HERRAMIENTA DE MAPEO ISO 27002:2017 - ISO 27002:2022

Este documento describe la relación entre los controles de la norma ISO 27002:2017 y la nueva norma ISO 27002:2022.

CÓDIGO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27002:2017			CÓDIGO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27002:2022	
5	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**	**CONTROLES FUSIONADOS ISO 27002:2017**	**REFERENCIA CONTROL**	
5.1.1	Políticas de seguridad de la información	5.1.1, 5.1.2	5.1	Políticas de seguridad de la información
5.1.2	Revisión de las políticas de seguridad de la información	5.1.1, 5.1.2	5.1	Políticas de seguridad de la información
6.1	**Organización interna**			
6.1.1	Funciones y responsabilidades en materia de seguridad de la información		5.2	Funciones y responsabilidades en materia de seguridad de la información
6.1.2	Segregación de funciones		5.3	Segregación de funciones
6.1.3	Contacto con las autoridades		5.5	Contacto con las autoridades
6.1.4	Contacto con grupos de especial interés		5.6	Contacto con grupos de especial interés
			5.7 (nuevo)	Inteligencia sobre amenazas
6.1.5	Seguridad de la información en la gestión de proyectos	6.1.5, 14.1.1	5.8	Seguridad de la información en la gestión de proyectos
6.2	**Dispositivos móviles y teletrabajo**			
6.2.1	Política de dispositivos móviles		8.1	Dispositivos de punto final del usuario
6.2.2	Teletrabajo		6.7	Trabajo a distancia
7.1	**Antes del empleo**			
7.1.1	Cribado		6.1	Cribado
7.1.2	Condiciones de empleo		6.2	Condiciones de empleo
7.2	**Durante el empleo**			
7.2.1	Responsabilidades de gestión		5.4	Responsabilidades de gestión
7.2.2	Sensibilización, educación y formación en materia de seguridad de la información		6.3	Sensibilización, educación y formación en materia de seguridad de la información
7.2.3	Proceso disciplinario		6.4	Proceso disciplinario
7.3	Cese y cambio de empleo			
7.3.1	Cese o cambio de responsabilidades laborales		6.5	Responsabilidades tras el cese o el cambio de empleo
8.1	**Responsabilidad de los activos**			
8.1.1	Inventario de activos	8.1.1, 8.1.2	5.9	Inventario de información y otros activos asociados
8.1.2	Propiedad de los activos	8.1.1, 8.1.2	5.9	Inventario de información y otros activos asociados
8.1.3	Uso aceptable de los activos	8.1.3, 8.2.3	5.10	Uso aceptable de la información y otros activos asociados
8.1.4	Devolución de activos		5.11	Devolución de activos
8.2	**Clasificación de la información**			
8.2.1	Directrices de clasificación		5.12	Clasificación de la información
8.2.2	Etiquetado de la información		5.13	Etiquetado de la información
8.2.3	Manejo de activos	8.1.3, 8.2.3	5.10	Uso aceptable de la información y otros activos asociados
8.3	**Manejo de los medios de comunicación**			
8.3.1	Gestión de soportes extraíbles	8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Medios de almacenamiento
8.3.2	Eliminación de soportes	8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Medios de almacenamiento
8.3.3	Transferencia de medios físicos	8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Medios de almacenamiento
9.1	**Requisitos empresariales del control de acceso**			
9.1.1	Política de control de acceso	9.1.1, 9.1.2	5.15	Control de acceso
9.1.2	Acceso a redes y servicios de red	9.1.1, 9.1.2	5.15	Control de acceso
9.2	**Gestión del acceso de los usuarios**			
9.2.1	Registro y baja de usuarios		5.16	Gestión de la identidad
9.2.2	Provisión de acceso a los usuarios	9.2.2, 9.2.5, 9.2.6	5.18	Derechos de acceso
9.2.3	Gestión de los derechos de acceso privilegiados		8.2	Derechos de acceso privilegiados
