ISO/IEC 27001:2022

Anexo A

Organización por categorías lógicas.

Categorías lógicas: ISO/IEC 27001:2022

Categoría 1: Políticas y Gobernanza de Seguridad

Esta categoría establece el marco estratégico y de gobernanza para el SGSI, definiendo políticas, roles, responsabilidades y la dirección general de la seguridad de la información.

Control 5.1 - Políticas de Seguridad de la Información

Conjunto de políticas documentadas y aprobadas por la dirección que establecen el compromiso organizacional con la seguridad.

Control 5.2 - Roles y Responsabilidades de Seguridad

Definición clara de roles (CISO, oficiales de seguridad, propietarios de activos) y sus responsabilidades específicas.

Control 5.3 - Segregación de Funciones

Separación de funciones críticas para prevenir fraude, errores y conflictos de interés.

Control 5.4 - Responsabilidades de la Dirección

Compromiso demostrable de la alta dirección con el SGSI, incluyendo provisión de recursos y revisiones periódicas.

Control 5.35 - Revisión Independiente de la Seguridad

Auditorías independientes para verificar efectividad y conformidad del SGSI.

Control 5.36 - Cumplimiento de Políticas y Estándares

Procesos para asegurar cumplimiento de políticas internas, requisitos legales y contractuales.

Controles en esta categoría: 5.1, 5.2, 5.3, 5.4, 5.35, 5.36

Categoría 2: Gestión de Activos y Clasificación

Identificación, clasificación, etiquetado y protección de activos de información según su criticidad y sensibilidad.

Control 5.9 - Inventario de Activos

Mantenimiento de inventario actualizado de todos los activos de información (hardware, software, datos, servicios).

Control 5.10 - Uso Aceptable de Activos

Políticas que definen uso apropiado de activos organizacionales, incluyendo dispositivos personales (BYOD).

Control 5.11 - Devolución de Activos

Procedimientos para devolución de activos al terminar empleo, contrato o proyecto.

Control 5.12 - Clasificación de la Información

Esquema de clasificación (Público, Interno, Confidencial, Secreto) basado en valor, requisitos legales y criticidad.

Control 5.13 - Etiquetado de Información

Etiquetado físico y electrónico de información según su clasificación para facilitar manejo apropiado.

Control 5.14 - Transferencia de Información

Controles para proteger información durante transferencia (cifrado, canales seguros, acuerdos de confidencialidad).

Controles en esta categoría: 5.9, 5.10, 5.11, 5.12, 5.13, 5.14

Categoría 3: Gestión de Riesgos de Seguridad

Proceso sistemático para identificar, evaluar, tratar y monitorear riesgos de seguridad de la información.

Control 5.7 - Intelligence de Amenazas (NUEVO 2022)

Recopilación y análisis de información sobre amenazas emergentes y tendencias de ataques para defensa proactiva.

Control 5.8 - Seguridad de la Información en Gestión de Proyectos

Integración de requisitos de seguridad en metodologías de gestión de proyectos desde la fase de iniciación.

Control 8.8 - Gestión de Vulnerabilidades Técnicas

Identificación, evaluación y remediación de vulnerabilidades en sistemas, aplicaciones e infraestructura.

Control 5.29 - Seguridad Durante Interrupciones

Mantenimiento de seguridad durante situaciones de crisis, desastres o emergencias operacionales.

Control 5.30 - Preparación de TIC para Continuidad del Negocio

Planes y capacidades para mantener operaciones críticas de TI durante interrupciones mayores.

Controles en esta categoría: 5.7, 5.8, 5.29, 5.30, 8.8

Categoría 4: Control de Acceso e Identidad (IAM)

Gestión de identidades, autenticación, autorización y control de acceso a sistemas y datos.

Control 5.15 - Control de Acceso

Políticas y procedimientos para controlar acceso físico y lógico basados en requisitos de negocio y seguridad.

Control 5.16 - Gestión de Identidades

Ciclo de vida completo de identidades: aprovisionamiento, modificación, desaprovisionamiento.

Control 5.17 - Información de Autenticación

Protección de credenciales (contraseñas, tokens, certificados) y gestión segura de secretos.

