



Ministerio de Economía y Finanzas
Auditoría Interna de la Nación

Norma Técnica: Seguridad de la Información



Temario

- | | |
|----|------------------------------------|
| 01 | Necesidad y fundamento de la norma |
| 02 | Objetivo de la norma |
| 03 | Marco normativo de referencia |
| 04 | Estructura de la norma |
| 05 | Actividades Propuestas 2026 |



Marco de Ciberseguridad de AGESIC: referencia para auditorías exhaustivas.



Necesidad de una herramienta práctica para auditorías internas de seguridad de la información.



Apoyo técnico en la aplicación de la norma.





Establecer un conjunto simplificado y operativo de requisitos para auditorías internas de seguridad de la información



Apoyar a los auditores no especialistas en la evaluación de controles en materia de Seguridad de la Información.



Asegurar alineación con el Marco de Ciberseguridad de AGESIC y buenas prácticas



Eficiencia, uniformidad y trazabilidad

Marco de Ciberseguridad de AGESIC: selección de requisitos relevantes y aplicables priorizados según riesgo y experiencia en auditorías internas.

Estándares internacionales, principalmente ISO/IEC 27001, para garantizar alineación con buenas prácticas globales.



- Organizada en 8 módulos que cubren los principales dominios de seguridad de la información.
- Cada módulo agrupa riesgos, controles y procedimientos de auditoría para evaluar el diseño y la efectividad de los controles.
- Incluye áreas estratégicas y operativas
- Visión integral y ordenada





GOBERNANZA, ORGANIZACIÓN Y GESTION DE RIESGOS

- Estructuras formales de gobernanza y roles claros
- Procesos para identificar y gestionar los riesgos
- Cumplimiento de requisitos normativos y contractuales



GESTIÓN DE ACTIVOS

- Identificación y clasificación de activos de información
- Protección y control de información crítica
- Responsabilidad y custodia de activos



CONTROL DE ACCESO Y SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

- Gestión de accesos
- Capacitación del personal
- Acuerdos de confidencialidad



GESTIÓN DE CAMBIOS EN SISTEMAS DE INFORMACIÓN

- Evaluación de impacto y aprobación previa
- Comunicación a las partes interesadas
- Revisión posterior



RELACIONAMIENTO CON TERCERAS PARTES

- Contratos y SLA
- Evaluación de seguridad
- Cláusulas de seguridad, confidencialidad y continuidad



GESTIÓN DE LA CONTINUIDAD OPERATIVA E INCIDENTES DE SEGURIDAD

- Proceso de gestión de incidente
- Capacitación periódica
- Plan de recuperación y continuidad de las operaciones.



SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA

- Configuración segura de equipos y redes
- Gestión de parches
- Acceso remoto (Teletrabajo)



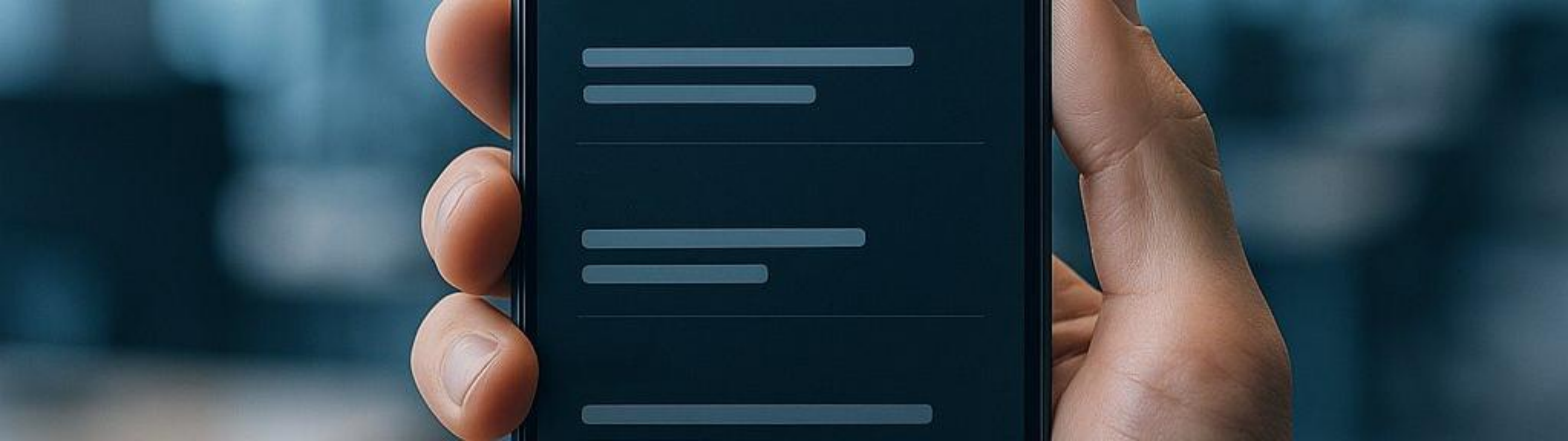
SEGURIDAD FÍSICA

- Control de acceso a áreas críticas y equipos
- Protección contra riesgos ambientales
- Almacenamiento seguro y control de acceso a documentos físicos.

- Apoyo técnico en la implementación de la norma
- Feedback de las UAI
- Revisión y mejora continua







Gracias