Manual SGSI para el INE

4Geeks Academy

FELIPE ALONSO GOMEZ HENRY
ESTUDIANTE BOOTCAMP CIBERSEGURIDAD

4Geeks

Tabla de contenido

4Geeks

Introducción

Organismo: Instituto Nacional de Estadísticas (INE)

Fecha: 12-05-2025

Version: 1.0

Responsable: Felipe Gómez H

Un Sistema de Gestión de Seguridad de la Información (SGSI), es una metodología con un enfoque sistemático para proteger la información de una organización. Para el caso estudiado el SGSI del Instituto Nacional de Estadísticas (INE) tiene como propósito establecer una estructura organizativa, técnica y normativa que permita proteger de forma efectiva los activos de información de la institución y los principios definidos en la política institucional de seguridad. El objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información crítica asociada a los procesos estadísticos nacionales mientras se cumplan los estatutos de la ley de transparencia de la república de Chile.

El presente manual establece el marco del Sistema de Gestión de Seguridad de la Información (SGSI), alineado con los estándares ISO/IEC 27001:2022, NIST SP 800-53, y con las leyes chilenas N° 19.628 y 21.663.

4Geeks

Alcance del SGSI

El SGSI aplica a todas las unidades del INE, incluidas oficinas regionales. También se incluyen procesos de recolección, tratamiento y publicación de información estadística. Es aplicable a sistemas críticos: microdatos censales, portal web, sistemas de encuestas, plataformas de interoperabilidad y servidores. Y es necesario considerar también a personal, contratistas y terceros que acceden a información o sistemas institucionales.

1) Ámbitos organizacionales:
    a) Dirección de Tecnología de la Información
    b) Subdepartamento de Gestión de la Información
    c) Dirección de Estudios y Coordinación Estadística
    d) Oficinas regionales (por su rol en la recolección y procesamiento de datos)
2) Procesos cubiertos:
    a) Recolección de datos censales, encuestas y registros administrativos
    b) Almacenamiento, tratamiento y análisis de microdatos
    c) Publicación de estadísticas e indicadores nacionales
    d) Gestión de infraestructura TI, respaldo y continuidad operativa

Organización de la seguridad

Estructura de Gobernanza

El Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto Nacional de Estadísticas (INE) se soporta en una estructura organizacional formal, conforme a la estructura vigente al año 2024.

Las unidades responsables del diseño, implementación y operación del SGSI están distribuidas entre la Dirección Nacional, la Subdirección de Tecnologías de la Información y Comunicaciones (TIC), la Unidad de Seguridad de la Información, y áreas regionales.

4Geeks

Roles Clave

Unidad/Rol	Responsabilidad dentro del SGSI
Dirección Nacional	Aprobar lineamientos estratégicos del SGSI, asignar presupuesto y definir prioridades institucionales
Departamento de Seguridad de la Información.	Coordinar y supervisar la implementación del SGSI. Emitir políticas, auditar cumplimiento y gestionar incidentes.
Subdepartamento de Ciberseguridad (TIC).	Diseñar, implementar y mantener controles técnicos de ciberseguridad. Aplicación de estándares ISO/NIST.
Departamento de Continuidad Operativa	Garantizar la disponibilidad y recuperación de los servicios críticos ante interrupciones o incidentes.
Subdepartamento de Infraestructura y Telecomunicaciones	Controlar el acceso a la red, gestionar firewalls, VPN y segmentación interna.
Unidad de Gobierno de Datos	Supervisar la calidad, privacidad y trazabilidad de la información estadística y microdatos.
Unidad de Transparencia y Atención Ciudadana	Asegurar el cumplimiento de la Ley de Acceso a la Información Pública y responder a solicitudes externas.
Subdepartamento de Soporte a Usuarios	Asegurar el cumplimiento de políticas de acceso y seguridad en el endpoint, incluyendo MDM y control de dispositivos.
Direcciones Regionales	Ejecutar localmente las políticas de seguridad, con reportes a la Dirección Nacional.

Comité de Seguridad de la Información

El Comité está compuesto por representantes de:

- Dirección Nacional
- Departamento de Seguridad de la Información
- Subdirección TIC
- Departamento de Continuidad Operativa
- Unidad de Gobierno de Datos
- Jurídico y Transparencia

Funciones del Comité:

- Aprobar políticas de seguridad y procedimientos críticos.
- Revisar los resultados de auditorías internas y externas.
- Monitorear los KPIs del SGSI.
- Validar el plan de respuesta a incidentes y de continuidad operativa.
- Autorizar excepciones bajo control documentado.