Control 5.18 - Derechos de Acceso

Asignación, revisión y revocación de derechos de acceso basados en principio de menor privilegio (least privilege).

Control 8.2 - Derechos de Acceso Privilegiados

Controles especiales para cuentas con privilegios administrativos (MFA obligatorio, logging detallado, PAM).

Control 8.3 - Restricción de Acceso a Información

Limitación de acceso a información y funciones de aplicación basada en necesidad de conocer.

Control 8.4 - Acceso al Código Fuente

Protección estricta de repositorios de código fuente con control de versiones y auditoría de cambios.

Control 8.5 - Autenticación Segura

Implementación de autenticación multifactor (MFA) y métodos fuertes de autenticación.

Controles en esta categoría: 5.15, 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5

Categoría 5: Seguridad de Recursos Humanos

Controles relacionados con personal durante todo el ciclo de empleo: pre-contratación, durante empleo y post-terminación.

Control 6.1 - Verificación (Screening)

Verificación de antecedentes de candidatos antes de contratación, proporcional a requisitos de seguridad del rol.

Control 6.2 - Términos y Condiciones de Empleo

Contratos que incluyen responsabilidades de seguridad, acuerdos de confidencialidad y consecuencias de incumplimiento.

Control 6.3 - Concienciación, Educación y Entrenamiento

Programas de capacitación continua en seguridad para todos los empleados, con entrenamiento especializado por rol.

Control 6.4 - Proceso Disciplinario

Procedimientos formales para tratar violaciones de políticas de seguridad.

Control 6.5 - Responsabilidades tras Terminación

Procesos para revocar accesos, recuperar activos y mantener confidencialidad post-empleo.

Control 6.6 - Acuerdos de Confidencialidad o No Divulgación (NDA)

NDAs con empleados, contratistas y terceros que accedan a información sensible.

Control 6.7 - Trabajo Remoto

Políticas y controles técnicos para proteger información cuando se trabaja fuera de instalaciones (VPN, cifrado, MDM).

Control 6.8 - Reporte de Eventos de Seguridad

Canales claros y cultura que fomenta reporte rápido de incidentes, anomalías o debilidades percibidas.

Controles en esta categoría: 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8

Categoría 6: Seguridad Física y Ambiental

Protección física de instalaciones, equipamiento e infraestructura crítica contra accesos no autorizados, daños y interferencias.

Control 7.1 - Perímetros de Seguridad Física

Definición de perímetros de seguridad (externo, edificio, áreas sensibles) con barreras físicas apropiadas.

Control 7.2 - Entrada Física

Controles de acceso físico: tarjetas, biometría, guardias, registros de visitantes.

Control 7.3 - Seguridad de Oficinas, Salas e Instalaciones

Protección de espacios de trabajo, salas de servidores y áreas donde se procesa información sensible.

Control 7.4 - Monitoreo de Seguridad Física

CCTV, alarmas, sensores de movimiento para detección y disuasión de accesos no autorizados.

Control 7.5 - Protección contra Amenazas Físicas y Ambientales

Defensa contra incendios, inundaciones, terremotos, cortes de energía (UPS, generadores, supresión de incendios).

Control 7.6 - Trabajo en Áreas Seguras

Procedimientos especiales para trabajar en zonas de alta seguridad (data centers, salas seguras).

Control 7.7 - Escritorio Limpio y Pantalla Limpia (Clear Desk/Screen)

Políticas para minimizar información sensible visible en escritorios y pantallas cuando no se usan.

Control 7.8 - Ubicación y Protección de Equipos

Colocación estratégica de equipos para minimizar riesgos ambientales y de acceso no autorizado.

Control 7.9 - Seguridad de Activos Fuera de las Instalaciones

Protección de laptops, dispositivos móviles y documentos cuando se transportan o usan fuera de oficinas.

Control 7.10 - Medios de Almacenamiento

Gestión segura de medios físicos (discos, cintas, USB): almacenamiento, transporte, disposición.

Control 7.11 - Servicios de Soporte (Utilities)

Protección de infraestructura de soporte crítica: electricidad, climatización, telecomunicaciones.

Control 7.12 - Seguridad de Cableado

Protección de cables de red y energía contra interceptación, daño o interferencia.

