Plan Gestión de Riesgos de Seguridad y Privacidad de la Información – IDEAR

1. INTRODUCCIÓN

El MSPI orienta la implementación del SGSI, su integración con el programa de protección de datos personales y la gestión de riesgos en entida7ydes públicas; por ello, el IDEAR adopta un enfoque institucional para salvaguardar la información bajo los pilares de confidencialidad, integridad y disponibilidad.

Este Plan 2026 convierte el procedimiento P-GTI-01 en una operación periódica y verificable para identificar, analizar, evaluar, tratar y monitorear riesgos de seguridad y privacidad, dejando trazabilidad y evidencia de cada ciclo. OBJETIVO

2. 2. Objetivo y alcance

2.1 Objetivo general

Establecer y ejecutar durante la vigencia 2026 un enfoque sistemático, documentado y verificable para la gestión de riesgos de seguridad y privacidad de la información en el IDEAR, orientado a identificar, analizar, evaluar, tratar y monitorear de manera periódica los riesgos que puedan afectar los activos de información. Este enfoque busca garantizar la confidencialidad (acceso únicamente por usuarios autorizados), la integridad (exactitud y no alteración no autorizada) y la disponibilidad (acceso oportuno a la información y servicios cuando se requiera) de la información institucional, minimizando la probabilidad e impacto de incidentes, fallas tecnológicas y accesos indebidos.

Asimismo, la gestión sistemática del riesgo permitirá priorizar acciones y recursos sobre los riesgos críticos, asegurar la continuidad de los procesos misionales y de apoyo, fortalecer la trazabilidad mediante evidencias de ejecución y facilitar el seguimiento por parte de la alta dirección y los órganos de control, consolidando una cultura de mejora continua y cumplimiento institucional en materia de seguridad y privacidad de la información.

2.2 Alcance

Este procedimiento y su plan de implementación aplica a todos los procesos misionales, estratégicos y de apoyo del IDEAR, así como a los activos de información asociados (físicos y digitales), los sistemas de información, la infraestructura tecnológica y los recursos documentales que soportan la operación institucional. De igual forma, cobija a todo el personal (servidores, contratistas, practicantes y terceros autorizados) que, por razón de sus funciones, crea, consulta, administra, transmite o custodia información de la entidad, incluyendo datos sensibles, datos personales y datos operativos.

3. Marco normativo y lineamientos

El Plan Institucional 2026 se rige por el procedimiento P-GTI-01, el cual define la forma en que el IDEAR debe gestionar de manera ordenada y verificable los riesgos de seguridad y privacidad de la información. En particular,

el procedimiento exige la aplicación del ciclo completo de gestión del riesgo —identificación, análisis, evaluación, tratamiento y monitoreo—, asegurando que los riesgos no se queden únicamente en su reconocimiento, sino que sean valorados, priorizados y gestionados mediante acciones concretas que reduzcan su probabilidad e impacto sobre los activos de información.

De igual forma, el procedimiento establece controles documentales que garantizan trazabilidad, transparencia y evidencia institucional: uso de formatos oficiales (registro y matriz de riesgos, plan de tratamiento), definición de responsables, y conservación de soportes que permitan demostrar decisiones y avances ante la alta dirección y órganos de control. Finalmente, determina una periodicidad de actualización que mantiene vigente la gestión del riesgo, realizando revisiones semestrales y activando actualizaciones extraordinarias cuando se presenten cambios significativos (por ejemplo, ajustes en infraestructura, incorporación de nuevos sistemas, hallazgos de auditoría o incidentes relevantes), con el fin de asegurar la mejora continua y la resiliencia institucional.

4. Metodología

Se implementa el mismo ciclo del procedimiento:

1. **Identificación:** inventario de activos, amenazas, vulnerabilidades y registro estructurado.
2. **Análisis:** probabilidad e impacto, clasificación y priorización con matriz.
3. **Evaluación:** comparación contra criterios de aceptación; se definen riesgos aceptables/no aceptables y se reportan los no aceptables a alta dirección.
4. **Tratamiento:** mitigar/transferir/aceptar/evitar; diseñar controles, implementar, probar efectividad y documentar.
5. **Monitoreo y revisión:** programa semestral, revisión de cambios del entorno, efectividad de controles, ajustes y comunicación de resultados.