4Geeks

Coordinación con Organismos Nacionales

- El INE mantiene vínculo operativo y técnico con
- CSIRT de Gobierno: Para gestión de incidentes nivel 2 y 3.
- Consejo para la Transparencia (CPLT): Para gestión de solicitudes de información o reclamos por incumplimientos.
- INE Regionales: Implementación operativa y feedback local.

Inventario y Clasificación de Activos de Información

Establecer un inventario exhaustivo y actualizado de los activos de información del Instituto Nacional de Estadísticas (INE), clasificándolos según su tipo, propietario, valor, criticidad y nivel de sensibilidad, conforme a los principios de gestión de activos definidos por la norma ISO/IEC 27001:2022 (Control 5.9) y la política institucional del SGSI.

Categoría de Activos

Categoría	Descripción
Datos	Microdatos censales, encuestas, indicadores, bases de datos estadísticas
Software	Sistemas de recolección, análisis, visualización, gestión documental
Hardware	Servidores, tablets, laptops, firewalls, dispositivos de red
Personas	Funcionarios, encuestadores, analistas, operadores
Infraestructura	Redes internas, enlaces WAN, sistemas cloud externos.
Documentación	Manuales técnicos, procedimientos, informes internos.

4Geeks

Inventario de Activos Críticos

ID	Activo	Tipo	Descripción	Clasificación
A1	Microdatos censales	Datos	Datos de encuestas y censos recolectados a nivel nacional	Crítico
A2	Sistemas de gestión de encuestas	Software	Plataforma para recolección y validación de datos en línea	Crítico
A3	Portal web institucional	Aplicación	Sitio de publicación de estadísticas, acceso público	Alto
A4	Servidores de base de datos	Hardware	Infraestructura donde se almacenan los microdatos	Alto
A5	Equipos de recolección móvil	Hardware	Tablets o dispositivos usados por encuestadores en terreno	Medio
A6	Personal encuestador	Humano	Agentes que recolectan información directamente con la ciudadanía	Alto
A7	Red interna del INE	Red	Conectividad interna de oficinas y centros regionales	Alto
A8	Copias de seguridad	Procedimiento	Respaldos de información crítica del sistema	Crítico
A9	Manuales técnicos de procesamiento	Documentación	Instrucciones internas para validación y limpieza de datos	Medio
A10	Plataforma de interoperabilidad estadística.	Software	Sistema que permite el intercambio de datos con otros organismos del Estado	Crítico
A11	Infraestructura cloud contratada	Infraestructura	Servicios IaaS/PaaS utilizados para procesamiento de datos (ej. AWS, Azure)	Alto
A12	Plataforma de visualización de indicadores	Aplicación	Portal de dashboards estadísticos públicos e internos	Alto

4Geeks

Gestión del Ciclo de Vida de los activos de información

Todo activo debe tener un ciclo de vida documentado:

1. Adquisición: Registro y autorización.
2. Uso: Supervisión, mantenimiento, acceso autorizado.
3. Transferencia: Cifrado, logs, contratos de confidencialidad.
4. Baja: Borrado seguro, destrucción física o digital.

El inventario se debe revisar cada 6 meses y se debe actualizar con:

1. Incorporación de nuevos sistemas
2. Cambios de ubicación o propietario
3. Cambios en clasificación de seguridad

4Geeks

Análisis de Riesgos

Establecer un proceso estructurado y repetible para identificar, valorar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información gestionada por el Instituto Nacional de Estadísticas (INE).