Control 7.13 - Mantenimiento de Equipos

Mantenimiento preventivo y correctivo controlado para mantener disponibilidad y seguridad.

Control 7.14 - Eliminación Segura de Equipos

Sanitización de datos antes de disposición, venta o reutilización de equipos (borrado seguro, destrucción física).

Controles en esta categoría: 7.1 - 7.14 (14 controles)

Categoría 7: Criptografía y Protección de Datos

Uso de técnicas criptográficas para proteger confidencialidad, integridad y autenticidad de información.

Control 8.24 - Uso de Criptografía

Políticas sobre uso de cifrado para proteger información sensible en reposo y en tránsito.

Control 8.1 - Dispositivos de Usuario Final

Protección de laptops, smartphones, tablets mediante cifrado de disco completo (FDE), MDM, antivirus.

Control 8.11 - Enmascaramiento de Datos (NUEVO 2022)

Ofuscación o anonimización de datos sensibles en entornos no productivos (desarrollo, pruebas).

Control 5.33 - Protección de Registros (Logs)

Protección de logs de auditoría contra alteración y acceso no autorizado (integridad criptográfica, almacenamiento seguro).

Control 5.34 - Privacidad y Protección de PII

Controles específicos para proteger información personal identificable según regulaciones (GDPR, CCPA).

Controles en esta categoría: 5.33, 5.34, 8.1, 8.11, 8.24

Categoría 8: Seguridad en Operaciones

Procedimientos y responsabilidades operacionales para mantener procesamiento correcto y seguro de información.

Control 5.37 - Procedimientos Operacionales Documentados

Documentación de procedimientos operativos para tareas rutinarias y de emergencia.

Control 5.20 - Gestión de Cambios

Control formal de cambios en sistemas, aplicaciones, infraestructura para prevenir interrupciones o vulnerabilidades.

Control 5.21 - Gestión de Capacidad

Monitoreo y planificación de capacidad para asegurar desempeño adecuado y prevenir saturación.

Control 5.22 - Separación de Ambientes (Dev/Test/Prod)

Segregación estricta entre ambientes de desarrollo, pruebas y producción.

Control 5.23 - Seguridad de Información en la Nube (NUEVO 2022)

Controles específicos para servicios cloud: selección de proveedores, configuración segura, monitoreo.

Control 8.6 - Gestión de Capacidad Técnica

Monitoreo técnico de uso de recursos (CPU, memoria, almacenamiento, red).

Control 8.9 - Gestión de Configuración (NUEVO 2022)

Documentación y control de configuraciones de hardware, software, servicios y redes.

Control 8.10 - Eliminación de Información

Borrado seguro de información cuando ya no es necesaria, según políticas de retención.

Control 8.12 - Prevención de Fuga de Datos (DLP)

Controles técnicos y procedimentales para prevenir exfiltración no autorizada de datos sensibles.

Control 8.13 - Respaldo de Información (Backup)

Copias de seguridad regulares, almacenamiento offsite, pruebas de restauración.

Control 8.14 - Redundancia de Instalaciones de Procesamiento

Sistemas redundantes, alta disponibilidad, failover automático para servicios críticos.

Control 8.19 - Instalación de Software en Sistemas Operacionales

Control estricto sobre qué software puede instalarse en sistemas de producción.

Controles en esta categoría: 5.20, 5.21, 5.22, 5.23, 5.37, 8.6, 8.9, 8.10, 8.12, 8.13, 8.14, 8.19

Categoría 9: Seguridad en Redes y Comunicaciones

Protección de información en redes y seguridad de servicios de red y comunicaciones.

Control 8.20 - Seguridad de Redes

Implementación de controles de red: firewalls, segmentación, DMZ, VLANs.

Control 8.21 - Seguridad de Servicios de Red

Configuración segura de servicios: DNS, DHCP, NTP, proxies. Desactivación de servicios innecesarios.

Control 8.22 - Segregación de Redes

Separación lógica de redes por nivel de sensibilidad (corporativa, guest, servidores, IoT).

Control 8.23 - Filtrado Web

Control de acceso a sitios web mediante proxies, listas negras/blancas, análisis de contenido.

Control 5.14 - Transferencia de Información

Protección durante transferencia: cifrado en tránsito (TLS/SSL), VPNs, canales seguros.