9.2.4	Gestión de la información secreta de autentificación de los usuarios	9.2.4, 9.3.1, 9.4.3	5.17	Información de autentificación
9.2.5	Revisión de los derechos de acceso de los usuarios	9.2.2, 9.2.5, 9.2.6	5.18	Derechos de acceso
9.2.6	Supresión o ajuste de los derechos de acceso	9.2.2, 9.2.5, 9.2.6	5.18	Derechos de acceso
9.3	**Responsabilidades del usuario**			
9.3.1	Uso de información secreta de autenticación	9.2.4, 9.3.1, 9.4.3	5.17	Información de autentificación
9.4	**Control de acceso al sistema y a las aplicaciones**			
9.4.1	Restricción del acceso a la información		8.3	Restricción del acceso a la información
9.4.2	Procedimientos seguros de inicio de sesión		8.5	Autenticación segura
9.4.3	Sistema de gestión de contraseñas	9.2.4, 9.3.1, 9.4.3	5.17	Información de autentificación
9.4.4	Uso de programas de utilidad privilegiados		8.18	Uso de programas de utilidad privilegiados
9.4.5	Control de acceso al código fuente del programa		8.4	Acceso al código fuente
10.1	**Controles criptográficos**			
10.1.1	Política de uso de controles criptográficos	10.1.1, 10.1.2	8.24	Uso de la criptografía
10.1.2	Gestión de claves	10.1.1, 10.1.2	8.24	Uso de la criptografía
11.1	**Zonas seguras**			
11.1.1	Perímetro de seguridad física		7.1	Perímetro de seguridad física
11.1.2	Controles físicos de entrada	11.1.2, 11.1.6	7.2	Entrada física
11.1.3	Asegurar las oficinas, salas e instalaciones		7.3	Asegurar las oficinas, salas e instalaciones
			7.4 (nuevo)	Vigilancia de la seguridad física
11.1.4	Protección contra las amenazas externas y medioambientales		7.5	Protección contra las amenazas físicas y medioambientales
11.1.5	Trabajar en zonas seguras		7.6	Trabajar en zonas seguras
11.1.6	Zonas de entrega y carga	11.1.2, 11.1.6	7.2	Entrada física
11.2	**Seguridad de los equipos**			
11.2.1	Ubicación y protección de los equipos		7.8	Ubicación y protección de los equipos
11.2.2	Servicios públicos de apoyo		7.11	Servicios públicos de apoyo
11.2.3	Seguridad del cableado		7.12	Seguridad del cableado
11.2.4	Mantenimiento de los equipos		7.13	Mantenimiento de los equipos
11.2.5	Retirada de activos	8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Medios de almacenamiento
11.2.6	Seguridad de los equipos fuera de las instalaciones		7.9	Seguridad de los activos fuera de las instalaciones
11.2.7	Eliminación segura o reutilización de los equipos		7.14	Eliminación segura o reutilización de los equipos
11.2.8	Equipo de usuario desatendido		8.1	Dispositivos de punto final del usuario
11.2.9	Política de mesas y pantallas despejadas		7.7	Escritorio y pantalla despejados
12.1	**Procedimientos operativos y responsabilidades**			
12.1.1	Procedimientos operativos documentados		5.37	Procedimientos operativos documentados
			8.10 (nuevo)	Eliminación de información
12.1.2	Gestión del cambio	12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Gestión del cambio
12.1.3	Planificación de la capacidad		8.6	Gestión de la capacidad
12.1.4	Separación de los entornos de desarrollo y operativos		8.31	Separación de los entornos de desarrollo, prueba y producción
12.2	**Protección contra el malware**			
12.2.1	Controles contra el malware		8.7	Protección contra el malware
12.3	**Copia de seguridad**			
12.3.1	Información de respaldo		8.13	Información de respaldo
12.4	**Registro y control**			
12.4.1	Registro de eventos	12.4.1, 12.4.2, 12.4.3	8.15	Registro
12.4.2	Protección de la información de los registros	12.4.1, 12.4.2, 12.4.3	8.15	Registro
12.4.3	Registros del administrador y del operador	12.4.1, 12.4.2, 12.4.3	8.15	Registro
