Plan

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

2026

Gobierno de Procesos

Proceso	Gestión TICS
Tipo de proceso	Procesos de Apoyo
Área Responsable	Grupo de TICS
Vigencia	2026

Control de Emisión

	NOMBRE	CARGO
APROBÓ	MG. Andrés Guzmán Morales	Presidente
REVISÓ	Rafael Alberto Velasquez Garavito	Jefe Oficina Planeación
REVISÓ	Alejandra Bernal Wesso	Coordinadora SIGCA
REVISÓ	Luisa Carolina Sabas Echavarria	Vicepresidenta Administrativa
ELABORÓ	Te. Jessica Tatiana Cifuentes Dimas	Coordinadora Grupo TICS

Matriz para Control de Cambios

Versión	Fecha	Motivo
1	19-JUN-2026	Este documento homologa al documento PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN , Código: PLN-7-00-002 , Versión: 9, de acuerdo con la nueva estructura documental definida en el SIGCA.

OBJETIVO

Espacio intencionalmente en blanco

DESARROLLO

Para la gestión de riesgos en seguridad y privacidad de la información y seguridad digital se toma como referencia la metodología establecida en el MAN-OPLAI-002 Manual del Sistema Integral de Gestión de Riesgos CIAC y las metodologías relacionadas con seguridad digital y ciberseguridad.

1. IDENTIFICACIÓN DEL RIESGO

La identificación de los riegos busca una relación de los posibles puntos de peligro, lo que se identifique será analizado, lo que no quedará como riesgo oculto o ignorado.

Para la identificación de riesgos de seguridad de la información digital, es necesario identificar los activos de la información, teniendo en cuenta los siguientes pasos:

1. Listar los activos por cada proceso
2. Identificar el dueño de los activos
3. Clasificar los activos
4. Clasificar la información
5. Determinar la criticidad del activo
6. Identificar si existe infraestructura crítica cibernética

A nivel de seguridad de la información se identifica los siguientes tres (3) tipos riesgos:

- Pérdida de confidencialidad
- Pérdida de integridad
- Pérdida de la disponibilidad

Así mismo, se debe analizar las posibles amenazas y vulnerabilidades que podrían causar la materialización de cada riesgo, ocasionando pérdidas o alteración en el funcionamiento de la Corporación o poniendo en riesgo el cumplimiento de los objetivos corporativos.

Se debe tener en cuenta que la sola presencia de una vulnerabilidad no causa daños por sí misma, debido a que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

A continuación, se muestra ejemplos de vulnerabilidades y amenazas, de acuerdo con el tipo de activo.

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Tomado de la Guía paras la administración del riesgo y el diseño de controles en entidades públicas Vr. 6

2. VALORACIÓN DEL RIESGO

Previo a la valoración del riesgo de seguridad de la información y seguridad digital, se debe contar con el inventario de activos de información, que es la base para la valoración de los riesgos.

La valoración es la determinación del costo que supondría recuperarse de una incidencia que dañe el activo.

La valoración puede ser cuantitativa o cualitativa. La valoración se puede ver desde la

perspectiva de la necesidad de proteger, pues cuanto más valioso es un activo, mayor nivel de protección requiere para que no se vea afectada su confidencialidad, integridad o su disponibilidad, según sea pertinente.

3. IDENTIFICACIÓN Y EVALUACIÓN DE LOS CONTROLES EXISTENTES

Una vez identificados y valorados los riesgos, se debe identificar y evaluar los controles existentes, los cuales se toman como referencia el Anexo A de la Norma ISO IEC 27001, como insumo base para mitigar los riesgos de seguridad digital y seguridad de la información, siempre y cuando se ajusten al análisis de riesgos.

