27001:2022
Controles Tecnológicos

"Los Controles Tecnológicos (Dominio A.8) son el sistema nervioso de la resiliencia organizacional: no se trata de acumular software, sino de orquestar la seguridad desde el código hasta la nube. Desde la gestión de activos y la protección contra malware, hasta el desarrollo seguro y la prevención de fugas, este bloque de la ISO 27001 asegura que la tecnología trabaje para el negocio y no en su contra. En un mundo hiperconectado, tener herramientas sin controles es solo una ilusión de protección; la verdadera transformación digital exige que cada bit de información tenga un guardián y cada acceso, un propósito claro."

27001:2022
Controles Tecnológicos

INFOGRAFÍAS

Pilar 1: Cimientos y Configuración

Pilar 2: Vigilancia y Operaciones

Pilar 3: Ciclo de Vida del Dato y Acceso

Pilar 4: Desarrollo, Cambios y Resiliencia

Ingrid Mora Consultora

27001:2022
Controles Tecnológicos

Pilar 1: Cimientos y Configuración

A8.1 Inventario de Activos
Identificar y catalogar todos los activos del sistema.

A8..9 Gestión de Privilegios
Controlar y asignar acceso basado en roles.

A.8.22 Segregación de Redes
Dividir la red para mejorar la seguridad.

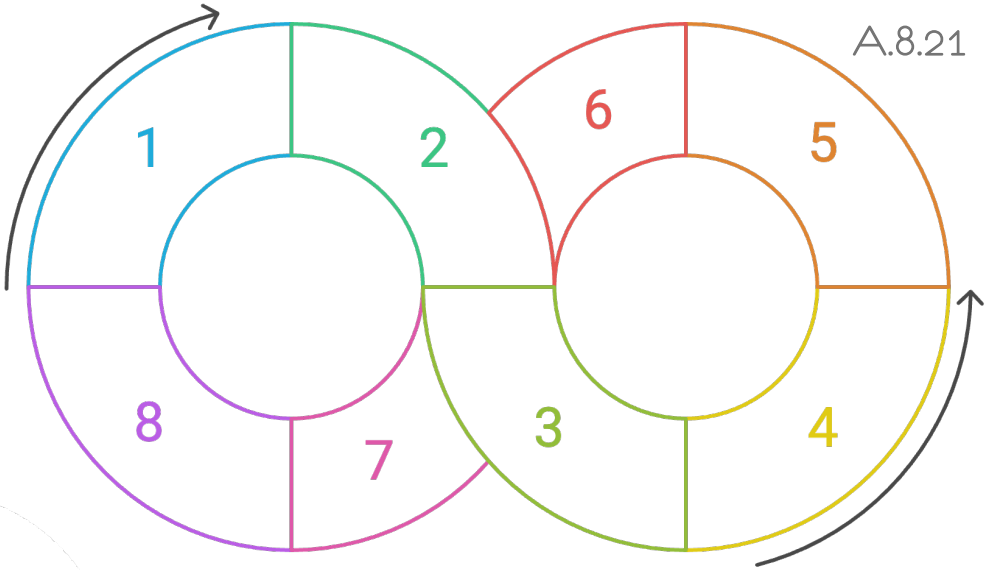
A.8.21 Seguridad de Servicios
Asegurar la protección de los servicios de red.

A.8.20 Controles de Red
Implementar medidas para proteger la red.

A.8.19 Instalación de Software
Instalar software de forma segura y actualizada.

A.8.23 Filtrado Web
Bloquear contenido web malicioso.

A.8.24 Uso de Criptografía
Cifrar datos para proteger la privacidad.



