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

Corpocaldas

PLAN INSTITUCIONAL DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
2024

CORPORACIÓN AUTÓNOMA REGIONAL DE CALDAS – CORPOCALDAS

Subdirección Administrativa y Financiera
Proceso Gestión tecnológica

Manizales, enero de 2024

PLAN INSTITUCIONAL DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN VIGENCIA 2024

Proceso Gestión tecnológica
Subproceso Gestión de TIC

Autores:
Ruben Dario Jaramillo Parra, Líder del Subproceso de Gestión de las TIC
Luisa Fernanda Callejas Orrego, Oficial de seguridad de la información (Contratista)

Aprobado por:
Comité Institucional de Gestión y Desempeño
Fecha de aprobación: 26 de enero de 2024
Acta de Aprobación No. 1 de 2024
Fecha de publicación: enero 31 de 2024

Tabla de contenido

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de privacidad y seguridad de la información, define las actuaciones de Corpocaldas entorno a la gestión de riesgo enfocada a procesos, que le permite identificar, evaluar, tratar y dar seguimientos a los riesgos de seguridad de la información a los que estén expuestos los activos de información, para prevenir su materialización y/o reducir los impactos negativos en la gestión institucional y de esta manera fomentar el desarrollo de la cultura preventiva en este entorno.

Es por esta razón, cabe resaltar que 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, adiciona 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 como obligación la elaboración anual del "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" para la entidad.

Este documento se basa en las recomendaciones técnicas establecidas por el ministerio de las tecnologías de la información y comunicación MinTIC, apoyadas en sugerencias emitidas por el departamento administrativo de la función pública DAFP para la gestión de riesgos, adoptadas por medio del plan de gestión de riesgos de la Corporación y demás normas internacionales y normativas nacionales establecidas por el estado colombiano.

