ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Social

MANUAL ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Hoja de Ruta Operativa y de Ciberseguridad 2026



Subdirección de Diseño y Análisis Estratégico (SDAE)
Versión 08 | Enero 2026

Confidencialidad • Integridad • Disponibilidad

La Información es el Activo Estratégico del IPES

En un entorno interconectado, la información no es solo un registro; es el motor de nuestras decisiones y servicios. Este plan alinea nuestra operación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y el MIPG.



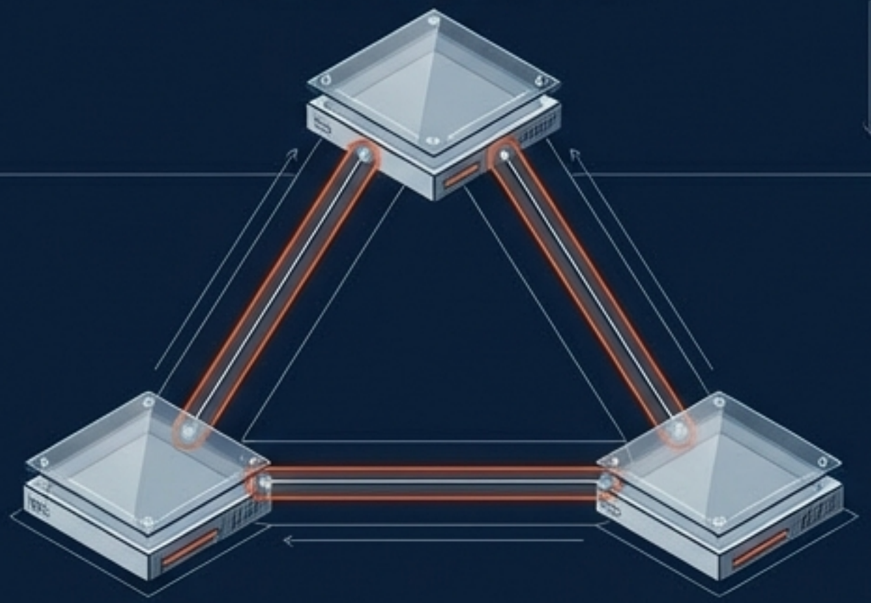


Proteger los activos frente a amenazas avanzadas para asegurar **la continuidad del negocio** y maximizar la confianza pública.

Actualización 2026: Incorporación de la dimensión de **Seguridad Digital**, extendiendo la protección al entorno digital y la **Infraestructura Crítica Cibernética (ICC)**.

Objetivos del Sistema de Gestión (SGSI)