El SGSI del INE aplica controles en 4 categorías:

1. Controles técnicos: cifrado, segmentación, IDS, WAF.
2. Controles organizacionales: políticas de clasificación, roles, revisión de accesos.
3. Controles físicos: control de ingreso a oficinas, seguridad perimetral.
4. Controles procedimentales: respaldo, gestión de cambios, respuesta a incidentes

La selección de controles se basa en:

- ISO/IEC 27001:2022 Anexo A
- NIST SP 800-53 Rev. 5

La elección se centra en:

- Riesgos críticos y altos
- Factibilidad en una organización pública
- Recursos humanos y técnicos del INE

Metodologías de evaluación

Se utilizó una matriz cualitativa de riesgos basada en:

- Probabilidad (baja [1], media [2], alta [3])
- Impacto (bajo [1], medio [2], alto [3])

El nivel de riesgo se calcula con:

- Riesgo = Probabilidad × Impacto

Luego se prioriza en tres niveles: Crítico, Alto, Medio

4Geeks

Clasificación de Activos según Sensibilidad

ID	Amenaza Potencial	Probabilidad	Impacto	Nivel de riesgo	clasificación
A1	Acceso no autorizado	3	3	9	Crítico
A2	Interrupción del servicio (DoS/DDoS)	2	3	6	Alto
A3	Desfiguración del sitio (defacement)	2	2	4	Medio
A4	Ransomware o borrado malicioso	3	3	9	Crítico
A5	Robo o pérdida de los dispositivos	3	2	6	Alto
A6	Ingeniería social / suplantación	3	2	6	Alto
A7	Escaneo y pivoting lateral	2	3	6	Alto
A8	Corrupción de respaldos	2	3	6	Alto
A9	Fuga de información confidencial	2	2	4	Medio
A10	Man-in-the-middle (MITM) en transferencia.	2	3	6	Alto
A11	Acceso no autorizado	3	3	9	Crítico
A12	Inyección de código (XSS/HTML)	2	3	6	Alto

Plan de Tratamiento

Los riesgos Críticos y Altos serán tratados con:

- Controles técnicos y organizativos concretos
- Plazos definidos
- Revisiones periódicas del estado del tratamiento

Riesgos de nivel Medio se aceptan con monitoreo continuo. No se tolerarán riesgos críticos sin mitigación

4Geeks

Revisión del Riesgo Residual

Una vez aplicados los controles, se reevalúa cada riesgo y se estima el riesgo residual. Si aún es Alto o Crítico, se refuerzan los controles o se reconsidera el proceso.

Ejemplo:

- Riesgo Critico: Tras aplicar RBAC + MFA -> residual: Medio
- Riesgo Alto a medio: Tras implementar WAF + alertas -> residual: Bajo

Controles de Seguridad

Establecer e implementar controles proporcionales a los riesgos identificados, que permitan garantizar la confidencialidad, integridad y disponibilidad de los activos del INE, conforme a las buenas prácticas definidas en:

- ISO/IEC 27001:2022 Anexo A
- NIST SP 800-53 Rev. 5

Tipos de controles

Tipo	Descripción
Técnicos	Medidas automatizadas o de infraestructura (ej. MFA, cifrado, firewalls).
Organizativos	Políticas, capacitación, segregación de funciones.
Físicos	Controles de acceso a instalaciones y protección de equipos.
Procedimentales	Procedimientos documentados: backups, respuesta a incidentes, gestión de cambios.

4Geeks

Controles Seleccionados y Riesgos a Mitigar

Riesgo Asociado	Control Aplicado	Tipo	Norma/Referencia
Acceso indebido a microdatos (R1)	MFA + RBAC + monitoreo de accesos	Técnico	ISO A.9.2.1 / CIS 6.3
Ransomware (R2)	Antimalware + segmentación de red + backups cifrados	Técnico / Procedimental	ISO A.12.2.1 / CIS 10.1
Robo de tablets (R3)	Cifrado completo + MDM + wipe remoto	Técnico / Físico	ISO A.11.2.7 / CIS 4.5
DoS a encuestas (R4)	WAF + limitación de peticiones + CDN	Técnico	NIST SC-5 / CIS 9.1
Defacement de portal (R5)	Gestión de cambios + revisión de permisos	Procedimental	ISO A.12.1.2 / NIST CM-3
Phishing a personal clave (R6)	Capacitación + simulacros + política de contraseñas	Organizativo	ISO A.7.2.2 / CIS 14.5

Aplicación de Controles Críticos

Autenticación y Control de Accesos:

- Todos los sistemas críticos requieren MFA obligatorio.
- Se aplica principio de mínimo privilegio (Least Privilege).
- Auditoría de accesos críticos cada trimestre.

Respaldo y Continuidad

- Backups automáticos diarios, cifrados con AES-256.
- Prueba de restauración completa mensual.
- Copias replicadas en nube segura (infraestructura contratada).