Ingrid Mora Consultora

27001:2022
Controles Tecnológicos

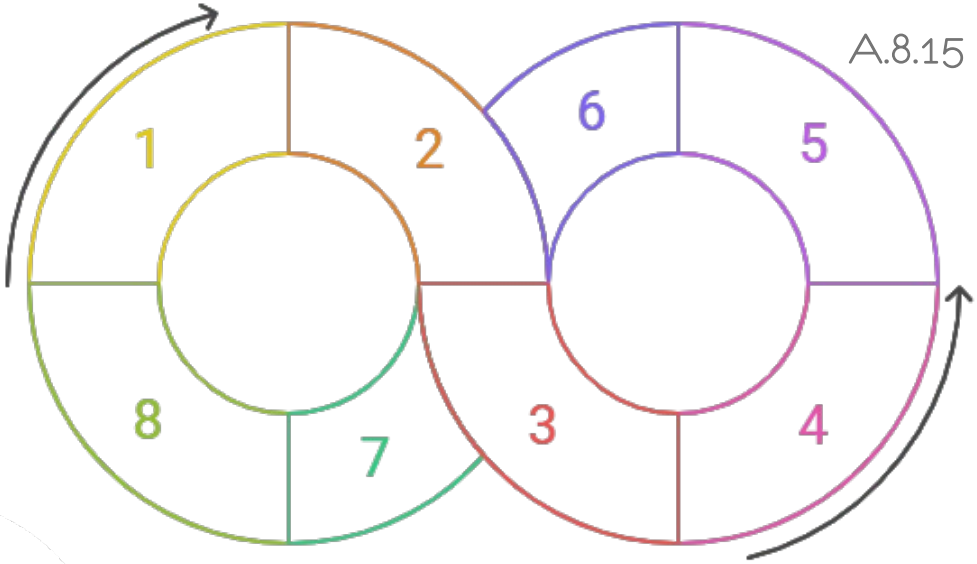
Pilar 2: Vigilancia y Operaciones

Etiquetar Información A8..3
Asignar etiquetas para identificar y proteger

Monitorear Actividades A.8.16
Supervisar el uso del sistema para detectar anomalías

Clasificar Información A8.2
Organizar datos según su sensibilidad

Registrar Eventos A.8.15
Documentar actividades para auditoría



Usar Utilidades Privilegiadas A.8.18
Emplear herramientas avanzadas para tareas de seguridad

Gestionar Vulnerabilidades A.8.8
Identificar y abordar debilidades técnicas

Sincronizar Reloj A.8.17
Asegurar la coherencia temporal en los sistemas

Proteger contra Malware A.8.7
Implementar medidas para prevenir infecciones

Ingrid Mora Consultora

27001:2022
Controles Tecnológicos

Pilar 3: Ciclo de Vida del Dato y Acceso

A8.5 Control de Acceso
Restringir el acceso a datos sensibles

Enmascaramiento de Datos A.8.26
Ocultar información sensible

A8.4 Manejo de Activos
Gestionar y organizar activos de datos

A.8.25 Borrado de Información
Eliminar datos de forma segura

A.8.28 Prevención de Fuga de Datos (Detección)
Monitorear y detectar posibles fugas

A.811 Gestión de Capacidades
Controlar las acciones que los usuarios pueden realizar

A.8.27 Prevención de Fuga de Datos (DLP)
Implementar medidas para evitar fugas

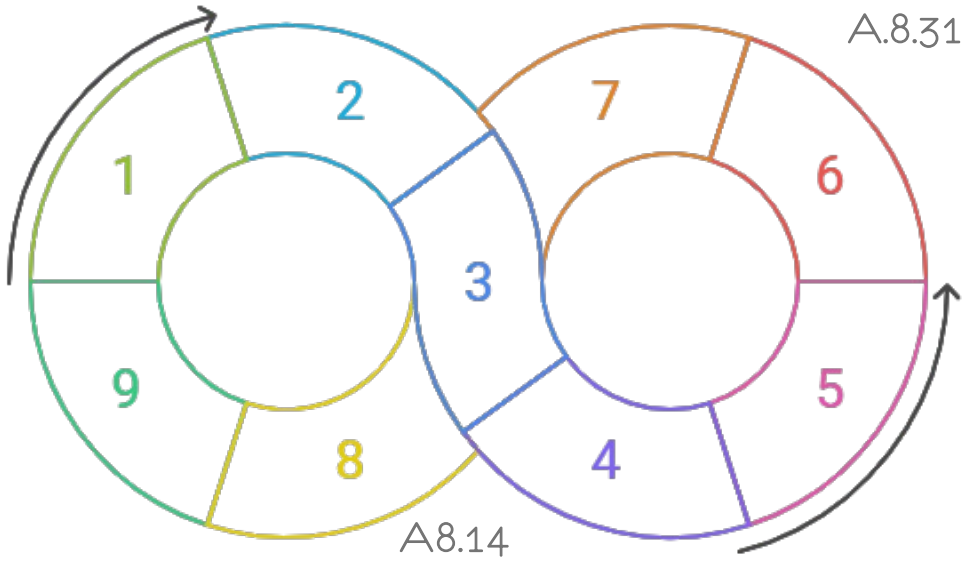
A8.6 Gestión de Derechos de Acceso
Asignar y administrar permisos de acceso

Autenticación de Información Sensible A.8.10
Verificar la identidad de los usuarios