5. Contexto institucional

El IDEAR requiere que los riesgos de seguridad y privacidad se gestionen como un proceso transversal que soporte la continuidad y confiabilidad de la operación institucional. El procedimiento define que la gestión parte de activos, políticas, auditorías e historial de incidentes como insumos para construir y mantener el registro y la matriz de riesgos.

6. Diagnóstico

Fortalezas del documento

- Define el ciclo completo, entradas/salidas y pasos por etapa.
- Define roles, indicadores, formatos y periodicidad de actualización.

Ajustes recomendados (para que el plan quede 100% ejecutable)

Sin cambiar el espíritu del procedimiento, en 2026 conviene dejar “aterrizados”:

- **Escalas y criterios**: definir en anexo la escala de probabilidad/impacto (1–5 o baja/media/alta) y el umbral de "no aceptable", porque el procedimiento menciona escalas y criterios, pero no los parametriza.
- **Plantillas de evidencia**: el documento menciona "registro, matriz, plan de tratamiento" como formatos; el plan debe institucionalizarlos (nombre, campos, repositorio, responsable, versión).
- **Calendario fijo**: aunque se indica revisión semestral, conviene fijar fechas (ej.: junio y noviembre) y una revisión "eventual" por cambios significativos.

7. Situación deseada

Al cierre de 2026, IDEAR contará con:

- **Inventario de activos** actualizado, con responsables y criticidad, como base para la identificación de riesgos.
- **Registro institucional de riesgos** y **matriz de riesgos** priorizada vigente.
- **Riesgos no aceptables** reportados a alta dirección con recomendación de tratamiento.
- **Plan de tratamiento** ejecutado con verificación de efectividad y evidencias.

8. Gobernanza (Roles y Responsabilidades)

La gobernanza del proceso de gestión de riesgos de seguridad y privacidad en el IDEAR se organiza para asegurar dirección, control y ejecución efectiva: el Líder de Seguridad coordina la identificación, análisis y consolidación de los riesgos; el Comité de Gestión de Riesgos revisa los resultados, prioriza y aprueba las estrategias de tratamiento; la Alta Dirección valida los planes de acción, toma decisiones frente a riesgos no aceptables y garantiza la asignación de recursos necesarios; y el personal operativo aporta información del día a día, reporta incidentes y contribuye en la implementación y cumplimiento de los controles definidos, asegurando que la gestión del riesgo sea transversal y sostenible en la entidad.

9. Documentación y control

- **Formatos utilizados:** Registro de riesgos, matriz de riesgos, plan de tratamiento.
- **Frecuencia de actualización:** semestral o ante cambios significativos.
- **Responsable del control documental:** Líder de Seguridad de la Información.

10. DOCUMENTACIÓN Y CONTROL

- **Formatos Utilizados:** Registro de riesgos, matriz de riesgos, plan de tratamiento.
- **Responsable del Control Documental:** Líder de Seguridad de la Información.

CONTROL DE CAMBIOS

Control de Cambios		
Versión	Fecha de Aprobación (D/M/A)	Descripción del cambio
01	31 de enero de 2025	Emisión del documento
02	21 de enero de 2026	Se presento el documento al comité institucional de gestión y desempeño para socialización y viabilizacion, quedó aprobado mediante Acta No. 02.

Elaboró	Revisó	Aprobó
Nombre: **JORGE SORIANO HURTADO**	**Nombre:** Comité Institucional de Gestión y Desempeño Acta No. 02 del 21/01/2026	**Nombre:** Comité Institucional de Gestión y Desempeño Acta No. 02 del 21/01/2026
Cargo: Profesional Universitario Requerimientos Tecnológicos	**Cargo:** N/A	**Cargo:** N/A
Firma: ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO
Fecha: 14 de enero de 2026	**Fecha:** 21 de enero de 2026	**Fecha:** 21 de enero de 2026
Revisó Aspectos SIG: ADRIANA SÁNCHEZ ORJUELA / Profesional de Apoyo SIG		