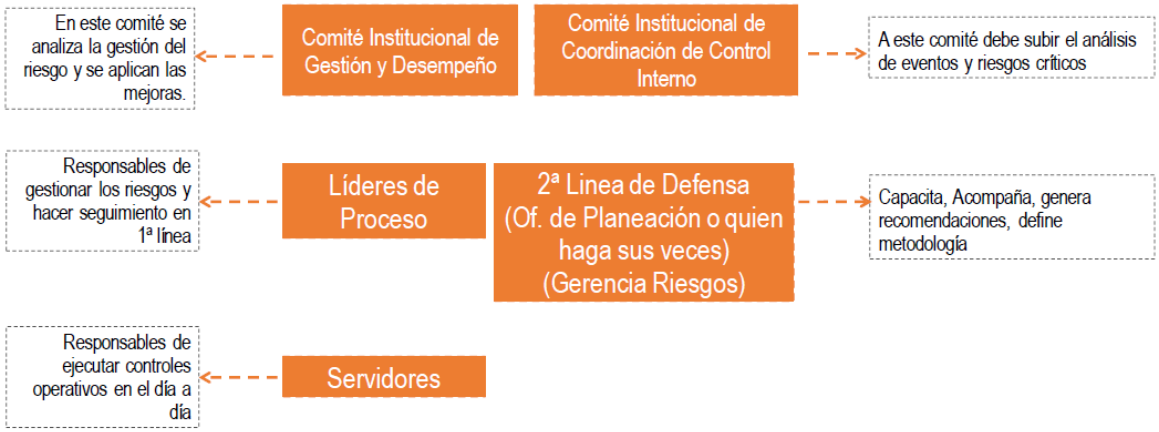


Figura No.1 Operatividad Institucional para la administración del riesgo.
Fuente: *Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.*

El establecimiento de las responsabilidades y autoridades frente a la gestión del riesgo se registran en la Guía de roles, responsabilidades y autoridades en el Sistema de Gestión Integral en su versión vigente.

Cabe resaltar que, la Coordinación del Sistema de Gestión Integrado 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 y oportunidades 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 gestión, la Oficina de Control Interno de la Corporación realizará la revisión a los riesgos que han sido consolidados en el Mapa de riesgo y oportunidades de los procesos, con el fin de evaluar el diseño, efectividad e idoneidad de los controles y determinar si los riesgos se han materializado.

6.3 ACTUALIZACIÓN DE LOS MAPAS DE RIESGOS Y OPORTUNIDADES

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

7. METODOLOGÍA

En la tabla 1, se contemplan las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, las cuales se estructuraron siguiendo las recomendaciones antes descritas, y los lineamientos de la Guía para la gestión integral del riesgo en entidades pública en su versión vigente:

Objetivo	Actividad	Responsable (s)	Fechas Programación		Evidencia
			Inicio	Fin	
Actualizar los lineamientos para la gestión de riesgos de seguridad de la información	Revisar la política, metodología y lineamientos de riesgos frente a cambios normativos, hallazgos de auditoría o resultados de la revisión por dirección, y ajustar lo que corresponda.	Secretaria General (SGI) Oficina Asesora CTeI Secretaria General (Gestión Documental y Archivo)	01-01-2026	30-12-2027	Acta de revisión; política/actualizada
Fortalecer la cultura de gestión de riesgos	Diseñar e implementar la estrategia de sensibilización institucional, con refuerzo específico en los procesos con riesgos alto/extremo.	Secretaria General (SGI) Oficina Asesora CTeI	01-01-2026	30-12-2027	Listas de asistencia, registro fotográfico, evaluaciones
Identificar y valorar los riesgos por proceso	Revisar el contexto interno/externo de la CRA y las partes interesadas, identificar/actualizar los riesgos en el mapa de riesgos y oportunidades de cada proceso, y validarlo ante la Coordinación del SGI	Secretaria General (SGI) Oficina Asesora CTeI Secretaria General (Gestión Documental y Archivo)	01-01-2026	30-12-2027	Mapa de riesgos y oportunidades validado, ajustados; análisis de contexto
Definir y aprobar el	Definir, por cada riesgo alto/extremo, los planes	Secretaria General (SGI)	01-01-	30-12-	Plan de tratamiento