Ingrid Mora Consultora

27001:2022
Controles Tecnológicos

Pilar 4: Desarrollo, Cambios y Resiliencia



A8.13 Seguridad en Desarrollo de Software
Proteger el código durante la creación

A.8.32 Gestión de Cambios
Controlar las modificaciones del sistema

A8.12 Seguridad en Sistemas Operativos
Asegurar la base del sistema

A.8.31 Separación de Entornos
Aislar entornos para seguridad

A.8.30 Desarrollo Externo
Gestionar la seguridad de proveedores externos

A.8.34 Protección de Sistemas
Salvaguardar los sistemas durante las pruebas

A8.14 Información de Prueba
Proteger los datos de prueba

A.8.33 Supervisión de Seguridad
Monitorear el proceso de desarrollo

A.8.29 Pruebas de Seguridad
Evaluar la seguridad antes del lanzamiento

Ingrid Mora Consultora

27001:2022
Controles Tecnológicos

CONTROLES

A.8.1 – A.8.4	Configuración y Desarrollo Seguro
A.8.5 – A.8.9	Autenticación y Vulnerabildades
A.8.10 – A.8.12	Vigilancia y Visibilidad
A.8.13 – A.8.16	Redes, Servicios y Seguridad en la nube
A.8.17 – A.8.20	Software y Red
A.8.21 – A.8.24	Criptografía y Servicios de Red
A.8.25 – A.8.29	Gestión y Protección de la Información
A.8.30 – A.8.32	Ciclo de Vida y Gestión de Cambio

Ingrid Mora Consultora

27001:2022 Configuración y Desarrollo Seguro

Link del artículo complete en:

Controles Tecnológicos

Código	Control	Descripción	Ejemplo práctico Tip de implementación
A.8.1	**Dispositivos de usuario final**	Se deben gestionar los riesgos asociados con los dispositivos que utilizan los usuarios para acceder a la información de la organización.	Implementar un MDM. Práctica: Forzar el cifrado de disco (BitLocker/FileVault) y habilitar el borrado remoto inmediato para casos de robo o pérdida.
A.8.2	**Derechos de acceso privilegiado**	La asignación y uso de derechos de acceso privilegiado debe estar restringida y controlada rigurosamente.	Aplicar el Privilegio Mínimo. Práctica: Eliminar permisos de "Administrador" local a todos los usuarios y usar una herramienta de PAM para otorgar acceso elevado solo bajo demanda y por tiempo limitado.
A.8.3	**Restricción de acceso a la información**	El acceso a la información y a las funciones del sistema debe estar restringido de acuerdo con la política de control de acceso.	Implementar RBAC (Acceso basado en roles). Práctica: Auditar trimestralmente que los accesos de cada empleado coincidan con su función actual; si cambió de puesto, se eliminan los accesos anteriores.
A.8.4	**Acceso al código fuente**	El acceso al código fuente de las aplicaciones debe estar restringido y protegido contra cambios no autorizados.	Blindar el repositorio. Práctica: Exigir MFA (Token físico) para cualquier "Push" al código y bloquear la descarga de repositorios completos a dispositivos que no sean propiedad de la empresa.

27001:2022
Autenticación y Vulnerabilidades

Link del artículo complete en:

Controles Tecnológicos

Código	Control	Descripción	Ejemplo práctico Tip de implementación
A.8.5	**Autenticación segura**	Implementar sistemas que validen la identidad del usuario con la fuerza necesaria según el riesgo.	Elimina la contraseña sola. Práctica: Implementar MFA (Autenticación Multi-Factor) obligatorio para todo acceso externo (VPN, Email, Nube) utilizando notificaciones push o llaves físicas.
A.8.6	**Gestión de vulnerabilidades técnicas**	Se debe obtener información sobre vulnerabilidades y tomar medidas para mitigar el riesgo asociado.	No esperes al ataque. Práctica: Realizar un Escaneo de Vulnerabilidades mensual y aplicar parches críticos en menos de 48 horas tras su detección.
A.8.7	**Protección contra malware**	Implementar controles para detectar, prevenir y recuperarse de software malicioso.	Olvida el antivirus tradicional. Práctica: Desplegar una solución de EDR (Endpoint Detection and Response) que analice comportamientos sospechosos, no solo firmas de virus conocidas.
A.8.8	**Gestión de la configuración**	Las configuraciones de hardware y software deben establecerse, documentarse y monitorearse.	Hardening de sistemas. Práctica: Deshabilitar servicios y puertos innecesarios en los servidores antes de ponerlos en producción (línea base de seguridad).

27001:2022 Vigilancia y Visibilidad

Link del artículo complete en:

Controles Tecnológicos

Ingrid Mora

Código	Control	Descripción	Ejemplo práctico Tip de implementación
A.8.9	**Gestión de registros (Logs)**	Generar y proteger registros de eventos que detallen acciones de usuarios, fallas y anomalías.	Tip: Logs inalterables. Práctica: Configura tus servidores para que envíen los logs a un WORM (Write Once Read Many). Así, aunque un hacker tome control total, no podrá borrar sus huellas.
A.8.10	**Monitoreo de actividades**	Vigilancia activa de los sistemas para identificar comportamientos sospechosos en tiempo real.	Análisis de comportamiento. Práctica: Implementar alertas automáticas si se detecta un acceso desde una IP geográficamente imposible (ej: logueo en CR y 5 minutos después en Rusia).
A.8.11	**Sincronización del reloj**	Asegurar que todos los sistemas tengan la misma hora exacta basada en una fuente confiable.	Fuente de tiempo oficial. Práctica: Sincroniza todo con servidores NTP de estrato 1. Sin esto, en un juicio legal, tus logs no tienen validez porque no hay una línea de tiempo coherente..
A.8.12	**Prevención de fuga de datos (DLP)**	Detectar y prevenir que información sensible sea extraída de la organización sin permiso.	Control de "Exfiltración". Práctica: Configurar el sistema para que bloquee cualquier correo saliente que contenga palabras como "Confidencial", "Plan de Negocios" o números de tarjetas de crédito.