Controles en esta categoría: 5.14, 8.20, 8.21, 8.22, 8.23

Categoría 10: Desarrollo y Mantenimiento Seguro

Integración de seguridad en el ciclo de vida de desarrollo de software (SDLC) y mantenimiento de aplicaciones.

Control 8.25 - Ciclo de Vida de Desarrollo Seguro (SSDLC)

Metodología que integra seguridad en todas las fases: requisitos, diseño, codificación, testing, despliegue.

Control 8.26 - Requisitos de Seguridad de Aplicaciones

Definición de requisitos de seguridad funcionales y no funcionales desde fase de especificación.

Control 8.27 - Arquitectura y Principios de Diseño Seguro

Aplicación de principios: defensa en profundidad, menor privilegio, fail-safe defaults, separación de funciones.

Control 8.28 - Codificación Segura

Estándares de codificación segura (OWASP), revisiones de código, análisis estático (SAST).

Control 8.29 - Pruebas de Seguridad en Desarrollo y Aceptación

Testing de seguridad: análisis dinámico (DAST), pruebas de penetración, fuzzing.

Control 8.30 - Desarrollo Externalizado

Controles cuando desarrollo es realizado por terceros: escrow de código, auditorías, acuerdos de seguridad.

Control 8.31 - Separación de Ambientes de Desarrollo, Prueba y Producción

Segregación estricta con datos ficticios en dev/test y controles de promoción a producción.

Control 8.32 - Gestión de Cambios (Aplicaciones)

Control de versiones, revisión y aprobación de cambios, deployment controlado.

Control 8.33 - Información de Prueba

Protección o anonimización de datos de producción usados en ambientes de testing.

Control 8.34 - Protección de Sistemas de Información Durante Pruebas de Auditoría

Controles para pruebas de auditoría/penetración que no interrumpan servicios ni comprometan datos.

Controles en esta categoría: 8.25, 8.26, 8.27, 8.28, 8.29, 8.30, 8.31, 8.32, 8.33, 8.34

Categoría 11: Gestión de Incidentes y Continuidad

Respuesta, gestión y recuperación ante incidentes de seguridad e interrupciones del negocio.

Control 5.24 - Planificación y Preparación de Gestión de Incidentes

Plan de respuesta a incidentes con roles, procedimientos, herramientas y contactos definidos.

Control 5.25 - Evaluación y Decisión sobre Eventos de Seguridad

Criterios para clasificar eventos y decidir si constituyen incidentes que requieren escalamiento.

Control 5.26 - Respuesta a Incidentes de Seguridad

Procedimientos de contención, erradicación, recuperación y análisis post-incidente.

Control 5.27 - Aprendizaje de Incidentes

Análisis de causa raíz, lecciones aprendidas, actualización de controles basada en incidentes.

Control 5.28 - Recolección de Evidencia

Procedimientos forenses para preservar evidencia digital en caso de investigaciones o litigios.

Control 5.29 - Seguridad Durante Interrupciones

Mantenimiento de controles de seguridad durante situaciones de crisis o recuperación.

Control 5.30 - Preparación de TIC para Continuidad del Negocio

Planes de continuidad para sistemas críticos, recuperación de desastres (DR), sitios alternos.

Controles en esta categoría: 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 5.30

Categoría 12: Monitoreo, Auditoría y Cumplimiento

Registro, monitoreo, análisis de eventos y cumplimiento con requisitos legales, regulatorios y contractuales.

Control 8.15 - Logging (Registro de Eventos)

Generación, recolección y retención de logs de eventos de seguridad, accesos, cambios.

Control 8.16 - Monitoreo de Actividades

Monitoreo continuo de sistemas, redes, aplicaciones para detectar anomalías y amenazas.

Control 8.17 - Sincronización de Relojes

Sincronización de relojes de sistemas mediante NTP para correlación precisa de eventos.

Control 8.18 - Uso de Programas Utilitarios Privilegiados

Control y logging de uso de herramientas privilegiadas que pueden eludir controles de seguridad.

Control 5.31 - Requisitos Legales, Estatutarios, Regulatorios y Contractuales

Identificación y documentación de requisitos aplicables (GDPR, leyes locales, contratos).