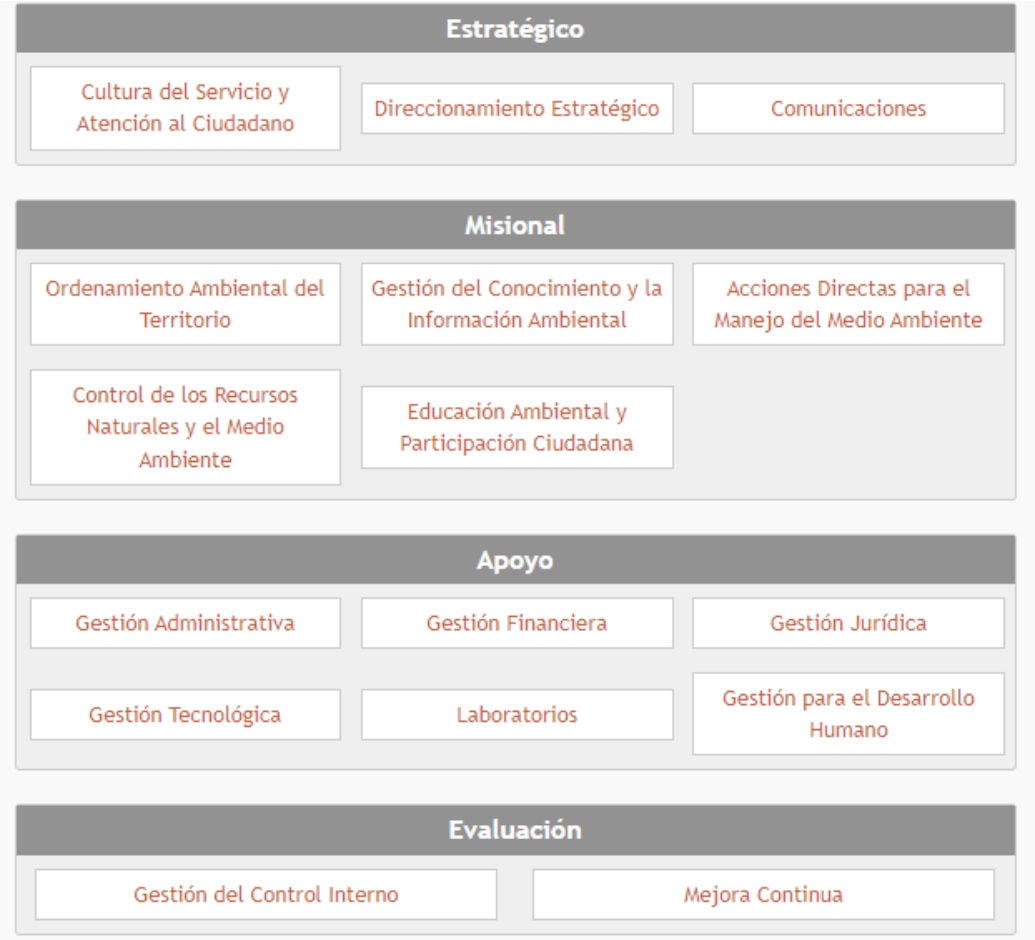
2. CONTEXTO ESTRATÉGICO DE LA ENTIDAD

Misión: Contribuimos al desarrollo sostenible del territorio, a través de la conservación y uso racional de los recursos naturales y el medio ambiente en el departamento de Caldas, mediante la aplicación de las normas y políticas ambientales, la modernización institucional y el fortalecimiento de la cultura del servicio hacia nuestros grupos de interés, con un talento humano comprometido y calificado.

Visión: Al 2031 Corpocaldas será el principal promotor del desarrollo sostenible del territorio para el bienestar de las generaciones presentes y futuras.

Mapa de operación por procesos:
Dentro del Sistema de Gestión Integrado, Corpocaldas cuenta con el mapa de procesos el cual se compone de cuatro tipos de procesos: ESTRATÉGICOS, MISIONALES, APOYO Y DE EVALUACIÓN. (Ver Mapa de Operación de Procesos).

Imagen 1. Mapa de procesos



Fuente: Elaboración propia. Sistema de información SGI.

3. ANÁLISIS DE LA SITUACIÓN ACTUAL

Para el año 2022 se identificaron las amenazas y las vulnerabilidades desde el área de TI, la Corporación elaboró y aprobó la política y metodología para la administración de riesgos de Corpocaldas, el cual se adopta para realizar todo el proceso de tratamiento de riesgo de Seguridad y privacidad de la Información.

Durante el año 2023 se realizó la identificación de activos de seguridad la información con base en el Índice de información clasificada y Reservada, el cual también se complementó como apoyo al proceso de gestión documental. Seguido a esto se inició la identificación, evaluación y clasificación de los riesgos de seguridad de la información, además de proponer los controles para cada uno de los procesos y subprocesos, en donde a su vez, se identificaron controles los cuales fueron implementados de manera efectiva por los lideres de proceso.

El proceso de la gestión de riesgos de seguridad de la información se realiza con base en la metodología del Departamento de Administrativo de la Función Pública - DAFT y la guía de gestión de riesgos de MinTIC, ajustando una metodología propia de acuerdo con las necesidades de la corporación y la cual se encuentra integrada a la política de gestión de riesgos de Corporcaldas que se encuentra en proceso de actualización.

4. MARCO NORMATIVO

Tabla 1: Marco normativo

NORMA	DESCRIPCIÓN
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Modelo de seguridad y privacidad de MINTIC	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
Decreto 1008 de 14 de junio de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Serie NTC/ISO 27000:2013	Estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) publicada en el año 2013
Serie NTC/ISO 27000:2022	Estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) publicada en el año 2022
ISO31000:2018	Gestión del Riesgo. Principios y directrices
Guía de administración del riesgo y el diseño de controles en entidades públicas – Versión 6	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública

Fuente: Elaboración propia. Corporación Autónoma Regional de Caldas.

5. OBJETIVO GENERAL

Determinar las acciones de tratamiento de riesgos de seguridad y privacidad de la información, mediante la identificación, análisis, valoración y tratamiento de los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información, para prevenir su materialización y/o reducir los impactos negativos en la gestión institucional.

