Proyecto Planificación SGSI

4Geeks Academy

FELIPE ALONSO GOMEZ HENRY
ESTUDIANTE BOOTCAMP CIBERSEGURIDAD

4Geeks

Contenido

4Geeks

Alcance definido SGSI

Organismo: Instituto Nacional de Estadísticas (INE)

Fecha: 12-05-2025

Version: 1.0

Responsable: Felipe Gómez H

Introducción

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, en concordancia con la Ley 19.628, la Ley 20.285 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.

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

4Geeks

Resultados de la evaluación de riesgos

Identificación de activos de información

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

Evaluación de riesgos – Amenazas y Vulnerabilidades

ID	Amenaza Potencial	Vulnerabilidad Identificada	Forma de explotación
A1	Acceso no autorizado	Ausencia de control de acceso granular.	Acceso directo desde sistemas internos o cuentas comprometidas.
A2	Interrupción del servicio (DoS/DDoS)	Falta de protección contra tráfico malicioso.	Ataque volumétrico sobre endpoints de recolección.
A3	Desfiguración del sitio (defacement)	Actualizaciones no aplicadas a CMS / plugins.	Explotación de vulnerabilidad conocida (ej. CVE de WordPress/Drupal).
A4	Ransomware o borrado malicioso	Acceso administrativo compartido o sin MFA.	Phishing o malware en cuentas privilegiadas.
A5	Robo o pérdida de los dispositivos	Sin cifrado completo del dispositivo ni control remoto de borrado.	Robo de tablet con datos temporales almacenados.
A6	Ingeniería social / suplantación	Ausencia de capacitación en seguridad	Llamadas falsas solicitando datos o accesos
A7	Escaneo y pivoting lateral	Red mal segmentada / puertos expuestos innecesariamente.	Compromiso de una estación y exploración del resto de la red
A8	Corrupción de respaldos	Almacenamiento local sin validación periódica.	Fallo en recuperación por pruebas no realizadas
A9	Fuga de información confidencial	Almacenamiento no controlado (discos compartidos o nube sin permisos).	Descarga accidental desde usuarios sin autorización
A10	Man-in-the-middle (MITM) en transferencia	Falta de cifrado TLS 1.2+ o autenticación mutua entre sistemas.	Ataque desde red comprometida interceptando intercambio de datos
A11	Acceso no autorizado	Configuración incorrecta de permisos IAM o políticas públicas de acceso	Enumeración de recursos abiertos + uso de credenciales filtradas
A12	Inyección de código (XSS/HTML)	Falta de sanitización en filtros o campos de búsqueda	Usuario malicioso inyecta script persistente en dashboard compartido.

4Geeks

Para clasificar las vulnerabilidades potenciales se utilizará una matriz de riesgo cualitativa, basada en dos factores:

1) Probabilidad:
   a) Alta (3): ocurre frecuentemente o es muy probable
   b) Media (2): podría ocurrir en ciertas condiciones
   c) Baja (1): improbable, pero posible
2) Impacto:
   a) Alto (3): afectación severa a datos, operaciones o cumplimiento legal
   b) Medio (2): impacto operativo o reputacional moderado
   c) Bajo (1): afectación menor, fácilmente controlable

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

4Geeks

Lista de controles seleccionados

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

Políticas y procedimientos de seguridad de la información en INE

1. Política General de Seguridad de la Información

1.1. Objetivo

Establecer las directrices fundamentales para garantizar la seguridad de la información procesada, almacenada y transmitida por el Instituto Nacional de Estadísticas (INE), asegurando la confidencialidad, integridad y disponibilidad de los activos de información, conforme a lo establecido en la Política Institucional de Seguridad de la Información del INE, la Ley N° 19.628 sobre Protección de la Vida Privada, y la Ley Marco de Ciberseguridad N° 21.663.

1.2. Alcance

Esta política aplica a:

- Todo el personal del INE, incluyendo funcionarios, contratistas y encuestadores.
- Todos los activos físicos y digitales relacionados con el procesamiento de información estadística.
- Procesos internos y sistemas tecnológicos utilizados en la recolección, almacenamiento, análisis y publicación de datos.

