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

CORPORACIÓN AUTÓNOMA REGIONAL DEL GUAVIO – CORPOGUAVIO

Enero 2025

INTRODUCCIÓN

La seguridad y la privacidad de la información son pilares fundamentales para garantizar la integridad, confidencialidad y disponibilidad de los datos en cualquier organización. En el caso de **CORPOGUAVIO**, como entidad ambiental comprometida con la gestión sostenible de los recursos naturales y el desarrollo regional, es imprescindible implementar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que se alinee con la normatividad vigente en Colombia, incluyendo los lineamientos establecidos en el Decreto 1377 de 2013, la Ley 1581 de 2012 sobre Protección de Datos Personales, y el Esquema de Seguridad de la Información contemplado en la Ley 1712 de 2014 (Ley de Transparencia).

Este plan tiene como objetivo mitigar los riesgos asociados al tratamiento de la información sensible, operativa y estratégica de la Corporación, mediante la identificación, valoración y aplicación de controles técnicos, administrativos y físicos adecuados. Para ello, se adopta un enfoque basado en la gestión de riesgos, siguiendo estándares internacionales como la norma ISO/IEC 27001 y las recomendaciones del Manual de Seguridad y Privacidad de la Información para Entidades Públicas.

En este contexto, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para CORPOGUAVIO busca no solo proteger los activos de información y garantizar la continuidad operativa, sino también fomentar la confianza de las partes interesadas, incluyendo comunidades, aliados estratégicos y entidades gubernamentales. A través de esta estrategia, se pretende fortalecer el cumplimiento normativo, la protección de datos personales y la implementación de una cultura de seguridad en todos los niveles de la organización.

Este documento detalla las acciones específicas que la Corporación llevará a cabo para gestionar los riesgos identificados, priorizando aquellos que tengas un mayor impacto sobre los objetivos estratégicos de CORPOGUAVIO, en pro de asegurar un manejo responsable, transparente y eficiente de la información.

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)
- **Confidencialidad:** Es la propiedad de la información, por la que se garantiza su acceso única y exclusivamente a personal autorizado a acceder a dicha información.
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos
- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad

OBJETIVO

Establecer un marco integral para la gestión de riesgos de seguridad y privacidad de la información en CORPOGUAVIO, mediante la implementación de controles que permitan mitigar los riesgos identificados, garantizar la protección de los datos sensibles, operativos y estratégicos, y asegurar el cumplimiento de la normatividad vigente, fomentando una cultura organizacional basada en la transparencia, la confianza y la seguridad.

OBJETIVOS ESPECÍFICOS

- Identificar y priorizar los riesgos asociados a la seguridad y privacidad de la información en CORPOGUAVIO, mediante el análisis de amenazas, vulnerabilidades y posibles impactos en los activos críticos de la organización
- Definir e implementar controles técnicos, administrativos y físicos alineados con los estándares internacionales y la normatividad vigente, que permitan mitigar los riesgos identificados y garantizar la confidencialidad, integridad y disponibilidad de la información
- Promover una cultura organizacional de seguridad de la información a través de la capacitación del personal, la sensibilización de las partes interesadas y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de CORPOGUAVIO aplica a todos los procesos, sistemas, personas y activos de información que intervienen en el manejo, almacenamiento, transmisión y protección de datos dentro de la entidad. Incluye la identificación, evaluación y mitigación de riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información, a incluir tanto datos sensibles como información operativa y estratégica.

Este plan comprende todas las áreas y dependencias de CORPOGUAVIO, así como los servicios tercerizados, aliados estratégicos y proveedores que gestionen información en nombre de la Corporación. Su implementación está alineada con los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI) y con la normatividad aplicable en Colombia, como la Ley 1581 de 2012, el Decreto 1377 de 2013, y las normas relacionadas con el Esquema de Seguridad de la Información en entidades públicas.

Asimismo, el alcance del plan incluye la aplicación de controles preventivos, detectivos y correctivos, así como la mejora continua de las adoptadas, con el fin de garantizar un entorno seguro para la información y reducir la materialización de riesgos que puedan comprometer los objetivos estratégicos. y operativos de CORPOGUAVIO.

METODOLOGIA

La metodología para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en CORPOGUAVIO se basa en un enfoque sistemático y estructurado, alineado con las mejores prácticas y la normatividad vigente. Esta se llevará a cabo en las siguientes fases

1. **Identificación de los riesgos**

   En esta fase se llevará a cabo un análisis exhaustivo de los activos de información, identificando tanto los riesgos internos como externos que podrían afectar la seguridad y privacidad de los datos. Se utilizarán herramientas de evaluación y matrices de riesgos para categorizar y clasificar las amenazas y vulnerabilidades asociadas a cada activo

2. **Evaluación y análisis de riesgos**

   Los riesgos identificados serán evaluados en función de su probabilidad de

ocurrencia y el impacto potencial en los objetivos de CORPOGUAVIO. Esta evaluación se realizará utilizando metodologías de análisis cualitativo y cuantitativo, como la matriz de probabilidad e impacto, y se establecerá una prioridad para su tratamiento.