Confidencialidad
Acceso solo a autorizados

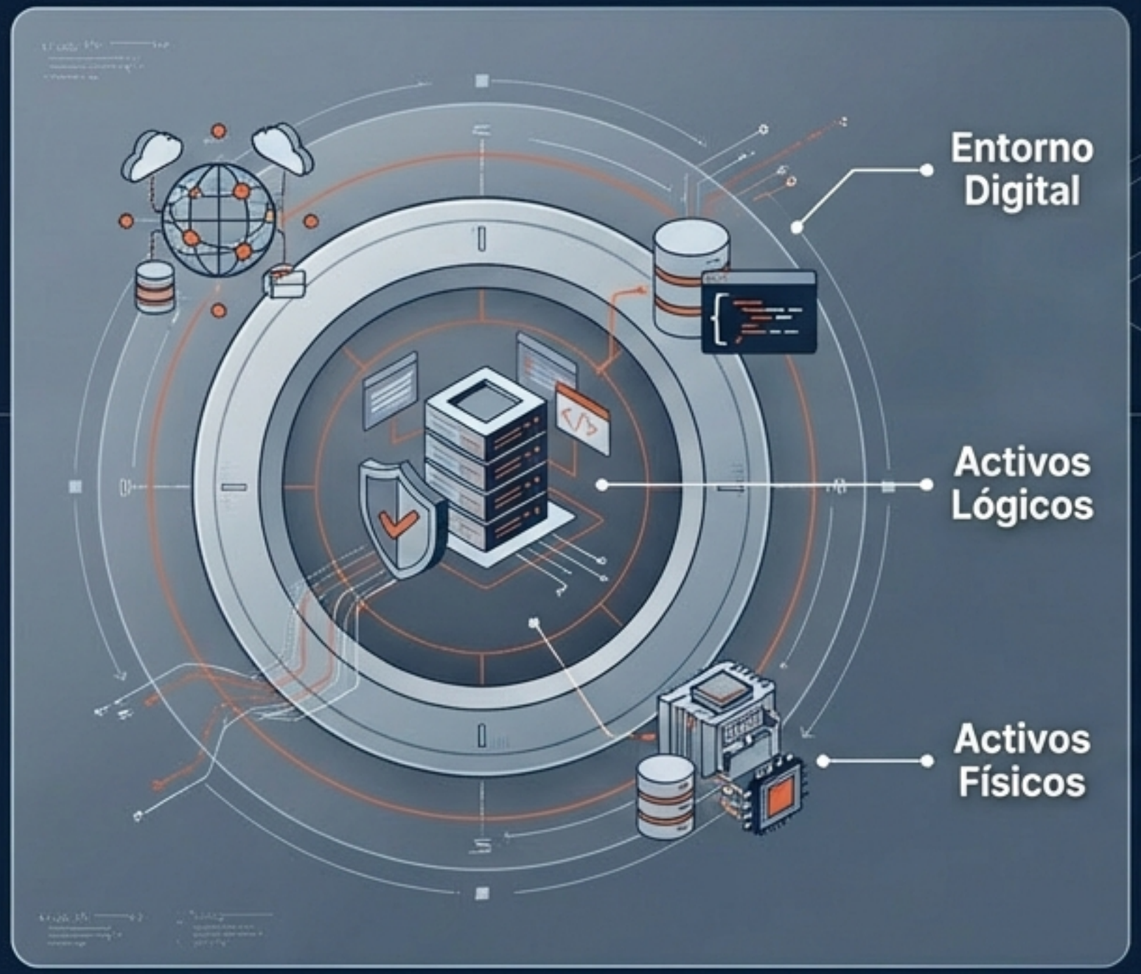


Disponibilidad
Acceso cuando se requiera

Integridad
Exactitud y completitud

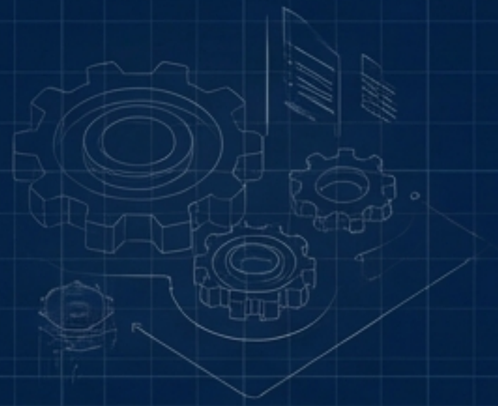
- Fortalecer la cultura organizacional de seguridad.
- Garantizar el cumplimiento legal (Ley 1581, Ley 1712).
- Gestionar riesgos de manera eficiente para asegurar la continuidad de los servicios de TI.

Alcance y Definiciones Clave



- **Amenaza:** Causa potencial de un incidente no deseado.
- **Vulnerabilidad:** Debilidad que puede ser explotada.
- **Riesgo:** Probabilidad de que una amenaza explote una vulnerabilidad.
- **Ciberseguridad:** Protección de activos en la infraestructura interconectada.

