CORPORACIÓN AUTÓNOMA REGIONAL DEL QUINDÍO

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

VERSION 06

ENERO 2025

CONTROL DE CAMBIOS

Versión	Fecha (dd/mm/aaaa)	Descripción
01	20/01/2020	Versión inicial del documento.
02	25/01/2020	Actualización del plan de acuerdo con la versión 5 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.
03	25/01/2022	Actualización del cronograma de acuerdo con lo planteado en el Plan de Seguridad y Privacidad de la Información.
04	30/01/2023	Actualización del documento.
05	30/01/2024	Actualización del documento.
06	31/01/2025	Actualización del documento.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones para Colombia.

La estrategia de Gobierno Digital, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la CRQ estará determinado por las necesidades y objetivos, los requisitos de seguridad y la estructura de procesos.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, es una orientación estratégica que requiere el fortalecimiento de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de su materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en la estrategia de tecnologías de la información y demás procesos de la Entidad.

2. OBJETIVOS

- Definir y aplicar los lineamientos legales y reglamentarios para el tratamiento de riesgos de seguridad y privacidad de la información en la CRQ.

- Integrar los riesgos de seguridad y privacidad de la información al componente estratégico de administración de riesgos definido en la Entidad.

- Aplicar la metodología y lineamientos definidos en la Entidad para la administración de riesgos.

3. Alcance

Aplica para todas las dependencias, funcionarios y contratistas de la CRQ, y para toda persona natural o jurídica que por sus funciones hagan uso de la información digital de la Entidad sin importar la ubicación, medio o formato.

4. POLITICA DE ADMINISTRACIÓN DE RIESGOS

La Corporación Autónoma Regional del Quindío diligenciará las matrices de riesgos por proceso, los cuales incluirán los riesgos de seguridad digital.

La Corporación Autónoma Regional del Quindío declara que aceptará, una vez valorados, aquellos riesgos que se ubiquen en zona de riesgo inferior y bajo. Por lo tanto, no es necesario el establecimiento de controles para su tratamiento, sin embargo, el responsable de la ejecución del proceso podrá establecer controles con el objetivo de disminuir el riesgo de materialización.

No obstante, los riesgos clasificados como Riesgos de Corrupción no tienen nivel de aceptación, lo que implica que deberá establecerse controles para los riesgos ubicados en todas las zonas de riesgo”.

5. METODOLOGÍA PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dentro del Marco de Seguridad del Modelo de Seguridad y Privacidad de la información - MSPI, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones.

Teniendo en cuenta que en el contexto organizacional de las entidades del Estado se ha venido desarrollando la integración de los diferentes sistemas de gestión, la metodología sugerida para la gestión de riesgos es la definida por el Departamento Administrativo de la Función Pública, para lo cual se tiene como referencia el documento “Guía para la administración del riesgo y el diseño de controles en entidades públicas”.

Igualmente, como referencia se tendrá la norma ISO 31000 Gestión del Riesgo, así como las normas ISO 27001 Sistemas de Gestión de Seguridad de la Información y la ISO 27005 Gestión de Riesgos de Seguridad de la Información.

