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

IDEA+ S.A.S

2025

CREDIANTIOQUIA
Le damos crédito a tus sueños

CONTENIDO

1 INTRODUCCIÓN

La Entidad ha implementado la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6, la cual establece los criterios para la identificación, evaluación, control y tratamiento de los riesgos de seguridad y privacidad de la información. Con ayuda de herramientas como la Matriz de Riesgos de la Entidad, se puede identificar la probabilidad inherente a la cual están expuestos los riesgos de seguridad y privacidad de la información, al igual que los controles asociados a los riesgos identificados y finalmente se lleva el inventario de los planes de acción que se deban aplicar para fortalecer los controles que nos ayudan a mitigar dichos riesgos.

2 DEFINICIONES[1]

- **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).
- **Probabilidad**: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata**: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz**: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Consecuencia**: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Punto de Riesgo**: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia,

[1] Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6.

explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

- **Control**: Medida que permite reducir o mitigar un riesgo.
- **Riesgo Inherente**: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual**: El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Factores de Riesgo**: Son las fuentes generadoras de riesgos.
- **Confidencialidad**: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de exactitud y completitud.
- **Disponibilidad**: Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Vulnerabilidad**: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
- **Activo**: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

3 OBJETIVOS

- Ejecutar los planes de acción identificados en la última evaluación de riesgos de la Entidad.
- Aplicar la metodología definida para la identificación y evaluación de riesgos de seguridad y privacidad de la información.
- Fortalecer los mecanismos relacionados con seguridad y privacidad de la información.
- Cumplir con la regulación y normas técnicas colombianas relacionadas con la materia.

4 ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información inicia con la identificación y evaluación de los riesgos, la cual nos permite como resultado hacer el levantamiento de los respectivos planes de acción que debe implementar la Entidad para disminuir la probabilidad de materialización de los riesgos o minimizar su impacto.

5 IDENTIFICACIÓN DE RIESGOS

En la evaluación de riesgos desarrollada en el III cuatrimestre de 2024, se identifican dos (2) riesgos, los cuales se exponen a continuación:

No. DEL RIESGO	PROCESO:	RIESGO
R14	Gestión de Tecnología	Pérdida de la disponibilidad por ataque cibernético a causa de fallas en los sistemas de seguridad de la entidad
R15	Gestión de Tecnología	Pérdida de la integridad por robo de información debido al acceso de la misma sin controles y perfiles.

Los cuales producto de la evaluación de los controles se identifica el tratamiento que se debe llevar a cabo:

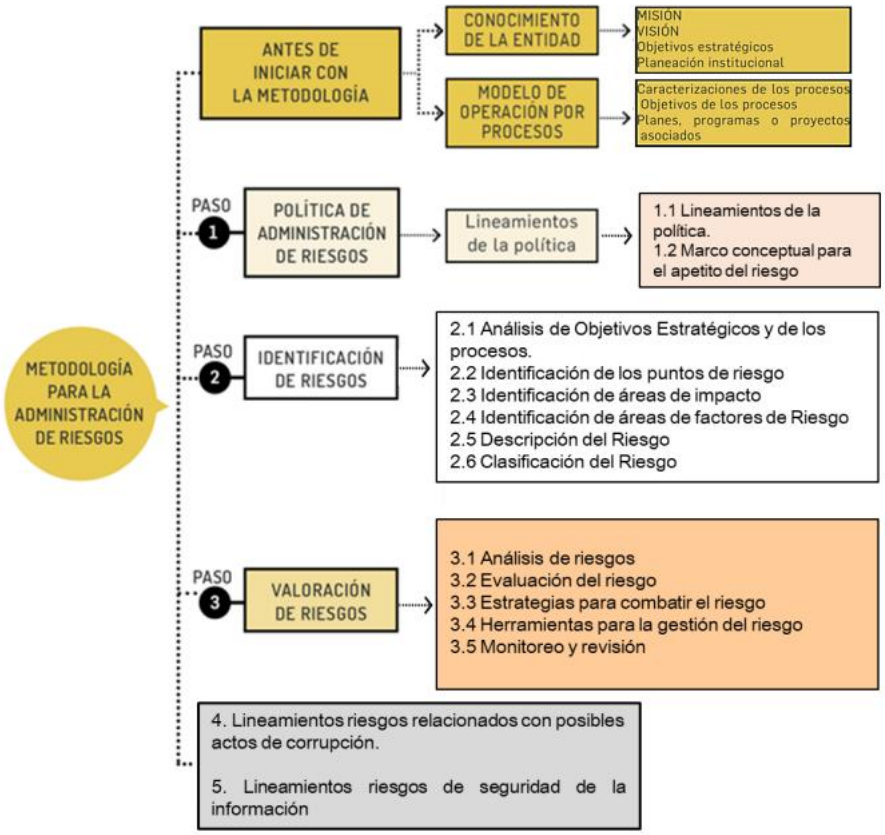
No. DEL RIESGO	¿Requiere Plan de Acción?	Tratamiento	Determine el tratamiento a seguir
R14	Requiere Plan de Acción	Reducir_mitigar_Transferir_Evitar	Reducir_Mitigar
R15	Requiere Plan de Acción	Reducir_mitigar_Transferir_Evitar	Reducir_Mitigar

6 PLAN DE ACCIÓN

Los planes para el tratamiento de los riesgos relacionados con seguridad y privacidad de la información contemplan las actividades que se desarrollaran en pro de mitigar los riesgos sobre los activos de información de la Entidad, a continuación, se detallan los planes de acción:

Descripción de la Acción, basado en el análisis de causas	Responsable (Cargo)	Fecha de Inicio	Fecha de Finalización
18/12/2024: 1. Monitorear el dispositivo de seguridad de red. 2. Supervisar las terminales para detectar infecciones en dispositivos concretos. 3. Solicitar las políticas de seguridad de la información y ciberseguridad del proveedor de la plataforma operativa y analizar si cumplen con los estándares que necesita la Entidad. 4. Establecer la política de seguridad de la información y ciberseguridad de la Entidad. 5. Desarrollar indicadores y KPI´s, relacionados con Ciberseguridad.	Profesional Tecnología y Analítica de Datos	10/09/2024	30/03/2025
30/08/2024: 1. Desarrollar un análisis de las aplicaciones que se utilizan en la entidad, para otorgar el acceso y permisos, según las funciones y necesidades de cada colaborador. 2. Diseñar los roles y perfiles, para el acceso, manejo y extracción de la información. **06/12/2024:** 3. Documentar el rol y perfil de acceso a la información.	Profesional Tecnología y Analítica de Datos	10/09/2024	30/03/2025

7 METODOLOGÍA[2]



[2] Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

8 RECURSOS

La Entidad pone a disposición los siguientes recursos, en compromiso con un efectivo tratamiento de los riegos de la entidad y el cumplimiento de los planes de acción.

Recursos	Variable
Humanos	Profesional Tecnología y Analítica de Datos.
Técnicos	· Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6. · ISO 27001. · ISO 31000:2018. · Matriz de Riesgos de la Entidad.
Logísticos	Equipos informáticos. Aplicaciones y softwares.

9 MEDICIÓN

Dentro de la metodología definida se hará seguimiento mensual al avance y ejecución de los planes de acción definidos en el punto 6 del presente documento, registrando esta gestión en la Matriz de Riesgos de la Entidad la cual deberá ser soportada con las respectivas evidencias que aporte el responsable asignado al plan de acción.