3. **Selección de controles de seguridad**

   En esta fase se determinarán los controles adecuados para mitigar los riesgos, calculando en las recomendaciones de estándares internacionales como ISO/IEC 27001 y las directrices nacionales sobre seguridad de la información. Los controles abarcarán medidas preventivas, detectivas y correctivas, adaptadas a las necesidades específicas de CORPOGUAVIO.

4. **Implementación de controles**

   Se procederá con la implementación de los controles de seguridad seleccionados, asignando responsabilidades claras a cada área de la organización. Además, se garantizará que todos los miembros del personal involucrado reciban la capacitación adecuada para aplicar y mantener los controles establecidos.

5. **Monitoreo y revisión continua**

   Una vez implementadas los controles, se establecerán mecanismos de monitoreo para evaluar su efectividad en la mitigación de los riesgos. Esto incluirá auditorías periódicas, revisión de desempeño y actualizaciones según sea necesario, adaptando el plan a nuevas amenazas y cambios en la normatividad

6. **Mejora continua**

   El proceso de tratamiento de riesgos se abordará de manera dinámica, promoviendo la mejora continua del sistema de gestión de seguridad de la información. A través de retroalimentación, lecciones aprendidas y la implementación de nuevas tecnologías y procedimientos, se ajustarán y optimizarán los controles para garantizar su efectividad a largo plazo.

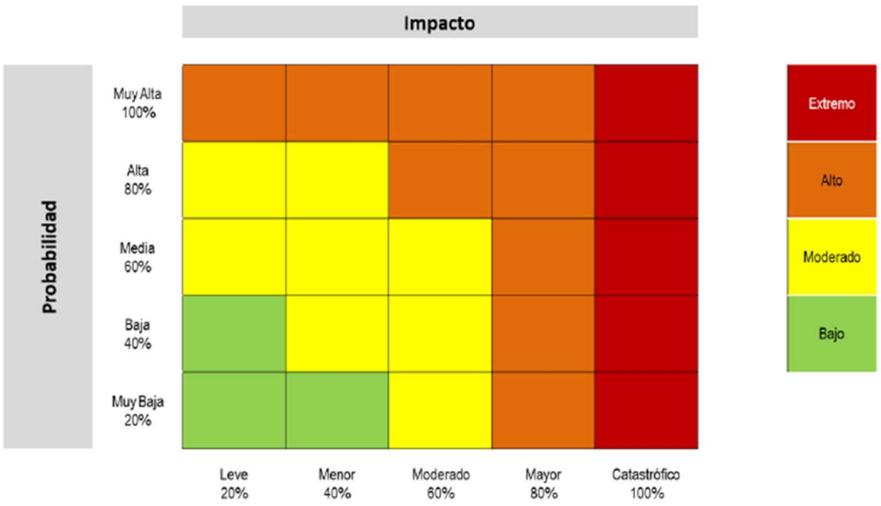
Esta metodología garantiza que el tratamiento de riesgos se realice de manera efectiva, permitiendo a CORPOGUAVIO proteger la información de manera proactiva, cumplir con la normatividad vigente y fomentar una cultura organizacional de seguridad y privacidad.

Análisis de los riesgos

ANALISIS DE RIESGOS	
Proceso	Proceso en el cual se encuentra diseñado el riesgo en concordancia con el macroproceso (Planificacion estrategica - Tecnologia de la informacion y las telecomunicaciones - Gerencia del sistema de gestion y control SIGYCO - Gestion de recursos - Gestion de la informacion y las comunicaciones).
Objetivo	Describcion clara del objetivo del proceso, en concordancia con el formato de caracterizacion de procesos en el cual se encuentra identificado los riesgos.
Alcance	Delimitacion del proceso al cual se esta proyectando o dentro del cual se desarrollo el riesgo a mitigar.
Riesgo de Seguridad de la Informaciòn	Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
Referencia	Es el consecutivo de los riesgos, lo que permite llevar una trazabilidad de los riesgos. Esta información la debe administrar la Subdireccion de planeación.
Activo de procesos	Para la identificación de los riesgos de seguridad de la Información, los procesos deben realizar inicialmente la identificación de Activos de Información acorde con los lineamientos establecidos en la GE-SIGYCO-GI-AR Guia para la Administración del Riesgo en Corpoguavio . En este momento es importante establecer cuáles son los activos críticos de los procesos.se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información: • Pérdida de la confidencialidad • Pérdida de la integridad • Pérdida de la disponibilidad
Descripcion del riesgo	Como parte del análisis de riesgos de seguridad de la información, es importante identificar tanto los riesgos como las amenazas que podrían afectar los activos. También es esencial que comprendas el significado de cada uno de estos términos. - Los riesgos se refieren a la probabilidad de que una vulnerabilidad en el sistema sea explotada por un atacante. Por ejemplo, un riesgo es la posibilidad real de que un virus informático infecte los sistemas y provoque que estos fallen. - Las amenazas son todas aquellas acciones malintencionadas o eventos que pueden comprometer la seguridad de la información. Estos pueden incluir ciberataques, phishing, desastres naturales o errores humanos. Por lo tanto, es importante que se identifiquen todas las amenazas potenciales para determinar el nivel de riesgo que podrían afectar los

