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

VIGENCIA 2026

Carrera 11 No 10 – 55 Esquina
Villagorgona (Candelaria)
Teléfono: (+57 2) 260 1403
www.emcandelaria.gov.co
contactenos@emcandelaria.gov.co
Valle del Cauca - Colombia

Alcaldía de Candelaria
Valle del Cauca, Colombia

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el contexto actual, en el cual la información se ha consolidado como uno de los activos estratégicos más importantes para las organizaciones, la adecuada gestión de los riesgos asociados a la seguridad y privacidad de la información se constituye en un elemento fundamental para garantizar la continuidad de la operación, la protección de los datos sensibles y el cumplimiento del marco legal y regulatorio aplicable. Para EMCANDELARIA S.A.S. E.S.P., entidad comprometida con la prestación eficiente y transparente de los servicios públicos, resulta indispensable contar con un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información alineado con los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

Este plan tiene como propósito identificar, evaluar, tratar y realizar seguimiento a los riesgos relacionados con la información y los sistemas que la soportan, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de los datos institucionales. Así mismo, busca asegurar el cumplimiento de los principios de gestión pública, la normativa vigente y la protección de los derechos de los ciudadanos, contribuyendo al fortalecimiento del control interno y a la mejora continua de la gestión institucional.

2. OBJETIVOS

2.1. GENERAL

Diseñar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de EMCANDELARIA S.A.S. E.S.P., en el marco de los planes institucionales del Modelo Integrado de Planeación y Gestión – MIPG, que permita identificar, evaluar, tratar y monitorear los riesgos asociados a la gestión de la información, garantizando la protección de los datos sensibles, el cumplimiento del marco normativo vigente y la continuidad operativa de la entidad.

2.2. ESPECÍFICOS

- **Identificar y categorizar los activos de información críticos de EMCANDELARIA S.A.S E.S.P.**, así como los riesgos asociados a su seguridad y privacidad, mediante un análisis detallado de los procesos, sistemas y flujos de datos de la organización.

- **Evaluar el nivel de riesgo de los activos de información** utilizando metodologías estandarizadas, con el fin de priorizar las acciones de tratamiento y asignar recursos de manera eficiente para la mitigación de los riesgos identificados.
- **Diseñar e implementar medidas de control y tratamiento de riesgos** que incluyan políticas, procedimientos, herramientas tecnológicas y capacitaciones, para reducir la probabilidad e impacto de los riesgos de seguridad y privacidad de la información.
- **Establecer un sistema de monitoreo y mejora continua** que permita evaluar la efectividad de las medidas implementadas, actualizar el plan de tratamiento de riesgos de acuerdo con los cambios en el entorno operativo y normativo, y garantizar el cumplimiento de los objetivos institucionales en el marco del MIPG.

3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de EMCANDELARIA S.A.S. E.S.P. aplica a todos los procesos, sistemas, activos de información y al personal de la entidad, así como a los terceros que, en el desarrollo de sus actividades, tengan acceso, manejo o tratamiento de la información institucional. Este plan comprende la identificación, evaluación, tratamiento y monitoreo de los riesgos asociados a la seguridad y privacidad de la información, en alineación con los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG y los objetivos estratégicos de la entidad.

El alcance del plan incluye los siguientes componentes:

- **Procesos y áreas involucradas:** Gestión de la información, tecnologías de la información, talento humano, operaciones, financiera y demás áreas administrativas que intervienen directa o indirectamente en el manejo de la información institucional.
- **Activos de información:** Bases de datos, sistemas de información, infraestructura tecnológica, documentación física y digital, comunicaciones y cualquier otro activo que contenga información clasificada, sensible o confidencial.

- **Terceros:** Proveedores, contratistas y aliados estratégicos que interactúen con los sistemas de información o tengan acceso a información de EMCANDELARIA S.A.S. E.S.P., bajo los lineamientos y controles establecidos por la entidad.
- **Ciclo de vida del plan:** Comprende desde la identificación y análisis de los riesgos hasta la definición e implementación de controles, así como el seguimiento y monitoreo permanente, con revisiones periódicas que garanticen su efectividad y actualización continua.

El presente plan no contempla la gestión de riesgos correspondientes a ámbitos distintos a la seguridad y privacidad de la información, tales como riesgos financieros, operativos o legales que no se encuentren directamente relacionados con el tratamiento y protección de los datos.