6.1. Objetivos específicos

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Identificar nuevos riesgos de la Corporación en la ejecución de sus funciones, alineados al propósito superior mega meta, objetivos de entidad y gobierno corporativo.
- Realizar seguimiento y validación sobre la gestión de riesgos identificados.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información, seguridad Digital y ciberseguridad.

6. ALCANCE DEL DOCUMENTO

Se dispone de la política y metodología para la administración de riesgos de Corpocaldas para la gestión de riesgos de seguridad de la información, la cual tiene fundamento en la Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6 del DAFP.

Para llevar a cabo el plan de tratamiento de riesgos para el presente año, se contempla la definición de actividades dentro de un cronograma listado en el presente documento, las cuales buscan realizar actividades que conlleven a mitigar los riesgos identificados por medio de la Matriz de riesgos de seguridad de la Información y llevar dichos riesgos a niveles aceptables.

El plan de trabajo involucra actividades con lideres de procesos y subprocesos, teniendo en cuenta el nivel de responsabilidad y compromisos para el manejo de los riesgos y los controles para mitigar dicho riesgo. Así mismo se hará el seguimiento y validación de los controles implementados, de acuerdo con el proceso de gestión del riesgo de seguridad de la información y de acuerdo con las etapas del Modelo de Seguridad y Privacidad de la información (MSPI):

Imagen 2. Etapas de MSPI en la gestión de riesgo

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Tomado de: la Guía de gestión de riesgos disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

Además, se cuenta con el registro de activos de información como base documental para la identificación, valoración y tratamiento de los riesgos de la Corporación.

7. MODELO DE PLANEACIÓN Y CRONOGRAMA DE EJECUCIÓN

Para dar cumplimiento al ciclo de riesgo, el cronograma se establece con temporalidad anual, así los riesgos de seguridad de la información y seguridad digital identificados se reflejarán en la Matriz de Riesgos de seguridad de la información Institucional, donde se establecerán las acciones de control y se hará un control semestral, la oficina de Tecnologías de la información apoyará el proceso de definición de los controles con los líderes de cada uno de los líderes de procesos y subprocesos:

Tabla 2: Cronograma de actividades

Actividad	Producto	Fecha inicio	Fecha fin	Responsable
Aprobar la matriz de riegos de seguridad de la información	Matriz de riegos de seguridad de la información aprobada en comité Institucional de Gestion y desempeño	1/02/2024	15/03/2024	Oficial de seguridad de la información
Realizar seguimiento a la implementación de controles de acuerdo con la matriz de riesgos y verificar la evidencia de los mismos	Matriz de seguimiento de controles Almera (SGI)	1/04/2024	29/11/2024	Oficial de seguridad de la información Control interno Mejora continua
Identificar nuevos controles para el tratamiento de riesgos residuales.	Propuesta de controles para riegos residuales	1/06/2024	28/10/2024	Oficial de seguridad de la información Líderes de subdirecciones Gestión de TIC

Actividad	Producto	Fecha inicio	Fecha fin	Responsable
Identificar nuevos riesgos de seguridad de la información y actualizar la matriz con líderes de subdirecciones y procesos.	Matriz de riesgos en Almera (SGI) actualizada	1/08/2023	28/12/2024	Oficial de seguridad de la información Líderes de subdirecciones
Elaborar y presentar informe de avance de implementación del plan institucional de tratamiento de riesgos	Informe de avance	7/11/2025	12/12/2025	Oficial de seguridad de la información Gestión de TIC

8. SEGUIMIENTO Y CONTROL

El comité de gestión y desempeño realizara seguimiento al cumplimiento del plan a través de la aplicación del siguiente indicador:

Nombre del Indicador:	Porcentaje de cumplimiento del plan institucional
Medición:	Numero de acciones ejecutadas/numero de acciones proyectadas

Control de cambios

VERSION	FECHA APROBACION	RESPONSABLE	DESCRIPCION DEL CAMBIO
V1	31/01/2024	Rubén Darío Jaramillo Parra -	Creación del documento.