27001:2022 Control de Redes, Servicios y Seguridad en la Nube

Link del artículo complete en:

Ingrid Mora Consultora

Controles Tecnológicos

Código	Control	Descripción	Ejemplo práctico Tip de implementación
A.8.13	**Seguridad en los servicios de red**	Se deben establecer mecanismos de seguridad y niveles de servicio para todos los servicios de red.	Exige SLAs de seguridad. Práctica: Asegurar que tu proveedor de internet o VPN incluya protección contra ataques DDoS y cifrado de extremo a extremo en los contratos.
A.8.14	**Segregación de redes**	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en redes distintas.	Divide y vencerás. Práctica: Crear VLANs separadas para que un invitado conectado al Wi-Fi de la oficina nunca pueda "ver" ni saltar a los servidores donde está la base de datos de clientes.
A.8.15	**Filtrado web**	El acceso a sitios web externos debe ser controlado para reducir la exposición a contenido malicioso.	Bloqueo proactivo. Práctica: Implementar un Proxy o DNS seguro, que impida que los empleados entren a sitios de phishing o descarga de software pirata.
A.8.16	**Seguridad en el uso de servicios en la nube**	Se deben establecer procesos para la adquisición, uso, gestión y salida de los servicios en la nube.	Responsabilidad compartida. Práctica: Realizar una auditoría de configuración de tus "buckets" de S3 o contenedores de Azure para asegurar que no sean públicos por error humano.

27001:2022 Control del Software y la Red

Link del artículo complete en:

WAFRA

Controles Tecnológicos

Ingrid Mora

Código	Control	Descripción	Ejemplo práctico Tip de implementación
A.8.17	**Instalación de software en sistemas operativos**	Se deben establecer y aplicar reglas para la instalación de software por parte de los usuarios.	El inventario es rey. Práctica: Crear un catálogo de software autorizado. Si no está en la lista, el sistema debe bloquear su ejecución automáticamente.
A.8.18	**Uso de privilegios de acceso**	El uso de funciones administrativas y de diagnóstico debe ser restringido y controlado.	No todos son especialistas. Práctica: El acceso a la configuración del servidor debe requerir una llave especial y solo usarse cuando hay una "orden de trabajo" abierta.
A.8.19	**Restricciones de instalación de software**	Implementar controles para prevenir la instalación de software no autorizado.	Candados. Práctica: Configurar los permisos de las laptops para que el usuario necesite una clave de soporte técnico si desea instalar cualquier programa nuevo.
A.8.20	**Seguridad de las redes**	Las redes deben ser protegidas, gestionadas y controladas para asegurar la información.	Pasillos limpios. Práctica: Asegurar que los datos de tus clientes viajen por "túneles" cerrados (VPN) y nunca por canales abiertos donde cualquiera pueda ver la data.

27001:2022 Criptografía y Servicios de Red

Link del artículo complete en:

Ingrid Mora Consultora

Controles Tecnológicos

Código	Control	Descripción	Ejemplo práctico Tip de implementación
A.8.21	**Seguridad de los servicios de red**	Se deben aplicar medidas de seguridad a los servicios de red (como internet o VPN) para proteger la información en tránsito.	Túneles seguros. Práctica: Exigir que cualquier conexión remota pase por una VPN con cifrado fuerte, evitando que el Wi-Fi de un aeropuerto o cafetería "escuche" tus datos.
A.8.22	**Segregación de redes**	Los sistemas y usuarios deben estar divididos en grupos separados para limitar el alcance de un posible ataque.	Aduanas internas. Práctica: Crear una red exclusiva para invitados y otra para contabilidad; si un virus entra por la red de invitados, no podrá "saltar" a tus cuentas bancarias.
A.8.23	**Filtrado web**	El acceso a sitios web externos debe ser controlado para evitar que el personal entre en sitios peligrosos o maliciosos.	Barrera contra el phishing. Práctica: Bloquear automáticamente el acceso a páginas de juegos, descargas piratas o sitios que imitan bancos, reduciendo el riesgo de infección accidental.
A.8.24	**Uso de criptografía**	Establecer reglas claras para cifrar la información sensible y proteger las llaves que la descifran.	Cifrado total. