icontec ISO 9001 SC-CER103099
icontec ISO 14001 SA-CER756031
IQNET CERTIFIED MANAGEMENT SYSTEM

Plan de tratamiento de Riesgos de Seguridad de la Información

Gestión de las tecnologías y la información

Gerencia TIC

Enero de 2026

Contenido

Objetivo General:

Definir los lineamientos y metodología a seguir para el análisis, valoración y tratamiento de riesgos de Seguridad, alineados con las políticas de seguridad y privacidad de la información.

Objetivos Específicos:

- Gestionar los eventos de seguridad de la información, con el fin de ser necesario clasificarlos como incidentes de seguridad.
- Establecer el alcance del presente plan.
- Identificar los activos con prioridad de proteger
- Identificar las potenciales amenazas que puedan afectar los activos de TI
- Establecer controles para minimizar los riesgos a los que está expuesto un activo.
- Evaluar el nivel de impacto de los riesgos después de implementar el presente plan.

Alcance:

La identificación y tratamiento de los riesgos de seguridad de la información será de estricta aplicabilidad y cumplimiento por parte de funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Alcaldía de Barranquilla; dicho tratamiento de riesgo involucra a todos los procesos, en especial los que impactan los objetivos misionales.

Contexto:

De conformidad con el Decreto acordal 0801 de 2020, por el cual de adopta la estructura organiza de la administración central del distrito, industrial y portuario de Barranquilla, el cual estipula en parágrafo del artículo 13, a la Gerencia de las TIC-Tecnologías de la información y comunicación, como Gerencia adscrita al Despacho del alcalde.

“ARTÍCULO 36. FUNCIONES DE LA GERENCIA DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES – TIC: Establecer políticas y programas en materia tecnológica que garanticen la seguridad de la información y la óptima operación de los procesos al interior de la entidad, logrando una eficiente prestación de los servicios a los ciudadanos, mejorando la calidad de vida de la comunidad y el acceso a mercados para el sector empresarial.”

Así mismo, en el artículo 36 del mismo Decreto señala las funciones segundarias de la Gerencia TIC: “Identificar, valorar, intervenir, monitorear y evaluar los riesgos de TI de la entidad para evitar la ocurrencia de incidentes de seguridad que pongan en riesgo la información y continuidad de operación de la entidad.”

La implementación del Sistema de Gestión de Seguridad de la Información surge en el contexto de lo expuesto en el Decreto Ministerial 1078 de 2015 referido a las obligaciones de los sujetos obligados en el artículo 2.2.9.1.1.2. para la implementación del habilitador de seguridad de la información, en atención a las orientaciones definidas en el Manual de Gobierno Digital, relacionadas con la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, refrendadas y actualizadas a través del Decreto Presidencial 767 de 2022 en lo referente al habilitador de seguridad y privacidad de la información, el cual derogo el Decreto 1008 de 2018.

De igual manera es importante resaltar que es a través del Decreto Presidencial 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, en su artículo 1, Página 8 de 21adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015, Único Reglamentario del Sector de Función Pública, agregando al anterior Decreto el artículo 2.2.22.3.14, por medio del cual se integran los planes institucionales y estratégicos al Plan de Acción, considerando en su numeral 11 y 12 como obligación la elaboración anual del “Plan de Tratamiento de Riesgos de

Seguridad y Privacidad de la Información" y del "Plan de Seguridad y Privacidad de la Información" respectivamente de cada Entidad, y lo señalado en la Ley 1474 de 2011 por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, señala en su artículo 74 denominado "Plan de acción de las entidades públicas", indicando que a partir de la vigencia de la presente Ley, todas las entidades del Estado a más tardar el 31 de enero de cada año, deberán publicar en su respectiva página web el Plan de Acción para el año siguiente". Coherente con lo anterior, la Gerencia de las TIC ha venido adelantando acciones en toda la entidad encaminadas a fortalecer las capacidades institucionales para dar cumplimiento a las disposiciones legales vigentes en materia de seguridad y privacidad de la información, atendiendo las orientaciones del Ministerio de Tecnologías de Información contenidas en la Resolución Ministerial 0500 de 2021 y sus respectivos anexos.