Control 5.32 - Derechos de Propiedad Intelectual

Protección de propiedad intelectual propia y respeto a derechos de terceros (licencias de software).

Control 5.33 - Protección de Registros

Protección de registros y logs contra pérdida, alteración y acceso no autorizado.

Control 5.34 - Privacidad y Protección de Información Personal

Cumplimiento de leyes de privacidad, consentimiento, derechos de sujetos de datos.

Control 5.35 - Revisión Independiente de Seguridad

Auditorías independientes regulares del SGSI por auditores internos o externos.

Control 5.36 - Cumplimiento con Políticas, Reglas y Estándares

Verificación periódica de cumplimiento con políticas internas y estándares técnicos.

Control 8.7 - Protección contra Malware

Controles anti-malware: antivirus, EDR, sandboxing, análisis comportamental.

Controles en esta categoría: 5.31, 5.32, 5.33, 5.34, 5.35, 5.36, 8.7, 8.15, 8.16, 8.17, 8.18

Controles Adicionales: Gestión de Terceros

Aunque integrados en las categorías anteriores, estos controles merecen mención especial por su criticidad en el ecosistema actual de cadena de suministro.

Control 5.19 - Seguridad de la Información en Relaciones con Proveedores

Políticas y procedimientos para gestionar riesgos de terceros que accedan, procesen o almacenen información organizacional.

Control 5.20 - Tratamiento de Seguridad en Acuerdos con Proveedores

Inclusión de requisitos de seguridad en contratos, SLAs, términos de referencia con proveedores.

Control 5.21 - Gestión de Seguridad en la Cadena de Suministro de TIC

Controles específicos para productos y servicios de TI adquiridos: evaluación de proveedores, escrow, auditorías.

Control 5.22 - Monitoreo, Revisión y Gestión de Cambios en Servicios de Proveedores

Supervisión continua del desempeño de seguridad de proveedores, revisiones periódicas, gestión de cambios.

Control 5.23 - Seguridad de Información en el Uso de Servicios Cloud

Controles específicos para SaaS, PaaS, IaaS: configuración segura, gestión de identidades cloud, monitoreo.

Controles relacionados con terceros: 5.19, 5.20, 5.21, 5.22, 5.23

Resumen: 12 Categorías y Distribución de Controles

#	Categoría	Controles	Total
1	Políticas y Gobernanza	5.1-5.4, 5.35-5.36	**6**
2	Gestión de Activos	5.9-5.14	**6**
3	Gestión de Riesgos	5.7-5.8, 5.29-5.30, 8.8	**5**
4	Control de Acceso (IAM)	5.15-5.18, 8.2-8.5	**8**
5	Seguridad de RRHH	6.1-6.8	**8**
6	Seguridad Física	7.1-7.14	**14**
7	Criptografía y Protección	5.33-5.34, 8.1, 8.11, 8.24	**5**
8	Operaciones de Seguridad	5.20-5.23, 5.37, 8.6, 8.9-8.10, 8.12-8.14, 8.19	**12**
9	Seguridad de Redes	5.14, 8.20-8.23	**5**
10	Desarrollo Seguro	8.25-8.34	**10**
11	Gestión de Incidentes	5.24-5.30	**7**
12	Monitoreo y Cumplimiento	5.31-5.36, 8.7, 8.15-8.18	**11**
	TOTAL		**93**

Conclusión

La reorganización de los 93 controles de ISO 27001:2022 en 12 categorías funcionales facilita:

- **Mejor comprensión:** Comprensión holística del alcance de la norma
- **Implementación práctica:** Asignación de responsabilidades por categoría funcional
- **Priorización estratégica:** Identificación de controles prioritarios según perfil de riesgo
- **Presentación ejecutiva:** Comunicación efectiva con stakeholders no técnicos
- **Integración con otras normas:** Mapeo simplificado con otras normas (PCI DSS, SOC 2, NIST)

Esta estructura de 12 categorías no sustituye la numeración oficial de ISO, pero proporciona un marco conceptual que mejora significativamente la gestión práctica del SGSI.

Cada organización debe adaptar estos controles a su contexto específico mediante el Statement of Applicability (SoA), justificando inclusiones y exclusiones basándose en evaluación de riesgos y requisitos del negocio.