Estructura de Gobernanza y Responsabilidad





Comité de Sistemas y Seguridad
Define políticas y asigna recursos

Oficial de Seguridad (CISO)
Lidera el SGSI y la estrategia de defensa

Infraestructura y Redes

Administradores de Aplicativos (HEMI)

Gestión Documental y SIG

Equipo de Gestión

Nivel Estratégico: Comité de Sistemas y Seguridad



Funciones Clave

Aprobar: El Plan Estratégico de TI (PETI) y políticas de seguridad.

Asignar: Recursos humanos, técnicos y financieros para el SGSI.

Diagnosticar: Evaluar el estado de ciberseguridad de la Entidad.

Definir: Roles y responsabilidades de seguridad.

Entregable Principal: Informe ejecutivo al Comité Institucional de Gestión y Desempeño.

Nivel Táctico: Oficial de Seguridad de la Información (CISO)



Player Profile Card

Rol asumido por el **Subdirector de Diseño y Análisis Estratégico (SDAE)**

Misión: Responsable de la triada Confidencialidad, Integridad, Disponibilidad.

1. **Escanear**: Ejecutar análisis de vulnerabilidades (Herramientas: Nessus, OpenVAS).
2. **Responder**: Coordinar la gestión de incidentes de seguridad.
3. **Liderar**: Implementación y mantenimiento del estándar ISO 27001.
4. **Reportar**: Documentar hallazgos y estado de madurez al Comité.

Entregable Principal: Informe de Estado de Seguridad Táctico y Plan de Mitigación.

Operación Técnica: Infraestructura y Comunicaciones

Administrador Infraestructura Tecnológica



Foco: Continuidad del servicio.

- Gestión de Backups
- Mantenimiento de servidores
- Manuales de despliegue
- Configuración de servicios críticos (HEMI, GOOBI)

Administrador Redes de Comunicaciones



Foco: Disponibilidad y conectividad.

- Configuración de equipos activos
- Gestión de garantías de activos críticos
- Respaldo de configuraciones

Operación Técnica: Datos y Aplicaciones

DBA (Administrador de Bases de Datos)



Meta: Fuente única de verdad. Garantizar integridad para reportes a entes de control.

- Gestión de acceso y permisos
- Optimización de rendimiento
- Auditoría y seguridad de datos

Administración HEMI (Misional)



Meta: Fuente oficial de información poblacional.
Control: Gestión de cambios y documentación (Diccionario de datos, Modelo ER).

- Actualización de modelos de datos
- Documentación técnica rigurosa
- Validación de integridad poblacional

Admin Sistemas Administrativos



Meta: Soporte a Nómina, Inventarios, Tesorería.
Acción Clave: Simulacros de restauración.

- Mantenimiento de aplicaciones
- Pruebas de recuperación ante desastres
- Soporte a usuarios funcionales

Soporte Transversal y Cultura

Responsable Gestión Documental



Velar por la clasificación de la información y la trazabilidad (Tablas de Retención).

Control de Documentos SIG



Garantizar la vigencia y control de versiones en el Sistema Integrado de Gestión.

Responsable de Sensibilización



Ejecutar el plan de comunicación para generar cultura de seguridad (Oficina Asesora de Comunicaciones).

Metodología de Gestión de Riesgos (ISO 27001:2022)

1. Comprensión del Contexto



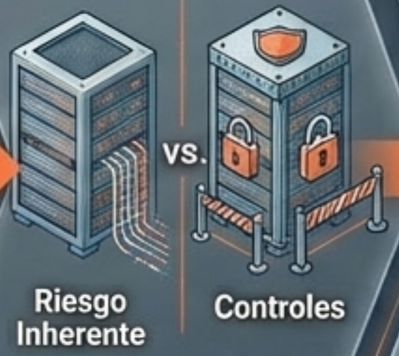
Factores internal/external.

2. Identificación



Risks affecting CIA triad.

3. Análisis



Riesgo Inherente vs. Controles.

4. Evaluación



Riesgo Residual.

5. Tratamiento



Definición del Plan PTR.

* Alineado con el Anexo A de la NTC-ISO/IEC 27001:2022.

