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

VIGENCIA 2025

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 3
2. OBJETIVOS 3
2.1. GENERAL 3
2.2. ESPECÍFICOS 3
3. ALCANCE 4
4. MARCO NORMATIVO 5
5. METODOLOGÍA 6
6. IDENTIFICACIÓN DE RIESGOS 7
7. EVALUACIÓN DE RIESGOS 7
8. TRATAMIENTO DE RIESGOS 7
9. SEGUIMIENTO Y EVALUACIÓN 8

1. INTRODUCCIÓN

En el contexto actual, donde la información se ha convertido en uno de los activos más valiosos para las organizaciones, la gestión de riesgos de seguridad y privacidad de la información se ha vuelto un componente crítico para garantizar la continuidad del negocio, la protección de datos sensibles y el cumplimiento de normativas legales y regulatorias. Para EMCANDELARIA S.A.S E.S.P., empresa comprometida con la excelencia en la prestación de sus servicios, es fundamental establecer un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que se alinee con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG).

Este plan busca identificar, evaluar, tratar y monitorear los riesgos asociados a la información, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de los datos, así como garantizar el cumplimiento de los principios institucionales y la protección de los derechos de los ciudadanos.

2. OBJETIVOS

2.1. GENERAL

Diseñar e implementar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para EMCANDELARIA S.A.S E.S.P., en el marco de los planes institucionales del MIPG, que permita identificar, evaluar, mitigar y monitorear los riesgos asociados a la gestión de la información, asegurando la protección de los datos sensibles, el cumplimiento normativo y la continuidad operativa de la organización.

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 para EMCANDELARIA S.A.S E.S.P. se aplicará a todos los procesos, sistemas, activos de información y personal de la organización, incluyendo terceros que tengan acceso a la información de la empresa. Este plan abarca la identificación, evaluación, tratamiento y monitoreo de riesgos asociados a la seguridad y privacidad de la información, alineándose con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y los objetivos institucionales de la empresa.

El alcance incluye:

- **Procesos y áreas involucradas**: Gestión de información, tecnología de la información, recursos humanos, operaciones, finanzas y áreas administrativas.
- **Activos de información**: Bases de datos, sistemas informáticos, documentación física y digital, comunicaciones y cualquier otro recurso que contenga información sensible.
- **Terceros**: Proveedores, contratistas y aliados estratégicos que interactúen con los sistemas o la información de EMCANDELARIA S.A.S E.S.P.
- **Ciclo de vida del plan**: Desde la identificación de riesgos hasta la implementación de controles y el monitoreo continuo, con revisiones periódicas para asegurar su efectividad y actualización.

Este plan no cubre riesgos asociados a áreas ajenas a la seguridad y privacidad de la información, como riesgos financieros, operativos o legales no relacionados con la gestión de 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.