			8.16 (nuevo)	Actividades de seguimiento
12.4.4	Sincronización de relojes		8.17	Sincronización de relojes
12.5	**Control del software operativo**			
12.5.1	Control del software operativo		8.19	Instalación de software en sistemas operativos
12.6	**Gestión de la vulnerabilidad técnica**			
12.6.1	Control de las vulnerabilidades técnicas		8.8	Gestión de las vulnerabilidades técnicas
			8.9 (nuevo)	Gestión de la configuración
12.6.2	Restricciones a la instalación de software		8.19	Instalación de software en sistemas operativos
12.7	**Consideraciones sobre la auditoría de los sistemas de información**			
12.7.1	Controles de auditoría de los sistemas de información		8.34	Protección de los sistemas de información durante las pruebas de auditoría
13.1	**Gestión de la seguridad de la red**			
13.1.1	Controles de red		8.20	Seguridad de las redes
13.1.2	Seguridad de los servicios de red		8.21	Seguridad de los servicios de red
13.1.3	Segregación en las redes		8.22	Segregación de redes
			8.23 (nuevo)	Filtro web
13.2	**Intercambio de información**			
13.2.1	Políticas y procedimientos de intercambio de información	13.2.1, 13.2.2, 13.2.3	5.14	Transferencia de información
13.2.2	Acuerdo sobre la transferencia de información	13.2.1, 13.2.2, 13.2.3	5.14	Transferencia de información
13.2.3	Mensajería electrónica	13.2.1, 13.2.2, 13.2.3	5.14	Transferencia de información
13.2.4	"Acuerdos de confidencialidad o no divulgación"		6.6	Acuerdos de confidencialidad o no divulgación
14.1	**Requisitos de seguridad de los sistemas de información**			
14.1.1	Análisis y especificación de los requisitos de seguridad	6.1.5, 14.1.1	5.8	Seguridad de la información en la gestión de proyectos
14.1.2	Seguridad de los servicios de aplicaciones en las redes públicas	14.1.2, 14.1.3	8.26	Requisitos de seguridad de las aplicaciones
14.1.3	Protección de las transacciones de los servicios de aplicación	14.1.2, 14.1.3	8.26	Requisitos de seguridad de las aplicaciones
14.2	**Seguridad en los procesos de desarrollo y apoyo**			
14.2.1	Política de desarrollo segura		8.25	Ciclo de vida de desarrollo seguro
14.2.2	Procedimientos de control de cambios del sistema	12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Gestión del cambio
14.2.3	Revisión técnica de las aplicaciones tras cambios de plataforma operativa	12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Gestión del cambio
14.2.4	Restricciones a los cambios en los paquetes de software	12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Gestión del cambio
14.2.5	Principios de ingeniería de sistemas seguros		8.27	Arquitectura de sistemas seguros y principios de ingeniería
			8.28 (nuevo)	Codificación segura
14.2.6	Entorno de desarrollo seguro		8.31	Separación de los entornos de desarrollo, prueba y producción
14.2.7	Desarrollo de software subcontratado		8.30	Desarrollo externalizado
14.2.8	Pruebas de seguridad del sistema	14.2.8, 14.2.9	8.29	Pruebas de seguridad en el desarrollo y la aceptación
14.2.9	Pruebas de aceptación del sistema	14.2.8, 14.2.9	8.29	Pruebas de seguridad en el desarrollo y la aceptación
14.3	**Datos de la prueba**			
14.3.1	Protección de los datos de prueba del sistema		8.33	Información de la prueba
15.1	**Seguridad de la información en las relaciones con los proveedores**			
15.1.1	Política de seguridad de la información para las relaciones con los proveedores		5.19	Seguridad de la información en las relaciones con los proveedores
15.1.2	"Abordar la seguridad en los acuerdos con los proveedores"		5.20	Abordar la seguridad de la información en los acuerdos con proveedores