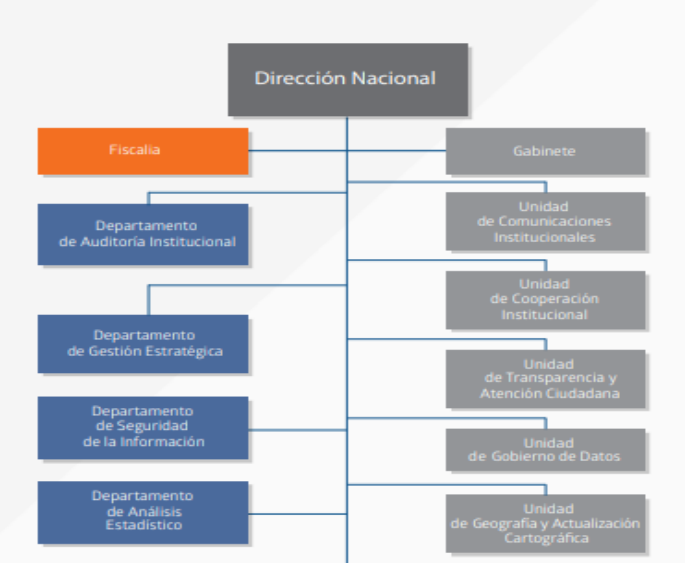
1.3. Principios de Seguridad

Principios que rigen las practicas necesarias para garantizar que los engranajes de seguridad funcionen como es debido:

- Confidencialidad: acceso solo a personas autorizadas.
- Integridad: la información debe mantenerse exacta, sin alteraciones no autorizadas.
- Disponibilidad: los sistemas y datos deben estar accesibles cuando se necesiten.

1.4. Compromiso de la Dirección

La Alta Dirección del INE respalda y financia el SGSI como una función estratégica de soporte institucional. Se establece el Comité de Seguridad de la Información como ente rector del cumplimiento, revisión y mejora continua del SGSI.



2. Procedimiento de Control de Accesos

2.1. Objetivo

Establecer controles técnicos y administrativos que regulen el acceso a los sistemas, aplicaciones, bases de datos y redes del INE.

2.2. Lineamientos

- Todo acceso debe estar respaldado por una autorización formal y documentada.
- Se debe aplicar el principio de mínimo privilegio y control por roles (RBAC).
- Accesos privilegiados requieren autenticación multifactor (MFA).

- El acceso a microdatos y sistemas críticos debe ser auditado y monitoreado en tiempo real.

2.3. Gestión de Usuarios

- Creación: Validación por Recursos Humanos + Autorización del área solicitante.
- Modificación: Revisión de cambios de rol o funciones.
- Revocación: Desactivación inmediata al finalizar la relación laboral o contrato.

3. Política de Respaldo y Restauración

3.1. Objetivo

Garantizar la continuidad operativa y la recuperación de información en caso de pérdida, corrupción o ataque.

3.2. Directrices

- Todos los sistemas críticos deben contar con copias de seguridad diarias automáticas.
- Las copias deben almacenarse en localización geográficamente separada (cloud o segundo datacenter).
- Debe realizarse una prueba de restauración completa cada mes.
- Los respaldos deben estar cifrados (AES-256) y protegidos contra escritura posterior.

4. Gestión de Incidentes de Seguridad

4.1. Objetivo

Establecer un protocolo para reportar, analizar y mitigar incidentes de seguridad de la información en el INE.

4.2. Clasificación de Incidentes

- Nivel 1: Fallas menores sin impacto sobre operaciones.
- Nivel 2: Accesos indebidos, infecciones, pérdida de datos no sensibles.
- Nivel 3: Fugas de microdatos, ransomware, interrupción de servicios críticos.

4.3. Protocolo de Actuación

- Detección y reporte inmediato al CSIRT interno del INE.
- Contención y aislamiento del activo afectado.
- Análisis forense si corresponde.
- Remediación y restauración.
- Lecciones aprendidas y documentación del incidente.

5. Política de Capacitación y Concienciación

5.1. Objetivo

Fomentar una cultura institucional de seguridad de la información.

5.2. Lineamientos

- Todos los funcionarios deben realizar un curso anual de ciberseguridad.
- Se realizarán campañas semestrales con afiches, cápsulas de video y simulaciones de phishing.
- La asistencia y evaluación del personal será registrada como parte de los KPIs del SGSI.