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

CORPORACIÓN AUTÓNOMA REGIONAL DEL GUAVIO – CORPOGUAVIO

Enero 2026

INTRODUCCIÓN

La seguridad y la privacidad de la información constituyen pilares fundamentales para garantizar la confidencialidad, integridad y disponibilidad de los datos que soportan la gestión institucional. En el caso de la Corporación Autónoma Regional del Guavio – CORPOGUAVIO, como entidad ambiental encargada de la gestión sostenible de los recursos naturales y del desarrollo regional, resulta indispensable contar con un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que permita proteger de manera adecuada sus activos de información.

Este plan se formula en concordancia con la normatividad vigente en Colombia, en especial con la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales, la Ley 1712 de 2014 de transparencia y acceso a la información pública, así como con los lineamientos establecidos en el Modelo y el Manual de Seguridad y Privacidad de la Información para Entidades Públicas. Así mismo, adopta un enfoque basado en la gestión del riesgo, alineado con buenas prácticas y estándares internacionales como la norma ISO/IEC 27001.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como propósito principal identificar, analizar y mitigar los riesgos que puedan afectar la información sensible, operativa y estratégica de CORPOGUAVIO, mediante la definición e implementación de controles técnicos, administrativos y físicos acordes con el nivel de impacto y probabilidad de cada riesgo.

De esta manera, el plan busca no solo proteger los activos de información y apoyar la continuidad de los procesos institucionales, sino también fortalecer la confianza de las partes interesadas, incluyendo comunidades, aliados estratégicos y entidades del Estado. A través de su aplicación, CORPOGUAVIO reafirma su compromiso con el cumplimiento normativo, la protección de los datos personales y la consolidación de una cultura organizacional orientada a la gestión responsable, transparente y segura de la información.

Finalmente, este documento presenta las acciones y medidas que la Corporación implementará para el tratamiento de los riesgos identificados, priorizando aquellos que representan un mayor impacto sobre los objetivos estratégicos de la entidad, con el fin de garantizar un manejo eficiente y confiable 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

Gestionar y mitigar los riesgos de seguridad y privacidad de la información en CORPOGUAVIO, mediante la identificación, análisis, tratamiento y seguimiento de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando el cumplimiento normativo y la continuidad de los procesos institucionales.

OBJETIVOS ESPECÍFICOS

- Identificar y evaluar los riesgos asociados al tratamiento de la información institucional, considerando amenazas, vulnerabilidades e impactos sobre los procesos misionales, estratégicos y de apoyo de CORPOGUAVIO.
- Definir e implementar medidas de tratamiento de riesgos, a través de controles técnicos, administrativos y físicos, acordes con el nivel de riesgo identificado y alineados con la normativa vigente y el Modelo de Seguridad y Privacidad de la Información.
- Realizar seguimiento periódico a los riesgos de seguridad y privacidad de la información, con el fin de evaluar la efectividad de los controles implementados y promover la mejora continua en la gestión de la seguridad de la información.

ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a todos los activos de información de CORPOGUAVIO, independientemente de su formato, medio de almacenamiento o procesamiento, e incluye información física y digital, sistemas de información, plataformas tecnológicas y servicios en la nube utilizados por la entidad.

El alcance del plan comprende a todas las dependencias, procesos y proyectos institucionales, así como al talento humano, contratistas, proveedores y terceros que, en el desarrollo de sus funciones, tengan acceso, manejen o traten información de la Corporación.

De igual forma, el plan abarca la identificación, análisis, tratamiento y seguimiento de los riesgos asociados a la seguridad y privacidad de la información, considerando los entornos físicos, tecnológicos y organizacionales en los que se gestionan los activos de información 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.

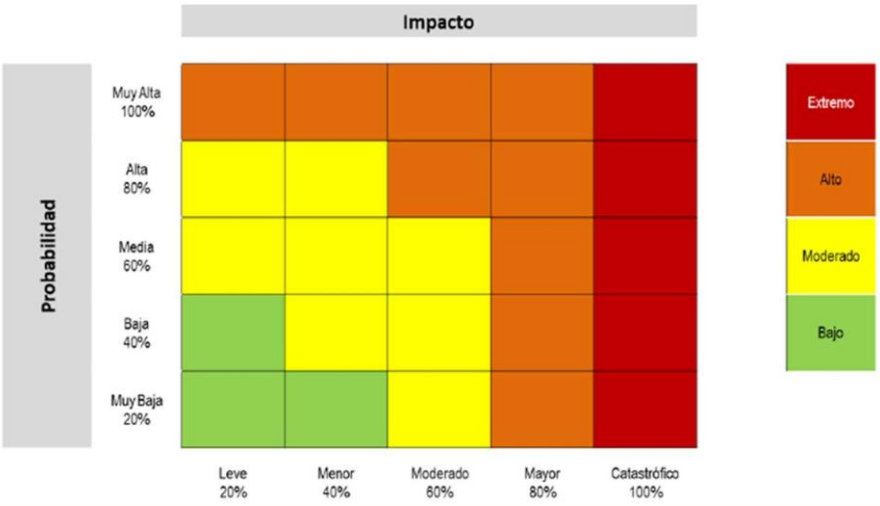
Esta metodología garantiza que el tratamiento de riesgos se realice de manera efectiva, permitiendo a CORPOGUAVIO proteger la información de manera proactiva, cumplir con la normatividad vigente y fomentar una cultura organizacional de seguridad y privacidad.

