



Declaración de Aplicabilidad (SoA)

Código: SGSI-ME-01.FO-04
Versión: 2
Fecha: 13/01/2026
Clasificación: USO INTERNO
Página: 1 de 6

Fecha: XX/XX/20XX

CATEGORÍA	ISO 27001:2022	CONTROL	APLICA	JUSTIFICACIÓN DE LA INCLUSIÓN / EXCLUSIÓN	DOCUMENTO RELACIONADO
CONTROLES ORGANIZACIONALES (ISO 27001-A.5)	5.1	Políticas para la seguridad de la información			
	5.2	Roles y responsabilidades en seguridad de la información			
	5.3	Segregación de funciones			
	5.4	Responsabilidades de la dirección			
	5.5	Contacto con autoridades			
	5.6	Contacto con grupos especiales de interés			
	5.7	Inteligencia de amenazas			
	5.8	Seguridad de la información en la gestión de proyectos			
	5.9	Inventario de información y otros activos asociados			
	5.10	Uso aceptable de la información y otros activos asociados			
	5.11	Devolución de activos			
	5.12	Clasificación de la información			
	5.13	Etiquetado de la información			
	5.14	Transferencia de información			
	5.15	Control de acceso			
	5.16	Gestión de identidades			
	5.17	Información de autenticación			
	5.18	Derechos de acceso			



Declaración de Aplicabilidad (SoA)

Código: SGSI-ME-01.FO-04
Versión: 2
Fecha: 13/01/2026
Clasificación: USO INTERNO
Página: 2 de 6

CATEGORÍA	ISO 27001:2022	CONTROL	APLICA	JUSTIFICACIÓN DE LA INCLUSIÓN / EXCLUSIÓN	DOCUMENTO RELACIONADO
	5.19	Seguridad de la información en las relaciones con los proveedores			
	5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores			
	5.21	Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (TIC)			
	5.22	Seguimiento, revisión y gestión de cambios en servicios de proveedores			
	5.23	Seguridad de la información en el uso de servicios en la nube			
	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información			
	5.25	Evaluación y decisión sobre eventos de seguridad de la información			
	5.26	Respuesta a incidentes de seguridad de la información			
	5.27	Aprendizaje de los incidentes de seguridad de la información			
	5.28	Recolección de evidencia			
	5.29	Seguridad de la información durante una interrupción			
	5.30	Preparación para las TIC para la continuidad del negocio			



Declaración de Aplicabilidad (SoA)

Código: SGSI-ME-01.FO-04
Versión: 2
Fecha: 13/01/2026
Clasificación: USO INTERNO
Página: 3 de 6

CATEGORÍA	ISO 27001:2022	CONTROL	APLICA	JUSTIFICACIÓN DE LA INCLUSIÓN / EXCLUSIÓN	DOCUMENTO RELACIONADO
	5.31	Requisitos legales, estatutarios, regulatorios y contractuales			
	5.32	Derechos de propiedad intelectual			
	5.33	Protección de registros			
	5.34	Privacidad y protección de la información de identificación personal (IIP)			
	5.35	Revisión independiente de la seguridad de la información			
	5.36	Cumplimiento con políticas, reglas y normas de seguridad de la información			
	5.37	Procedimientos operativos documentados			
CONTROLES DE PERSONAL (ISO 27001-A.6)	6.1	Selección			
	6.2	Términos y condiciones del empleo			
	6.3	Toma de conciencia, educación y entrenamiento sobre la seguridad de la información			
	6.4	Proceso disciplinario			
	6.5	Responsabilidades después del cese o cambio de empleo			
	6.6	Acuerdos de confidencialidad o no divulgación			
	6.7	Trabajo remoto			
	6.8	Reporte de eventos de seguridad de la información			
CONTROLES FÍSICOS	7.1	Perímetros de seguridad física			
	7.2	Ingreso físico			



Declaración de Aplicabilidad (SoA)

Código: SGSI-ME-01.FO-04
Versión: 2
Fecha: 13/01/2026
Clasificación: USO INTERNO
Página: 4 de 6

CATEGORÍA	ISO 27001:2022	CONTROL	APLICA	JUSTIFICACIÓN DE LA INCLUSIÓN / EXCLUSIÓN	DOCUMENTO RELACIONADO
(ISO 27001-A.7)	7.3	Asegurar oficinas, salas e instalaciones			
	7.4	Supervisión de la seguridad física			
	7.5	Protección contra amenazas físicas y ambientales			
	7.6	Trabajo en áreas seguras			
	7.7	Escritorio y pantalla limpios			
	7.8	Ubicación y protección de los equipos			
	7.9	Seguridad de los activos fuera de las instalaciones			
	7.10	Medios de almacenamiento			
	7.11	Servicios de suministro de apoyo			
	7.12	Seguridad del cableado			
	7.13	Mantenimiento de equipos			
	7.14	Eliminación segura o reutilización de equipos			
CONTROLES TECNOLÓGICOS (ISO 27001-A.8)	8.1	Dispositivos terminales del usuario			
	8.2	Derechos de acceso privilegiados			
	8.3	Restricción de acceso a la información			
	8.4	Acceso al código fuente			
	8.5	Autenticación segura			
	8.6	Gestión de capacidad			
	8.7	Protección contra programas maliciosos (malware)			
	8.8	Gestión de vulnerabilidades técnicas			
	8.9	Gestión de la configuración			
	8.10	Eliminación de información			



Declaración de Aplicabilidad (SoA)

Código: SGSI-ME-01.FO-04
Versión: 2
Fecha: 13/01/2026
Clasificación: USO INTERNO
Página: 5 de 6

CATEGORÍA	ISO 27001:2022	CONTROL	APLICA	JUSTIFICACIÓN DE LA INCLUSIÓN / EXCLUSIÓN	DOCUMENTO RELACIONADO
	8.11	Enmascaramiento de datos			
	8.12	Prevención de fugas de datos			
	8.13	Copia de seguridad de la información			
	8.14	Redundancia de instalaciones de procesamiento de información			
	8.15	Registro			
	8.16	Actividades de monitoreo			
	8.17	Sincronización de reloj			
	8.18	Uso de programas de utilidad privilegiados			
	8.19	Instalación de software en sistemas operativos			
	8.20	Seguridad de redes			
	8.21	Seguridad de servicios de red			
	8.22	Segregación de redes			
	8.23	Filtrado de la web			
	8.24	Uso de criptografía			
	8.25	Ciclo de vida de desarrollo seguro			
	8.26	Requisitos de seguridad de la aplicación			
	8.27	Arquitectura de sistemas seguros y principios de ingeniería			
	8.28	Codificación segura			
	8.29	Pruebas de seguridad en desarrollo y aceptación			
	8.30	Desarrollo subcontratado			



Declaración de Aplicabilidad (SoA)

Código: SGSI-ME-01.FO-04
Versión: 2
Fecha: 13/01/2026
Clasificación: USO INTERNO
Página: 6 de 6

CATEGORÍA	ISO 27001:2022	CONTROL	APLICA	JUSTIFICACIÓN DE LA INCLUSIÓN / EXCLUSIÓN	DOCUMENTO RELACIONADO
	8.31	Separación de los entornos de desarrollo, prueba y producción			
	8.32	Gestión de cambios			
	8.33	Información de las pruebas			
	8.34	Protección de los sistemas de información durante las pruebas de auditoría			