tratamiento de los riesgos	de tratamiento, actualizar la Declaración de Aplicabilidad (SOA) y obtener la aprobación del propietario del riesgo.	Oficina Asesora CTeI Secretaria General (Gestión Documental y Archivo)	2026	2027	aprobado; Declaración de Aplicabilidad actualizada
Divulgar los riesgos institucionales	Publicar los mapas de riesgos y oportunidades y el plan de tratamiento aprobado en el canal institucional definido	Secretaria General (SGI) Oficina Asesora CTeI Secretaria General (Gestión Documental y Archivo)	01-01-2026	30-12-2027	Plan de tratamiento divulgado (registro de publicación)
Ejecutar el tratamiento de riesgos	Implementar los controles definidos, incluyendo como mínimo los aplicables del Anexo A de ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información, y verificar su ejecución	Secretaria General (SGI) Oficina Asesora CTeI Secretaria General (Gestión Documental y Archivo)	01-01-2026	30-12-2027	Plan de tratamiento ejecutado; soportes de controles
Evaluar el riesgo residual	Realizar el seguimiento a los riesgos residuales evaluados en los mapas de riesgos y oportunidades	Secretaria General (SGI) Oficina Asesora CTeI	01-01-2026	30-12-2027	Mapa de riesgos con riesgo residual actualizado; aceptación firmada
Mejorar continuamente la gestión de riesgos	Identificar oportunidades de mejora a partir del seguimiento a controles, la evaluación de riesgo residual y los hallazgos de auditoría	Secretaria General (SGI) Oficina Asesora CTeI Secretaria General (Gestión Documental y	01-01-2026	30-12-2027	Seguimiento al plan de tratamiento; documento ajustado si aplica

		Archivo)			
Monitorear el desempeño de la gestión de riesgos	Medir, consolidar y reportar el indicador de ejecución de controles, articulándolo con la auditoría interna del SGSI y la revisión por la dirección	Secretaria General (SGI) Oficina Asesora CTeI Secretaria General (Gestión Documental y Archivo)	01-01-2026	30-12-2027	Medición de indicadores; informe de auditoría interna; acta de revisión por la dirección

Tabla No.1 Planificación de actividades para la gestión de riesgos de seguridad y privacidad de la información

Los controles para abordar los riesgos de Seguridad y Privacidad de la Información están establecidos en los mapas de riesgos y oportunidades de cada proceso.

7.1 PLAN DE TRATAMIENTO

El Plan de Tratamiento establece las acciones necesarias para gestionar los riesgos de seguridad de la información identificados en cada proceso que excedan el apetito de riesgo definido por la entidad, es decir, aquellos riesgos cuyo nivel de valoración supere los niveles bajo y moderado, considerados aceptables para la entidad, de acuerdo con los criterios establecidos en el Mapa de Riesgos y Oportunidades.

A continuación, en la tabla 2 se presentan las acciones de tratamiento con el fin de reducir la probabilidad de materialización y/o el impacto de los riesgos sobre el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información	Acciones de tratamiento	Responsable	Fecha límite de ejecución	Evidencia de cumplimiento	Alineación Controles ISO 27001 Anexo A
Pérdida de disponibilidad e integridad de la información en medios digitales	Diseñar el procedimiento para la Gestión de Incidentes, eventos y problemas	Profesional Especializado Oficina Asesora de CTeI	30/10/2026	Procedimiento de Gestión de Incidentes, eventos y problemas proyectado	5.24 5.25 5.26 5.27
	Adoptar del procedimiento para la gestión de incidentes, eventos y problemas	Coordinador SGI	30/10/2026	Acta de Comité Institucional de Gestión y Desempeño	5.24 5.25 5.26 5.27
	Implementar los lineamientos adoptados en el procedimiento	Profesional Especializado	31/12/2026	Registros de gestión de incidentes, eventos y problemas	5.24 5.25 5.26

	para la Gestión de Incidentes, eventos y problemas	Oficina Asesora de CTeI			5.27
	Diseñar de Procedimiento para la Administración de Capacidad de Tecnología	Profesional Especializado Oficina Asesora de CTeI	30/10/2026	Procedimiento para la Administración de Capacidad de Tecnología proyectado	8.6
	Adoptar el Procedimiento para la Administración de Capacidad de Tecnología	Coordinador SGI	30/10/2026	Acta de Comité Institucional de Gestión y Desempeño	8.6
	Implementar los lineamientos adoptados en el Procedimiento para la Administración de Capacidad de Tecnología	Profesional Especializado Oficina Asesora de CTeI	31/12/2026	Registros de la administración de la capacidad de tecnología	8.6
	Diseñar Política de Escritorios y Pantallas Limpias	Coordinador SGI Profesional Especializado Oficina Asesora de CTeI	30/10/2026	Política de Escritorios y Pantallas Limpias proyectada	7.7
	Adoptar Política de Escritorios y Pantallas Limpias	Coordinador SGI	30/10/2026	Acta de Comité Institucional de Gestión y Desempeño	7.7
	Socializar la Política de Escritorios y Pantallas Limpias	Coordinador SGI Profesional Especializado Oficina Asesora de CTeI	31/12/2026	Registros de Socialización de la Política de Escritorios y Pantallas Limpias	7.7 6.3
Pérdida de disponibilidad de la infraestructura tecnológica	Proyectar documentación pre contractual para la adquisición de servicios especializados en la identificación y evaluación de vulnerabilidades técnicas de las redes y equipos de tecnología de la C.R.A.	Jefe de oficina asesora de CTeI	31/01/2027	Documentación precontractual (estudios previos entre otros)	8.8
	Ejecutar la identificación y evaluación de las vulnerabilidades técnicas de las redes y equipos de tecnología de la C.R.A. a través de servicio especializado	Profesional(es) Especializado(s)	31/03/2027	Matriz de vulnerabilidades	8.8
	Diseñar el Plan de Atención de las vulnerabilidades identificadas	Profesional(es) Especializado(s)	30/04/2027	Plan de Atención de las vulnerabilidades identificadas	8.8
	Ejecutar las actividades establecidas en el plan de	Equipo designado por Jefe de oficina asesora de CTeI	31/12/2027	Registros de actividades de	8.8