15.1.3	Cadena de suministro de tecnologías de la información y la comunicación		5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC
15.2	**Gestión de la prestación de servicios de los proveedores**			
15.2.1	Seguimiento y revisión de los servicios de los proveedores	15.2.1, 15.2.2	5.22	Seguimiento, revisión y gestión de cambios de los servicios de proveedores
15.2.2	Gestión de los cambios en los servicios de los proveedores	15.2.1, 15.2.2	5.22	Seguimiento, revisión y gestión de cambios de los servicios de proveedores
			5.23 (nuevo)	Seguridad de la información para el uso de servicios en la nube
16.1	**Gestión de incidentes y mejoras en la seguridad de la información**			
16.1.1	Responsabilidades y procedimientos		5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información
16.1.2	Notificación de eventos de seguridad de la información	16.1.2, 16.1.3	6.8	Informes de eventos de seguridad de la información
16.1.3	Informar sobre los puntos débiles de la seguridad	16.1.2, 16.1.3	6.8	Informes de eventos de seguridad de la información
16.1.4	Evaluación y decisión sobre eventos de seguridad de la información		5.25	Evaluación y decisión sobre eventos de seguridad de la información
16.1.5	Respuesta a los incidentes de seguridad de la información		5.26	Respuesta a los incidentes de seguridad de la información
16.1.6	Aprender de los incidentes de seguridad de la información		5.27	Aprender de los incidentes de seguridad de la información
16.1.7	Recogida de pruebas		5.28	Recogida de pruebas
17.1	**Continuidad de la seguridad de la información**			
17.1.1	Planificación de la continuidad de la seguridad de la información	17.1.1, 17.1.2, 17.1.3	5.29	Seguridad de la información durante la interrupción
17.1.2	Implementación de la continuidad de la seguridad de la información	17.1.1, 17.1.2, 17.1.3	5.29	Seguridad de la información durante la interrupción
17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de información	17.1.1, 17.1.2, 17.1.3	5.29	Seguridad de la información durante la interrupción
			5.30 (nuevo)	Preparación de las TIC para la continuidad de la actividad
17.2	**Despidos**			
17.2.1	Disponibilidad de instalaciones para el tratamiento de la información		8.14	Redundancia de las instalaciones de tratamiento de la información
18.1	**Cumplimiento de los requisitos legales y contractuales**			
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	18.1.1, 18.1.5	5.31	Requisitos legales, reglamentarios y contractuales
18.1.2	Derechos de propiedad intelectual		5.32	Derechos de propiedad intelectual
18.1.3	Protección de los registros		5.33	Protección de los registros
			8.12 (nuevo)	Prevención de la fuga de datos
18.1.4	Privacidad y protección de la información personal identificable		5.34	Privacidad y protección de la información personali
			8.11 (nuevo)	Enmascaramiento de datos
18.1.5	Regulación de los controles criptográficos	18.1.1, 18.1.5	5.31	Requisitos legales, reglamentarios y contractuales
18.2	**Revisiones de la seguridad de la información**			
18.2.1	Revisión independiente de la seguridad de la información		5.35	Revisión independiente de la seguridad de la información
18.2.2	Cumplimiento de las políticas y normas de seguridad	18.2.2, 18.2.3	5.36	Cumplimiento de las políticas, reglas y normas de seguridad de la información
18.2.3	Revisión de la conformidad técnica	18.2.2, 18.2.3	5.36	Cumplimiento de las políticas, reglas y normas de seguridad de la información

NQA Certificación, S.L. Calle Mayor 73, 3º. 34001 Palencia, España.
T: 91 859 60 17 E: info@nqa.es @nqaglobal