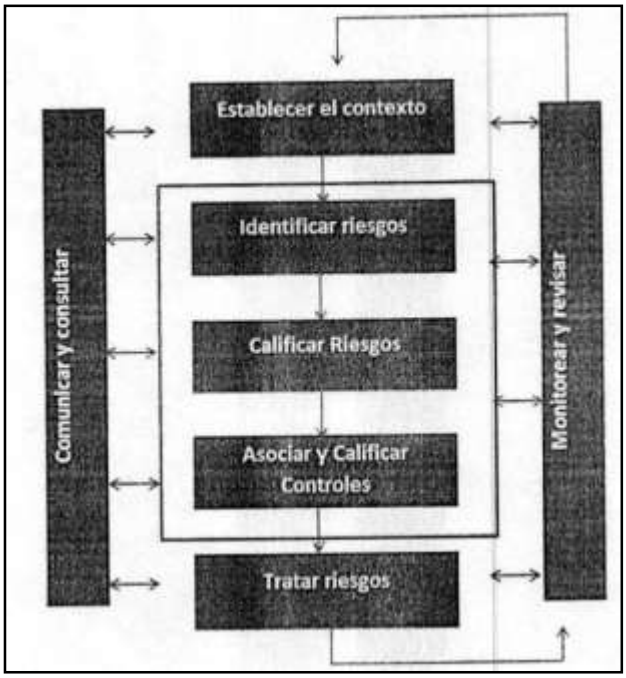

Figura 1. Metodología para la Gestión del Riesgo. Fuente: DAFP

Igualmente se utiliza como referencia la metodología definida por el Departamento Administrativo de la Función Pública – DAFP - a través del documento “Guía para la administración del riesgo y el diseño de controles en entidades públicas”.

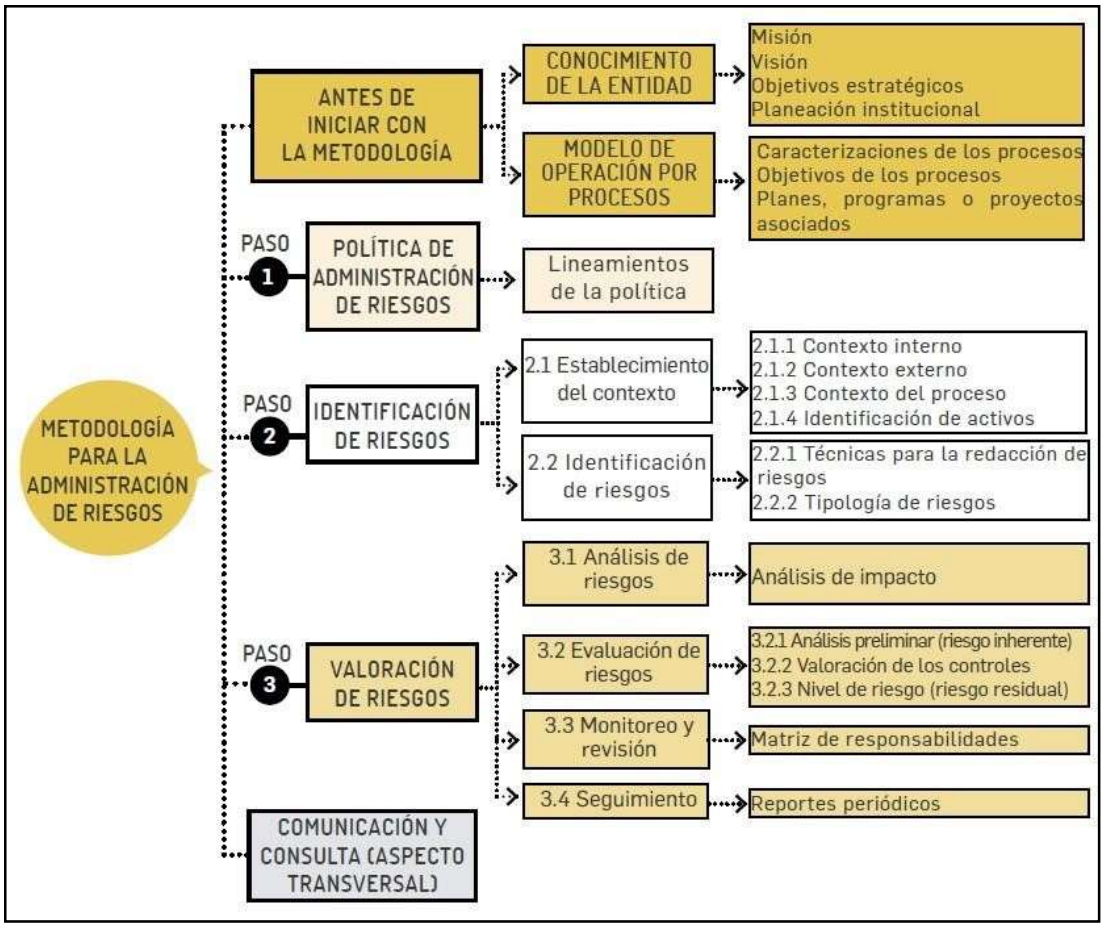

Figura 2. Metodología para la administración del riesgo del DAFP

Adicionalmente se integrará la metodología de la ISO 27005 Gestión de Riesgos de Seguridad de la Información.