Seguridad de Software y Servicios Web

- Todo sistema web pasa por revisión de código y test de OWASP Top 10.
- Implementación de CSP, X-Frame-Options y otros headers de seguridad.
- Actualización mensual obligatoria de CMS y frameworks.

Perímetro y Red

- Firewalls perimetrales y segmentación de red por función.
- IDS/IPS activos en el datacenter institucional.
- Todo tráfico externo pasa por inspección TLS y filtrado de paquetes.

4Geeks

Revisión y Validación

- La Unidad de Seguridad de la Información es responsable de auditar la aplicación de estos controles.
- Cada nuevo sistema deberá pasar por un checklist de cumplimiento SGSI.
- Se documentan las excepciones y se revisan cada 6 meses.

4Geeks

Políticas y Procedimientos

Establecer las políticas generales y procedimientos operativos necesarios para garantizar que la seguridad de la información sea gestionada de forma coherente, repetible y auditada dentro del Instituto Nacional de Estadísticas (INE).

Estas políticas se alinean con los requisitos de la ISO/IEC 27001:2022 y son de aplicación obligatoria para todo el personal, contratistas y terceros con acceso a sistemas del INE.

Políticas Principales del SGSI

Política	Resumen
Política General de Seguridad	Define el compromiso institucional con la seguridad, principios CIA y gobernanza del SGSI.
Control de Accesos	Regula el uso de roles, MFA, privilegios mínimos, y auditoría de accesos.
Gestión de Respaldo y Recuperación	Establece los mecanismos de respaldo diario, pruebas de restauración y cifrado de datos.
Gestión de Incidentes	Describe la clasificación, flujo de reporte, mitigación, comunicación y cierre de incidentes.
Capacitación y Concienciación	Obliga a la formación anual en ciberseguridad y simulacros de ingeniería social.

Procedimientos Estandarizados

Procedimiento	Puntos clave
Alta/Baja/Modificación de usuarios	Autorización formal, asignación por rol, revocación inmediata al egreso.
Gestión de cambios de TI	Evaluación de impacto, autorización, pruebas previas, documentación obligatoria.
Restauración ante incidente	Identificación de respaldo, validación de integridad, recuperación en entorno controlado.
Respuesta a phishing	Reporte inmediato, contención del acceso, análisis de logs, comunicación interna.
Clasificación de información	Etiquetado de datos: Crítico, Alto, Medio, Bajo. Se aplican controles según nivel.

Revisión y Actualización

- Todas las políticas son revisadas anualmente o tras eventos mayores.
- Las actualizaciones son aprobadas por el Comité de Seguridad de la Información.
- La versión vigente está publicada en la intranet institucional.

Cumplimiento y Sanciones

El incumplimiento de las políticas será evaluado como falta administrativa, y puede derivar en:

- Reporte a Recursos Humanos
- Suspensión de accesos
- Investigaciones internas o externas
- Notificación a la Contraloría General si corresponde

Gestión de incidentes de seguridad

Establecer un proceso estructurado y eficaz para la detección, reporte, análisis, contención, mitigación y documentación de incidentes de seguridad de la información en el Instituto Nacional de Estadísticas (INE). El objetivo final es minimizar el impacto de los incidentes, recuperar la normalidad operativa en el menor tiempo posible y preservar evidencia cuando sea necesario. Este procedimiento aplica a:

- Todos los incidentes de seguridad que afecten la información, sistemas, redes, dispositivos o personal del INE.
- Todo el personal institucional y proveedores tecnológicos.
- Cualquier evento que implique pérdida, alteración, divulgación o acceso no autorizado a información institucional.

4Geeks

Tipos de incidentes cubiertos

Tipo de Incidente	Ejemplos
Confidencialidad	Fuga de microdatos, accesos no autorizados, archivos mal compartidos.
Integridad	Modificación no autorizada de estadísticas o bases de datos.
Disponibilidad	Ataques DoS/DDoS, caídas de servicios, ransomware.
Ingeniería social	Phishing, vishing, llamadas de suplantación.
Malware y código malicioso	Ransomware, troyanos, spyware.

