1. Introducción y Propósito

El presente Plan Estratégico de Seguridad y Privacidad de la Información tiene como propósito establecer los lineamientos institucionales para proteger la confidencialidad, integridad y disponibilidad de la información de EMSA – Lotería de Manizales, en cumplimiento de la normatividad vigente y en articulación con el Modelo Integrado de Planeación y Gestión – MIPG.

Este Plan tiene como objetivos:

- Proteger la **confidencialidad, integridad y disponibilidad** de la información de EMSA.
- Garantizar el cumplimiento de **normas constitucionales y legales** aplicables en Colombia.
- Alinear la gestión de seguridad y privacidad con el **Plan Estratégico 2026-2027**.
- Establecer mecanismos de **control, prevención, respuesta y mejora continua**.

2. Marco Normativo Aplicable

El Plan debe estar fundamentado en:

2.1. Normatividad Nacional Colombiana

- **Constitución Política de Colombia** (Derecho a la intimidad y habeas data).
- **Ley 1581 de 2012** – Protección de Datos Personales.
- **Decreto 1377 de 2013** – Reglamento parcial de la Ley 1581.
- **Ley 1266 de 2008** – Hábitos financieros y crediticios (si aplica).
- **Ley 1712 de 2014** – Transparencia y acceso a la información pública (si aplica).
- **Ley 1273 de 2009** – Tipificación de delitos informáticos.
- **Estándares y Políticas del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**.

2.2. Normatividad de Gestión Pública

- **MIPG** – Modelo Integrado de Planeación y Gestión (estructura y gestión de riesgos, control interno, Gobierno TIC, etc.).
- **FURAG** – Formato Único de Reporte de Avances en Gestión (para gerencia y control).

3. Alineación con el Plan Estratégico 2026-2027

El Plan de Seguridad y Privacidad debe integrar totalmente los ejes estratégicos definidos por EMSA:

Ejes estratégicos típicos:

1. **Gobierno de la seguridad de la información**
2. **Gestión del riesgo**
3. **Protección de datos personales y privacidad**
4. **Ciberseguridad**
5. **Concientización y cultura**
6. **Monitoreo, respuesta y mejora continu**

4. Estructura del Plan de Seguridad y Privacidad

4.1. Alcance

- Define **activos, procesos, personas, sistemas** y unidades organizativas cubiertas.
- Identifica si aplica a terceros y aliados.

4.2. Gobierno y Roles de Responsabilidad

Define claramente funciones y responsabilidades:

Rol	Responsabilidad
Consejo Directivo / Alta Gerencia	Patrocinio, direccionamiento estratégico, recursos.
Oficial de Seguridad de la Información (CISO)	Liderar implementación, cumplimiento y seguimiento.
Oficial de Privacidad / DPO	Protección de datos personales, cumplimiento normativo.
Gestores de Riesgos	Evaluar y tratar riesgos.
Responsables de Procesos / Jefes de Área	Implementar medidas en su ámbito.
Usuarios	Cumplir políticas y reportar incidentes.

4.3. Identificación y Clasificación de Activos

- Inventario de activos (información, hardware, software, servicios).
- Clasificación por **nivel de sensibilidad** (pública, interna, confidencial, reservada).
- Propietarios asignados.

4.4. Gestión del Riesgo

1. **Identificación de riesgos** (amenazas y vulnerabilidades).
2. **Evaluación y análisis de riesgos** (impacto y probabilidad).
3. **Tratamiento de riesgos** (aceptar, transferir, mitigar, evitar).
4. **Plan de acción** con responsables y plazos.

4.5. Controles de Seguridad y Privacidad

Basados en mejores prácticas (ISO 27001, NIST, etc.):

Controles Organizacionales

- Políticas de seguridad y privacidad.
- Gestión documental y controles de versiones.
- Alineación con marcos normativos.

Controles Técnicos

- Autenticación y control de acceso.
- Cifrado de datos en tránsito y reposo.
- Gestión de parches y vulnerabilidades.
- Monitoreo continuo de eventos e incidentes.

Controles Físicos

- Acceso físico a centros de datos y equipos.
- Videovigilancia y controles de ingreso.

Controles de Privacidad

- Consentimiento y legitimación de tratamiento.
- Derechos de los titulares (acceso, rectificación, supresión).
- Gestión de transferencias de datos a terceros.
- Anonimizarían y minimización de datos personales

4.6. Gestión de Incidentes

- Procedimientos documentados para notificación, respuesta y recuperación.
- Categorización de incidentes de seguridad.
- Comunicación interna y (si aplica) notificación a autoridades.

4.7. Capacitación y Cultura

- Programa de formación periódica en:
  - Seguridad digital (phishing, contraseñas, redes sociales).
  - Privacidad y protección de datos personales.
- Indicadores de eficacia (evaluaciones, campañas).

4.8. Monitoreo y Métricas

Define indicadores para medir el desempeño del Plan:

Indicador	Ejemplo de Meta
% de cumplimiento de controles	≥ 90%
# de incidentes detectados y resueltos	Reduce anualmente
Tiempo promedio de respuesta a incidentes	≤ X horas
Nivel de madurez de seguridad	Mejora anual

Estos parámetros alimentan **FURAG** y permiten informar a gerencia.

4.9. Mejora Continua

- Ciclo PDCA (Planificar, Ejecutar, Verificar, Actuar).
- Revisión anual o por cambios de contexto.
- Ajustes con base en auditorías internas y externas.

5. Documentación Clave del Plan

El Plan debe estar acompañado por:

✓ Políticas y procedimientos estándares
✓ Manual de gestión de riesgos
✓ Matrices de control
✓ Registros de incidentes y lecciones aprendidas
✓ Planes de continuidad y recuperación frente a desastres
✓ Evidencias de capacitación

6. Integración con MIPG y FURAG

MIPG

- El Plan debe integrar procesos de **gestión documental, riesgos, control interno**, estrategia y objetivos.
- Asegura que la seguridad y privacidad estén incluidos en el ciclo de planeación institucional.

FURAG

- Define los **reportes de avance** (trimestrales/anuales) que se presentarán a la alta dirección.
- Incluye métricas de cumplimiento, gestión de riesgos y estado de controles.

7. Cronograma Sugerido

Fase	Actividades	Duración
Diagnóstico y alcance	Inventario, análisis inicial	4-6 semanas
Diseño de controles	Políticas y procedimientos	6-8 semanas
Implementación	Medidas técnicas y organizacionales	8-12 semanas
Pruebas y ajustes	Simulacros, validaciones	4-6 semanas
Reporte inicial FURAG	Presentación de resultados	2 semanas

Enero 28 de 2026.

Proyectado: CARLOS ALBERTO OCAMPO
Profesional Universitario
Sistemas

Elaborado por MCHV