Opciones de Tratamiento del Riesgo

Reducir

Aplicar controles para bajar el riesgo residual a nivel aceptable.



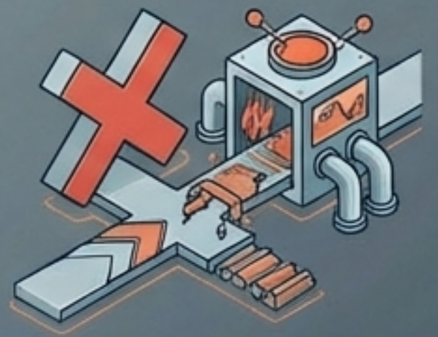


Compartir el riesgo con terceros (Seguros, Proveedores).

Asumir

Aceptar la pérdida si el costo del control supera el impacto.





Evitar

Eliminar la actividad o causa que genera el riesgo.

Componentes del Plan de Seguridad

SGSI



Infraestructura Crítica (ICC)

Identificación de activos donde la falla impacta el bienestar social.



Clasificación de Activos

Instructivo PA03-IN para inventariar Hardware, Software y Servicios.



Declaración de Aplicabilidad (SoA)

Justificación de controles ISO aplicados.



Políticas (PA03-MN)

Manual de reglas para funcionarios.

Hoja de Ruta 2026: Fase 1 - Diagnóstico y Planeación

January - March 2026

JANUARY			FEBRUARY			MARCH		
Week	W	W	Week	W	W	Week	W	W

Feb 01 - Feb 28

Diagnóstico de Madurez (Instrumento MSPI MinTIC)

Responsable: Profesional Seguridad.



Mar 01 - Mar 30

Análisis de Contexto y Partes Interesadas.



Mar 01 - Mar 22

Actualización de Política y Metodología de Riesgos (ISO 27001).



Hoja de Ruta 2026: Fase 2 - Activos y Riesgos

March - September 2026

MARCH		APRIL		MAY		JUNE		JULY		AUGUST		SEPTEMBER
Week		W	W		Week		W	W		Week		W	W

Identificación de Infraestructura Crítica Cibernética (ICC)

Mar 16 - Apr 30



Prioridad Alta.

Actualización de Inventarios (Software/Hardware).