Probabilidad inherente	Muy baja	La actividad que conlle va el riesgo se ejecuta como máximos 2 veces por año	20%
	Baja	Baja La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
	Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces	80%
	Muy alta	AltaLa actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%
Impacto Inherente	Leve - 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
	Menor - 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, deconocimiento general nivel interno, de junta directiva y
	Moderado - 60	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
	Mayor - 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo,
	Catastrofico - 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Matriz de calor (niveles de severidad del riesgo)



MATRIZ DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

Rerferencia	Activo	Descripcion del riesgo	Amenaza	Tipo	Probabilidad inherente	%	Impacto Inherente	%	Zona de riesgo inherente	VALORACION DEL RIESGO				PLAN DE ACCION				
										No.Control	Responsable	Accion	Complemento	Plan de accion	Responsable	Fecha de implementacion	Fecha seguimiento	Estado

1	Pérdida de la integridad	Existe el riesgo de que individuos no autorizados puedan acceder a información sensible o estratégica de CORPOGUAVIO, ya sea a través de fallas en los controles de autenticación, credenciales comprometidas o vulnerabilidades en el sistema de gestión de accesos. Esto	Acciones no autorizadas	4.Lugar	MUY BAJA	20	MAYOR	80	Alto	1	Profesional Tics	implementar controles de acceso	*Solicitud de parametros minimos requeridos para la creación de contraseñas seguras. *Formato de solicitud de creación de cuentas para el acceso de los diferentes aplicativos que manejara el contratista *Divulgación de Informacion relacionada con las politica	Verificar que los accesos asignados cumplan con los requisitos descritos en el Procedimiento creacion de cuentas de usuarios.	Oficina de TICS	2025-01-15	2025-06-14	En curso

		podría comprometer la confidencialidad de los datos y generar posibles filtraciones o uso indebido de la información.										de seguridad y privacidad de la infomación.					

2	Pérdida de la confidencialidad	CORPOGUAVIO podría ser objetivo de ataques cibernéticos, como ransomware, phishing o malware, que podrían afectar la disponibilidad de los sistemas de información o la integridad de los datos. Estos ataques pueden derivar en la interrupción de los servicios, pérdida	Acciones no autorizadas	2. software	BAJA	40	MAYOR	80	Alto	1	Profesional Tics	Instalar y mantener actualizado un software de protección contra malware y firewall en todos los sistemas y dispositivos.	Implementar sistemas de detección y prevención de intrusiones (IDS/IPS) para monitorear y bloquear actividades sospechosas en la red Capacitar a los empleados sobre prácticas seguras en el uso de correos electrónicos y navegación en línea, para prevenir ataques	Verificar que los equipos y aplicativos de la entidad cuenten con un sistema de antivirus actualizado	Oficina de TICS	2025-01-15	2025-06-14	En curso

		de datos importantes o el secuestro de información crítica, lo que afecta directamente las operaciones de la entidad													

3	Pérdida de la disponibilidad	Las interrupciones en los servicios de tecnología debido a problemas técnicos, cortes de energía, ataques cibernéticos o desastres naturales pueden afectar la capacidad de CORPOGUAVIO para operar de manera eficiente y cumplir con sus objetivos estratégicos	Pérdida de los servicios esenciales	4.Lugar	MUY BAJA	20	MODERADO	60	Moderado	1	Profesional Tics	Implementar un sistema de copias de seguridad periódicas y automatizadas para todos los datos críticos, asegurando su almacenamiento en ubicaciones seguras.	Utilizar tecnología redundante, como sistemas de almacenamiento en la nube con alta disponibilidad, para minimizar la probabilidad de pérdida de datos. Monitorear proactivamente la infraestructura tecnológica para identificar fallas y actuar de manera preventiva.	Realizar Copias de seguridad según Procedimiento Copias de seguridad Corporativas, Realizar Mantenimiento Preventivo y Correctivo a la infraestructura tecnologia de la entidad	Oficina de TICS	2025-01-15	2025-06-14	En curso