	atención de las vulnerabilidades identificadas			gestión de vulnerabilidades	
Pérdida de confidencialidad de la información asociada a las personas	Diseñar el Plan de Contingencia Específico (PCE) para la recuperación de la información sensible.	Jefe de Oficina Asesora de CTeI Jefe la Oficina de Gestión Humana Jefe de la Oficina Asesora Jurídica	31/03/2027	Plan de contingencia específico	5.24 5.25 5.26 5.27
	Adoptar el Plan de Contingencia Específico (PCE) para la recuperación de la información sensible.	Coordinador SGI	30/04/2027	Acta de Comité Institucional de Gestión y Desempeño	5.24 5.25 5.26 5.27
	Socializar el Plan de Contingencia Específico (PCE) para la recuperación de la información sensible.	Jefe de Oficina Asesora de CTeI	31/05/2027	Registros de Socialización	5.24 5.25 5.26 5.27 6.3
	Diseñar el procedimiento interno para la gestión de casos de incumplimiento a las políticas institucionales de seguridad y privacidad de la información	Jefe de Oficina Asesora de CTeI Jefe de la Oficina de Control Disciplinario Interno	31/03/2027	Plan de contingencia específico	6.4
	Adoptar procedimiento interno para la gestión de casos de incumplimiento a las políticas institucionales de seguridad y privacidad de la información	Coordinador SGI	30/04/2027	Acta de Comité Institucional de Gestión y Desempeño	6.4
	Socializar procedimiento interno para la gestión de casos de incumplimiento a las políticas institucionales de seguridad y privacidad de la información	Jefe de Oficina Asesora de CTeI	31/05/2027	Registros de Socialización	6.3 6.4

Tabla No.2 Plan de Tratamiento de riesgos de seguridad y privacidad de la información

8. RECURSOS

La C.R.A., 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, dispone de los recursos que se relacionan en la tabla 3.

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 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.

TIPO DE RECURSO	DESCRIPCIÓN
Humanos	• Profesional Especializado de Secretaría General – SGI • Profesional Especializado de la Oficina de CTI • Profesional Especializado de Secretaría General - Gestión Documental • Jefe de Oficina de Control Interno • Líderes de procesos
Técnicos	GM-GI-01 Guía para la gestión de riesgos y oportunidades Herramienta para la gestión de riesgos (Mapa de riesgos y oportunidades)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías en Seguridad y Privacidad de la Información. Se definirán y asignarán los recursos de acuerdo con la planeación estratégica institucional (Plan de Acción Institucional – PAI).

Tabla No.3 Recursos el tratamiento de riesgos de seguridad y privacidad de la información

9. MEDICIÓN

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información se realizará de acuerdo con el esquema de roles, responsabilidades y autoridades basados en las líneas de defensa del Control Interno.

Los resultados de esta medición se reportarán en las auditorías de gestión adelantas por la Oficina de Control Interno, y en las auditorías internas del Sistema de Gestión Integrado de la Corporación.

10. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección y el Comité Institucional de Gestión y Desempeño, con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

11. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
1	05/11/2024	Creación del documento.
2	22/06/2026	Se actualiza el documento acorde con los lineamientos definidos por la Guía para la Gestión Integral del Riesgo en Entidades Públicas en su versión vigente. Se incluye el concepto de apetito de riesgo. Se incluyen términos y definiciones. Se actualiza la metodología: se ajustan las actividades.
3	29/10/2026	Se incorpora el punto 7.1 Plan de tratamiento.