4. MARCO NORMATIVO

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para EMCANDELARIA S.A.S E.S.P. se desarrolla en cumplimiento de las siguientes normativas y estándares nacionales e internacionales:

1. **Constitución Política de Colombia:**
    - Artículo 15: Protección del derecho a la intimidad y al habeas data.
    - Artículo 20: Derecho a la información y su protección.
2. **Ley 1581 de 2012 (Ley de Protección de Datos Personales):**
    - Establece los principios y obligaciones para el tratamiento de datos personales en Colombia.
    - Regula la recolección, almacenamiento, uso y circulación de información personal.
3. **Decreto 1377 de 2013:**
    - Reglamenta la Ley 1581 de 2012 y define los procedimientos para la autorización y tratamiento de datos personales.
4. **Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública):**

- Promueve la transparencia en la gestión de la información pública y establece mecanismos para su protección.

5. **Modelo Integrado de Planeación y Gestión (MIPG):**
   - Directrices para la gestión de riesgos en entidades públicas y privadas que prestan servicios públicos.
   - Enfoque en la mejora continua, la eficiencia y la efectividad en la gestión institucional.
6. **Norma ISO/IEC 27001:**
   - Estándar internacional para la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI).
   - Proporciona un marco para identificar, evaluar y tratar riesgos de seguridad de la información.
7. **Norma ISO/IEC 27701:**
   - Extensión de la ISO/IEC 27001 para la gestión de la privacidad de la información.
   - Establece requisitos para un Sistema de Gestión de Información de Privacidad (PIMS).
8. **Resolución 695 de 2020 (ANLA):**
   - Establece lineamientos para la gestión de riesgos ambientales y de información en el sector empresarial.
9. **Reglamentación interna de EMCANDELARIA S.A.S E.S.P.:**
   - Políticas y procedimientos internos relacionados con la seguridad de la información, privacidad y gestión de riesgos.

5. METODOLOGÍA

1. **Identificación de riesgos**: Análisis de los activos de información, amenazas y vulnerabilidades.
2. **Evaluación de riesgos**: Determinación del impacto y la probabilidad de los riesgos identificados.

3. **Tratamiento de riesgos**: Implementación de medidas para mitigar, transferir, evitar o aceptar los riesgos.
4. **Seguimiento y evaluación**: Monitoreo de las medidas implementadas y ajustes según sea necesario.
5. **Capacitación y sensibilización**: Formación de los servidores públicos en temas de seguridad y privacidad.

6. IDENTIFICACIÓN DE RIESGOS

- **Riesgos tecnológicos**: Ataques de ransomware, phishing, malware, vulnerabilidades en sistemas y aplicaciones.
- **Riesgos humanos**: Errores humanos, falta de capacitación, acceso no autorizado a la información.
- **Riesgos físicos**: Robo de equipos, desastres naturales, fallas en la infraestructura física.
- **Riesgos legales**: Incumplimiento de normativas de protección de datos, sanciones legales.

7. EVALUACIÓN DE RIESGOS

- **Impacto**: Evaluación del daño potencial que podría causar un riesgo.
- **Probabilidad**: Estimación de la posibilidad de que un riesgo se materialice.
- **Nivel de riesgo**: Determinación del nivel de riesgo basado en el impacto y la probabilidad.

8. TRATAMIENTO DE RIESGOS

- **Mitigación**: Implementación de controles de seguridad para reducir el impacto o la probabilidad de un riesgo.
- **Transferencia**: Transferencia del riesgo a un tercero mediante seguros o acuerdos contractuales.
- **Evitación**: Eliminación de la actividad o proceso que genera el riesgo.
- **Aceptación**: Aceptación del riesgo cuando el costo de mitigación es mayor que el impacto potencial.

9. SEGUIMIENTO Y EVALUACIÓN

- **Indicadores de seguimiento**: Tasa de incidentes de seguridad, nivel de cumplimiento de normativas, nivel de satisfacción de los servidores públicos.
- **Evaluación periódica**: Análisis de resultados y ajustes al plan según las necesidades identificadas.
- **Comunicación de resultados**: Informar a los servidores públicos y directivos sobre los avances y mejoras implementadas.