Clasificación por severidad

Nivel	Descripción	Ejemplo
Nivel 1	Incidente menor, sin afectación a operaciones ni datos	Usuario olvidó contraseña
Nivel 2	Afecta un sistema o servicio con impacto limitado	Malware detectado en PC de oficina regional
Nivel 3	Afecta servicios críticos o involucra fuga de datos personales	Fuga de microdatos, ransomware en servidores

Flujo de gestión de Incidentes

1. DETECCIÓN: Reporte por usuarios, sistemas de monitoreo, alertas CSIRT.
2. CONTENCIÓN: Aislar sistemas, detener procesos, bloquear accesos.
3. ANÁLISIS: Identificar causa raíz, tipo de ataque, alcance.
4. ERRADICACIÓN: Eliminar software malicioso, restaurar configuraciones.
5. RECUPERACIÓN: Validar respaldos, restaurar servicios, seguimiento.
6. LECCIONES APRENDIDAS: Documentar hallazgos, actualizar políticas, capacitar.

Roles y Responsable

Rol / Unidad	Responsabilidad
CSIRT INE	Coordinación técnica del incidente, comunicación con CSIRT Gobierno
Departamento Seguridad de la Información	Documentación, análisis post-incidente, medidas de mejora
Subdirección TIC	Contención técnica, bloqueo, restauración
Comité de Seguridad	Revisión de incidentes graves, evaluación institucional
Funcionario afectado / informante	Reporte inmediato al CSIRT o mesa de ayuda

4Geeks

Registro y Documentación

Todos los incidentes deben registrarse en el Sistema de Gestión de Incidentes SGSI, incluyendo:

- Fecha y hora de detección
- Persona que lo reportó
- Activos involucrados
- Impacto
- Acciones tomadas
- Tiempo de respuesta y resolución
- Recomendaciones posteriores

4Geeks

Capacitación y Concientización

Establecer un programa permanente de formación, sensibilización y evaluación en materia de seguridad de la información para todos los funcionarios, contratistas y colaboradores del Instituto Nacional de Estadísticas (INE), con el fin de:

- Reducir los riesgos de incidentes provocados por errores humanos o negligencia.
- Fomentar una cultura organizacional alineada con la seguridad y protección de datos.
- Asegurar el cumplimiento normativo de leyes como la Ley 19.628, la Ley de Ciberseguridad 21.663 y la política SGSI institucional.

Esta política aplica a:

- Funcionarios de planta y contrata del INE.
- Personal a honorarios o en misión estadística temporal.
- Personal externo con acceso a sistemas o datos del INE.
- Directivos y altos cargos (formación especializada).

Plan anual de capacitación

Actividad	Periodicidad	Formato	Responsable
Curso de Ciberseguridad Básico	Anual (obligatorio)	E-learning + evaluación	Departamento Seguridad de la Información
Taller presencial de protección de datos	Anual	Presencial o remoto	Unidad de Transparencia
Simulacros de Phishing	Trimestral	Simulaciones reales por correo	Subdep. Ciberseguridad
Inducción SGSI nuevos funcionarios	En cada ingreso	Presencial / online	Recursos Humanos
Boletines de concienciación	Mensual	Mail / intranet / afiches	Unidad de Comunicaciones Institucional

Contenidos mínimos por nivel

Nivel de Usuario	Temas Clave
Básico (todo el personal)	Contraseñas seguras, phishing, dispositivos seguros, uso correcto del correo institucional
Intermedio (personal técnico)	Seguridad de endpoints, VPN, cifrado, backups, actualización de sistemas
Avanzado (TI y analistas)	Políticas SGSI, tratamiento de incidentes, análisis de logs, amenazas persistentes (APT)
Directivo	Riesgos reputacionales, cumplimiento legal, liderazgo en seguridad

4Geeks

Evaluación y Registro

- Todos los cursos incluyen una evaluación obligatoria.

- Se requiere al menos un 80% de aprobación para ser considerado “capacitado”.
- Se mantiene un registro centralizado de cumplimiento en el sistema de Recursos Humanos.
- El cumplimiento se reporta como KPI del SGSI.

Reforzamiento y mejora continua

- Cada incidente de seguridad de Nivel 2 o 3 con causa humana será seguido por un reentrenamiento específico.
- Se realizarán encuestas anuales de percepción en seguridad.
- El Comité de Seguridad evalúa la eficacia del plan anualmente y propone mejoras.