Mar 16 - Sep 29

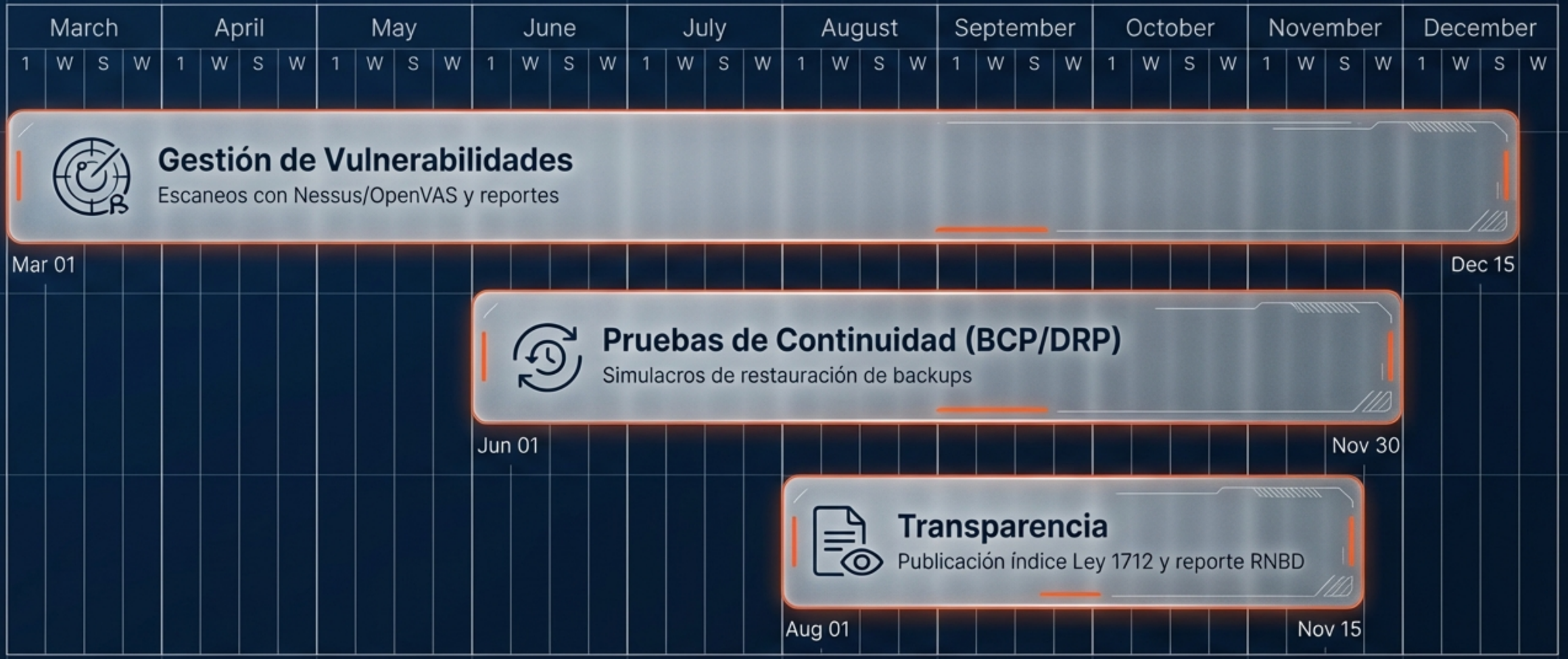


Aprobación del Plan de Tratamiento de Riesgos (PTR) y aceptación de riesgos residuales.

Apr 18 - Aug 30



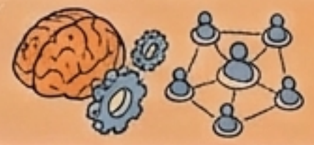
Hoja de Ruta 2026: Operación Técnica y Ciberseguridad



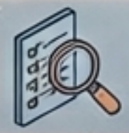
Hoja de Ruta 2026: Cultura y Mejora Continua

March - September 2026

FEB | MAR | APR | MAY | JUN | JUN | JUL | AUG | SEP | OCT | NOV | DEC



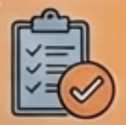
Plan de Cambio y Cultura
Capacitaciones y pruebas de ingeniería social.



Revisión por la Dirección.
JUN



Revisión por la Dirección.
DEC



Auditoría Interna.
NOV 10 — NOV 30



Acciones Correctivas y Cierre.
DEC 01 — DEC 31

Marco Normativo y Legal

Protección de Datos

- Ley 1581 de 2012
- Decreto 1377

Transparencia

- Ley 1712 de 2014

Delitos

- Ley 1273 de 2009 (Delitos Informáticos)

Estándares

- NTC-ISO/IEC 27001:2022

Política Nacional

- CONPES 3854
- CONPES 3995

Helvetica Now Display

Documentación Asociada y Procedimientos

- **PA03-PD-002:** Gestión de Incidentes de Seguridad.
- **PA03-PD-010:** Control de Cambios.
- **PA03-PD-005:** Trabajo en Áreas Seguras.
- **PA08-PD-003:** Gestión de Usuarios.
- **PA03-MN-002:** Manual Usuario HEMI.
- **PL-21:** Política de Tratamiento de Datos Personales.

Helvetica Now Display

La Seguridad es Responsabilidad de Todos

El fortalecimiento de un entorno seguro y confiable depende del cumplimiento estricto de estas políticas por parte de todos los funcionarios, contratistas y terceros.

Reporte cualquier incidente o debilidad identificada.