Marco normativo:

- Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales"
- Decreto 612 de 2018: "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".
- Resolución 00500 de 2021: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital".
- Resolución 746 de 2022: "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021"
- ISO/IEC 27001:2022 Norma técnica de seguridad de la información.

Términos y 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.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Seguridad de la Información: Conjunto de técnicas y métodos encaminados a la preservación de la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, medios de almacenamiento y/o difusión.

Tratamiento del Riesgo: Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos. El tratamiento de los riesgos puede hacerse

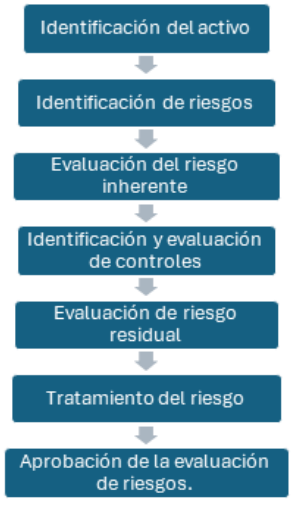
mediante la aplicación de la política de tratamiento definida que puede: aceptar el riesgo, reducir el riesgo, evitar el riesgo o compartir el riesgo.

Lineamientos en ejecución:

- ✓ La Gerencia de las TIC, lideran la correcta implementación de la Gestión de los riesgos de seguridad de la información en la entidad.
- ✓ En el procedo de valoración de riesgos deben estar involucrados todos los lideres de procesos, encargados y custodios de la información.
- ✓ El plan de tratamiento de riesgos debe estar aprobado y publicado.
- ✓ La periodicidad el análisis de riesgos será anual o cuando sea pertinente realizar actualizaciones por cambios significativos en la operación de los activos de TI.

Metodología de evaluación de riesgos de seguridad de la información:

Para iniciar el proceso de gestión de riesgos es necesario seguir la guía de administración de riesgos 2025, versión 3. En la cual se siguen los siguientes pasos:



Continuando con las directrices de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas, emitido por el departamento administrativo de función pública y para lograr un clico de mejora continua en la gestión y tratamiento de riesgos, se definen las siguientes fases:

Fase1 Análisis de la información: revisar los resultados de la evaluación de los activos de TI con los diferentes procesos para desarrollar las actividades:

- Verificar y analizar los riesgos identificados
- Determinar los controles aplicables a cada riesgo según el anexo de la 27001.

Fase 2 Desarrollo de medidas de tratamiento de riesgos

- Determinar la medida de tratamiento con sus responsables
- Establecer objetivo y acciones de cumplimiento.

Fase 3 Análisis de los riesgos y medidas aplicadas

- Validar la eficacia de los controles definidos
- Analizar la aplicabilidad de las medidas de mitigación y tratamiento.

Actividades de Plan de tratamiento de riesgos de seguridad de la información (PTRSI)

No	Actividad	Evidencia	Fecha Inicio	Fecha fin	Responsable
Plan de tratamiento de riesgos de seguridad de la información					
1	Definir documento preliminar PTRSI	Borrador del Plan	Diciembre 2025	Diciembre de 2025	Profesional universitario – Grupo administrativa GTIC
2	Revisar y aprobar PTRSI	Sección del comité institucional de gestión y desempeño	Enero 2026	Enero 2026	Secretaria de Planeación
3	Publicar en sede electrónica de la entidad	Url de la publicación del PTRSI	Enero 2026	Enero 2026	Asesor área administrativa GTIC
Riesgo de seguridad de la información					
1	Apoyar la identificación de riesgos de seguridad	Mapa de riesgos de	Septiembre de 2025	Diciembre de 2026	Profesional universitario – Grupo administrativa GTIC y

