PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026-2027

1. Introducción y Objetivo

Propósito del Plan:

Definir un marco estratégico para proteger la información institucional, reducir riesgos cibernéticos, garantizar la confidencialidad, integridad y disponibilidad de los activos de información, y cumplir con la **normatividad vigente** (FURAG, MIPG, demás regulaciones sectoriales y estándares internacionales).

Alcance
Aplica a:

- Información institucional (electrónica y física)
- Sistemas de información y plataformas digitales
- Procesos, servicios y personal
- Terceros y proveedores de servicios

2. Marco Normativo y Político

2.1 Normatividad Nacional

Debes incluir una tabla de referencia con leyes y decretos que guían la seguridad de la información:

Norma	Descripción
FURAG (Marco de Referencia de Arquitectura Empresarial)	Establece guías obligatorias para interoperabilidad y arquitectura de TI en entidades públicas.
MIPG (Modelo Integrado de Planeación y Gestión)	Define lineamientos para gestión y control interno, incluyendo el componente de seguridad de la información.
Ley 1581 de 2012	Protección de datos personales en Colombia.
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581.
Ley 1266 de 2008	Habeas Data financiero.
Circular externa de la Superintendencia de Industria y Comercio	Orientaciones aplicables a deberes de seguridad y gestión de incidentes de datos.
Otras disposiciones sectoriales	Dependiendo del sector de loterías y juegos de suerte.

3. Gobernanza de la Seguridad de la Información

3.1 Visión Estratégica

Proteger los activos de información frente a amenazas, garantizando la confianza, continuidad operativa y cumplimiento normativo.

3.2 Políticas Corporativas

El plan debe referenciar o incluir políticas internas como:

- Política de Seguridad de la Información
- Política de Control de Accesos
- Política de Gestión de Vulnerabilidades y Parcheo
- Política de Respuesta a Incidentes
- Política de Gestión de Datos Personales

3.3 Roles y Responsabilidades

Rol	Responsabilidades
Responsable de Seguridad de la Información (CISO/Oficial)	Liderar la implementación y monitoreo del plan.
Comité de Seguridad de la Información	Aprobar estrategias, revisar métricas y tomar decisiones.
Encargados de procesos funcionales	Asegurar aplicación de controles.
Usuarios finales	Cumplimiento de políticas y reportes oportunos.

4. Evaluación de Riesgos

4.1 Inventario de Activos de Información

Incluye hardware, software, datos, documentación, proveedores.

4.2 Identificación de Riesgos

Considera amenazas de:

- Ciberataques (phishing, ransomware)
- Fallas humanas y operativas
- Falla de proveedores
- Incumplimiento normativo

4.3 Análisis y Tratamiento de Riesgos

Asigna:

- Nivel de probabilidad e impacto
- Medidas de mitigación
- Propietario del riesgo
- Plan de acción

5. Controles y Estrategias

5.1 Controles Técnicos

- Gestión de accesos (roles, contraseñas, MFA)
- Firewall, IDS/IPS, segmentación de redes
- Anti-malware y control de endpoint
- Copias de seguridad y cifrado de datos

5.2 Controles de Procesos

- Gestión de cambios
- Monitoreo y registro de eventos (SIEM)
- Evaluaciones periódicas de vulnerabilidades y pruebas de penetración

5.3 Controles de Personal

- Concienciación y formación en seguridad
- Políticas de contratación de terceros
- Clausulas de confidencialidad

5.4 Privacidad y Protección de Datos

- Matrices de tratamiento de datos
- Consentimiento informado
- Procedimientos de derechos de los titulares (acceso, rectificación, supresión)

6. Gestión de Incidentes

6.1 Definición de Incidente

Cualquier evento que afecte seguridad, continuidad o integridad de la información.

6.2 Procedimiento Estructurado

- Detección y reporte
- Clasificación y priorización

- Contención y erradicación
- Recuperación
- Lecciones aprendidas

6.3 Registro y Métricas

Indicadores como:

- Incidentes detectados vs resueltos
- Tiempo medio de detección y respuesta

7. Plan de Acción 2026-2027

7.1 Objetivos Estratégicos

Objetivo	Meta	Indicador	Responsable
Mejorar la madurez de seguridad	Implementar 80% de controles críticos	% de controles implementados	Responsable de seguridad
Concienciación	Capacitar al 100% del personal	% asistencia (%)	RRHH / Seguridad
Gestión de incidentes	Reducir tiempo de resolución	TTR promedio	Equipo de TI

7.2 Línea de Tiempo (Roadmap)

Año 2026

- Q1: Evaluación inicial de madurez y riesgos
- Q2: Actualización de políticas y controles
- Q3: Campañas de concienciación

Año 2027

- Q1: Implantación de soluciones de SIEM
- Q2: Simulacros de incidentes
- Q3: Auditoría de cumplimiento

8. Métricas y Seguimiento

Definir KPIs incluidos en cuadros de mando:

- % cumplimiento de políticas
- % de incidentes resueltos en SLA
- Número de vulnerabilidades críticas abiertas

- Tiempo medio para aplicar parches

9. Documentación y Evidencia

Mantener registros:

- Políticas vigentes
- Actas de comités
- Resultados de auditorías
- Reportes de incidentes y lecciones aprendidas

10. Alineación con FURAG y MIPG

FURAG

El plan debe demostrar:

- Capacidad de interoperabilidad segura
- Cumplimiento con estándares de arquitectura empresarial y de seguridad
- Registro de activos, servicios y flujos de información

MIPG

Debe cumplir claramente con:

- **Componente de Control Interno** (cultura de control)
- **Gestión de Riesgos**
- **Gestión Documental**
- **Indicadores y Evaluación del Desempeño**

Conclusión

El **Plan Estratégico de Seguridad de la Información, Ciberseguridad y Privacidad 2026-2027** no es un documento estático, sino una estrategia dinámica que:

- ✓ Protege los activos de información
- ✓ Se alinea con la **normatividad vigente** (FURAG, MIPG y otras)
- ✓ Reduce riesgos tecnológicos y de datos.
- ✓ Fortalece la **confianza de los usuarios y la continuidad operativa**

Enero 28 de 2026.

Proyectado: CARLOS ALBERTO OCAMPO
Profesional Universitario
Sistegmas