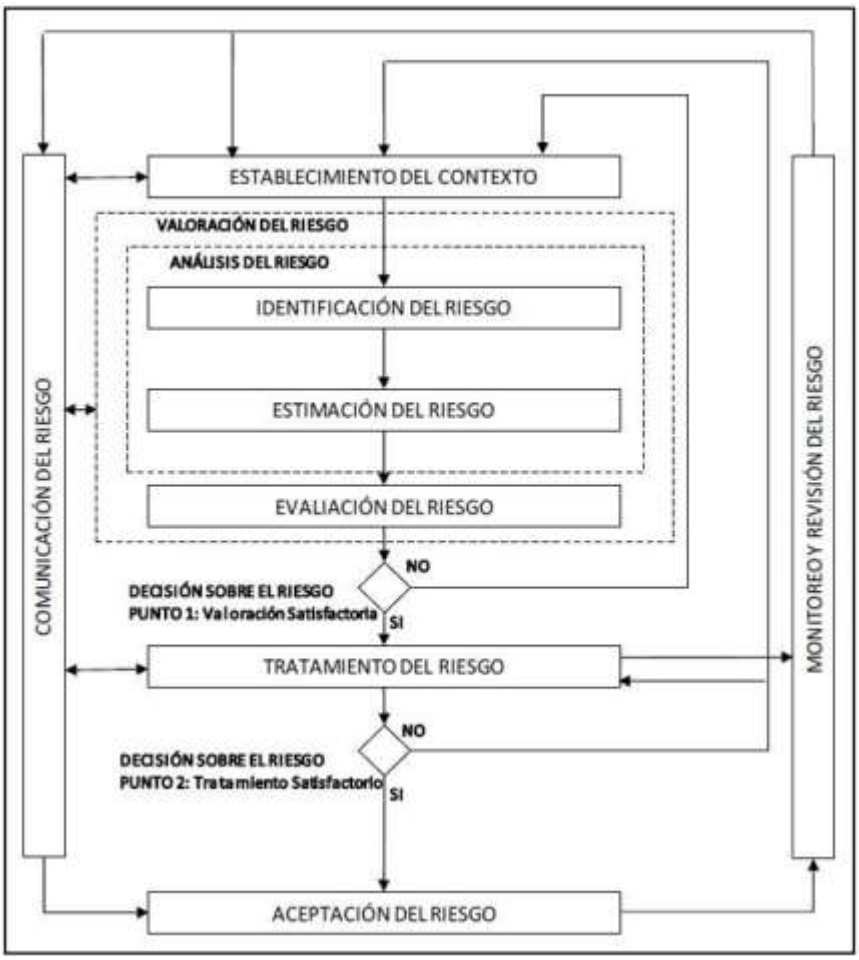

Figura 3. Metodología para la administración del riesgo ISO 27005

Como se muestra en la figura 2, el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

Los controles establecidos serán de acuerdo con los controles de la Norma ISO 27001, anexo A.

Igualmente, se tendrá en cuenta la nueva Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 de diciembre de 2020 de la del Departamento Administrativo de la Función Pública.

En esta nueva versión se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo. Es importante resaltar que se mantiene la estructura general bajo tres pasos principales, los cuales fundamentan la estructura metodológica que desde las primeras versiones de la guía se ha venido desarrollado.

A continuación se describe las fases y actividades a desarrollar las cuales se programarán de acuerdo con los planes y proyectos establecidos en el Plan de Acción de Entidad.

6. CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FASES / ACTIVIDADES	ENE.	FEB.	MAR.	ABR.	MAY.	JUN.	JUL.	AGO.	SEP.	OCT.	NOV.	DIC.
Establecer el Contexto												
Establecer el Contexto interno y externo												
Identificar el Inventario de activos de información												
Identificar Riesgos												
Identificar los riesgos de seguridad de acuerdo con el inventario de Activos de Información												
Valoración de Riesgos												
Análisis de impacto de los riesgos identificados												
Evaluación de Riesgos (Análisis preliminar - riesgo inherente, valoración de controles, nivel de riesgo - riesgo residual)												
Monitoreo y revisión, definir matriz de responsabilidades, indicadores												
Seguimiento												