No	Actividad	Evidencia	Fecha Inicio	Fecha fin	Responsable
	de la información a los procesos de la entidad	seguridad de la información			Enlaces TIC de procesos de la entidad.
2	Consolidar mapa de riesgos	Mapa de riesgos de seguridad de la información	Diciembre de 2025	Diciembre de 2025	Profesional universitario – Grupo administrativa GTIC
3	Acompañar técnicamente a los procesos en el seguimiento al mapa de riesgos de seguridad de la información	Correos institucionales y mapa de riesgos	Febrero 2026	Diciembre de 2026	Profesional universitario – Grupo administrativa GTIC y Enlace TIC de procesos de la entidad.
4	Identificación de oportunidades de mejora acorde a la ejecución de los controles y de los planes de tratamiento	Lecciones aprendidas y formato de oportunidades de mejora	Febrero 2026	Diciembre de 2026	Profesional universitario – Grupo administrativa GTIC y Enlace TIC de procesos de la entidad.
5	Revisión y/o actualización de lineamientos de riesgos de seguridad y privacidad de la información de acuerdo con las observaciones identificadas.	Acta de reunión, borrador del documento	Febrero 2026	Diciembre de 2026	Profesional universitario – Grupo administrativa GTIC y Enlace TIC de procesos de la entidad.

Acciones de tratamiento de riesgos identificados

Fecha	Activo	Acción	Responsable	Objetivo
Enero-diciembre	Sistemas de información desactualizados	Realizar análisis de vulnerabilidades técnicas a los activos de información	Lideres de proceso Gerente de las TIC	Monitorear y mantener actualizado los sistemas de información para minimizar vulnerabilidades

Fecha	Activo	Acción	Responsable	Objetivo
Enero-diciembre	Servidores	Plan de mantenimiento preventivo de infraestructura TI	Gerente de las TIC; Asesor de infraestructura	Tomar medidas apropiadas y oportunas en respuesta a posibles vulnerabilidades técnicas
Enero-diciembre	Aplicativos webs	Mejorar los controles de acceso y autenticación de usuarios de los aplicativos	Gerente de las TIC; Asesor de software; usuarios con privilegios	Implementar técnicas de autenticación adecuadas para el control de acceso
Enero-diciembre	Usuarios finales	Impulsar la cultura de seguridad de la información en los funcionarios, contratistas y terceros	Gerente de las TIC; Asesor administrativa	Fortalecer los conceptos de seguridad de la información dando a conocer los roles y responsabilidades con la política de seguridad.

En la gestión del tratamiento de riesgos debemos tener en cuenta los siguientes factores:

- Recibirán tratamiento todos los riesgos que tengan un nivel de exposición Alto y Extremo
- Si es susceptible de ser tratado a través de la implantación de un nuevo control o fortaleciendo los ya existentes.
- Si la decisión es aceptarlo, independiente de donde se encuentre ubicado y la afectación que pueda tener para Confidencialidad, Integridad y Disponibilidad de la información.
- Si se decide ignorar el riesgo se reinicia el análisis

Indicadores de Medición

La medición se realiza con un indicador que esta orientado principalmente a determinar el porcentaje de ejecución de controles definidos para mitigar los riesgos identificados, bajo la siguiente parametrización:

Metas		
Desde	Hasta	Calificación
90%	100%	Alto
70%	89%	Medio
0	69%	Bajo

Recomendaciones:

- Monitoreos periódicos a los controles asignados a los riesgos de seguridad identificados.
- Realizar los procesos de identificación y valoración a los riesgos identificados con el objetivo de verificar la nueva valoración y definir controles más efectivos.
- Realizar la clasificación de los activos de tecnología acatando los lineamientos establecidos en el Modelo de seguridad.
- Conformar grupos con los enlaces de las áreas que administraran infraestructura TI para mantener actualizados por planes pertinentes a la seguridad y privacidad de la información.

Control de cambio

Versión	Fecha	Descripción
1	19-01-2026	Primera versión del plan