4. TRATAMIENTO DEL RIESGO

Una vez identificados los riesgos, se define el tratamiento para cada uno de los riesgos analizados y evaluados, que involucra la selección de una o más actividades de control para disminuir sus consecuencias (impacto) o la frecuencia y así establecer si el nivel de riesgo residual (después de controles) se encuentra dentro de los niveles de aceptación por parte de la Corporación y que no se vea afectada la disponibilidad, integridad y confidencialidad de la información.

Para el tratamiento del riesgo se debe tomar alguna de las siguientes opciones:

- **Aceptar el riesgo:** Cuando se reconoce la existencia del riesgo y sus consecuencias (provisión de las posibles pérdidas), sin necesidad de tomar otras medidas de control diferentes a las que poseen. Algunos riesgos serán aceptados excepcionalmente mediante la aprobación del dueño del proceso, siempre y cuando el riesgo esté ubicado de acuerdo con el apetito de riesgo de la Corporación. Se debe realizar un seguimiento continuo del riesgo.

- **Evitar el riesgo:** Se evita el riesgo si se decide no proceder con la actividad que probablemente generaría el riesgo, utilizando un activo, servicio o producto distinto o modificando el proceso, de manera que las amenazas originales ya no lo afecten.

- **Transferir el riesgo:** Esto involucra que un externo a la entidad soporte o comparta el riesgo. Los mecanismos pueden incluir el uso de contratos, arreglos de seguros y estructuras organizacionales tales como sociedades entre otros.

- **Reducir o mitigar el riesgo:** Actividades y medidas tendientes a reducir la probabilidad y/o minimizar la severidad de su impacto. Se consigue mediante la

optimización de los procedimientos y la implementación de controles (prevención, planificación).

5. MATERIALIZACIÓN

En el caso de materializarse un riesgo se debe seguir el Instructivo Gestión de Incidentes de Seguridad de la Información(PRO-VICAD-032), y se deberá analizar el riesgo y realizar la respectiva valoración posterior a la materialización, dejando el registro en el mapa de riegos. Cuando se materialice un riesgo que no se haya identificado, deberá ser reportado e iniciar el respectivo procedimiento de valoración del riesgo.

CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	RESPONSABLE	FECHA DE INICIO	FECHA FIN	RESULTADO
Identificar y/o actualizar activos de información críticos según los lineamientos del MinTIC	Grupo TICS Grupo Administrativa Vicepresidentes, Jefes, Gerentes y Coordinadores	15/04/2026	31/12/2026	Inventario actualizado y clasificado
Actualizar el documento del registro de activos de información de la vigencia 2024 para publicación en datos abiertos de acuerdo con la Ley 1712 de 2013	Grupo TICS Grupo Administrativa Vicepresidentes, Jefes, Gerentes y Coordinadores	15/04/2026	31/07/2026	Documento actualizado en el portal de datos abiertos
Realizar talleres de identificación de riesgos con Vicepresidentes, Jefes, Gerentes y Coordinadores y	Grupo TICS Grupo Administrativa Profesional de Riesgos	15/04/2026	30/10/2026	Listado de asistencia

funcionarios clave				
Realizar y actualizar las políticas y reglas del NAC	Ingeniero de Infraestructura y Seguridad Informática	2/03/2026 1/06/2026 1/09/2026 1/12/2026	31/03/2026 30/06/2026 30/09/2026 31/12/2026	Políticas y reglas actualizadas
Optimizar el SIEM mediante Playbooks inteligentes	Ingeniero de Infraestructura y Seguridad Informática Profesionales del SOC	2/03/2026 1/06/2026 1/09/2026 1/12/2026	31/03/2026 30/06/2026 30/09/2026 31/12/2026	Reporte del proveedor
Desarrollar e implementar campañas de sensibilización en ciberseguridad	Grupo TICS Grupo CECSA	2/03/2026 1/06/2026 1/09/2026 1/12/2026	31/03/2026 30/06/2026 30/09/2026 31/12/2026	Formato de capacitaciones LMS y reporte del personal capacitado. O formato de asistencia a la sensibilización

ANEXOS

N/A