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 Información	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)



Corporación Autónoma Regional del Guavio - CORPOGUAVIO

MATRIZ DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

Proceso		CÓDIGO	VERSIÓN		FECHA
Objetivo		DE-SIGYCO-FT-MR	3		2025-01-29
alcance					

Referencia	Activo	Descripcion del riesgo	Amenaza	Tipo	Probabilidad inherente	%	Impacto Inherente	%	Zona de riesgo inherente	VALORACION DEL RIESGO																PLAN DE ACCION					
										No.Control	Descripcion del control	Responsable	Accion	Complemento	Atributos						Probabilidad residual	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento	Plan de accion	Responsable	Fecha de implementacion	Fecha seguimiento	Seguimiento	Estado
															Tipo	Implementacion	Calificacion	Documentacion	Frecuencia	Evidencia												
1	Pérdida de la integridad	Perdida de integridad de la información debido a acciones no autorizadas, por incumplimiento de las políticas de seguridad digital, así como la gestión inadecuada de los controles de acceso, protección de contraseñas y mecanismos de autenticación que permitan modificaciones no autorizadas en los aplicativos con los que cuenta la entidad.	Acciones no autorizadas	6. organización	MUY BAJA	20	MODERADO	60	Moderado	1	5.15. Control de acceso	Profesional Tics	Establecer y aplicar un procedimiento formal para la creación, modificación y eliminación de usuarios en los equipos y sistemas, con asignación de roles y permisos según el perfil de cada funcionario.	*Solicitud de parametros mínimos 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 información relacionada con las politica de seguridad y privacidad de la información.	Preventivo	Manual	40	Documentado	Continua	Con registro	12	MAY BAJA	12	LEVE	60	MODERADO	Reducir- Mitigar el Riesgo	Verificar que los accesos asignados cumplan con los requisitos descritos en el Procedimiento creacion de cuentas de usuario.	Oficina de TICS	2025-05-01	2025-12-31	Se realizo la creación de 230 usuarios en el primer cuatrimestre del año de los diferentes aplicativos que maneja la entidad segun el formato DE-TIC-FT-SCMCU Solicitud Creación y Mantenimiento de Cuentas, este formato es enviado por el lider del proceso y estipula a que aplicativos va a tener acceso el contratista. * Se actualiza de manera continua el Formato DE-TIC-FT-RCUI Registro Centralizado de Usuarios Institucionales con semaforizacion de terminacion de contrato(para tener un control oportuno del acceso a los aplicativos por parte de los contratistas) * Se verifica que las contraseñas creadas por los contratistas cumplan con los requisitos minimos	En curso
2	Pérdida de la confidencialidad	Perdida de confidencialidad por falta de respuesta de incidentes en seguridad de la información, los cuales pueden generar perdida de los servicios esenciales debido a la interrupción parcial o total de las operaciones institucionales a causa de ataques cibernéticos.	Pérdida de los servicios esenciales	3. red	BAJA	40	MODERADO	60	Moderado	1	5.26. Respuesta a incidentes de seguridad de la información	Profesional Tics	Actualizar y mantener vigente la licencia del firewall Fortinet de la entidad, garantizando la activación de servicios avanzados de seguridad (antimalware, filtrado web, IPS y protección contra ransomware), con el fin de fortalecer las capacidades de prevención y mitigación de ciberataques.	* Monitoreo y configuración permanente del firewall para asegurar que las políticas de seguridad estén correctamente aplicadas y alineadas con los riesgos institucionales.	Preventivo	Manual	40	Documentado	Continua	Con registro	24	BAJA	24	MENOR	60	BAJO	Reducir- Mitigar el Riesgo	Realizar la actualización de la licencia de Firewall de la entidad.	Oficina de TICS	2025-05-01	2025-12-31	Se realizó la verificación de la vigencia de la licencia del firewall Fortinet de la entidad, confirmando la correcta actualización y activación de los servicios avanzados de seguridad (antimalware, filtrado web, sistema de prevención de intrusiones – IPS y protección contra ransomware). Esta actualización garantiza que el dispositivo cuente con las últimas firmas y parches de seguridad, fortaleciendo así la capacidad institucional para prevenir, detectar y mitigar ciberataques.	En curso
3	Pérdida de la disponibilidad	Perdida de disponibilidad de información institucional por compromiso de la información a causa de la ausencia o inadecuada gestión de copias de seguridad, lo que puede afectar la integridad y continuidad de los servicios de la entidad.	Compromiso de la información	1, hardware	MEDIA	60	MENOR	40	Moderado	1	5.33. Protección de registros	Profesional Tics	Implementar y mantener un sistema de copias de seguridad periódicas de la información crítica de la entidad, almacenadas en medios seguros y fuera de línea, acompañado de pruebas de restauración programadas, con el fin de gasantizar la disponibilidad y continuidad de los servicios en caso de pérdida o incidente de seguridad.	Establecer la periodicidad de las copias de seguridad (diarias, semanales o mensuales, según el tipo de información) para garantizar la disponibilidad de datos actualizados. Diseñar y aplicar un procedimiento formal de copias de seguridad, que defina responsables, almacenamiento, protección de la información y tiempos de retención. Realizar pruebas periódicas de restauración para verificar	Preventivo	Manual	40	Documentado	Continua	Con registro	36	BAJA	36	MENOR	40	BAJO	Aceptar el Riesgo	Realizar las copias de seguridad segun procedimiento de la entidad.	Oficina de TICS	2025-09-01	2025-12-31	Se realizaron las diferentes copias de seguridad periódicas de la información perteneciente a los aplicativos (PCT, SIDCAR, SIGYCO, BASES DE DATOS), según procedimiento de copias de seguridad, al igual se verifico las copias de seguridad realizadas por el prestador de servicio de Hosting, garantizando su almacenamiento	En curso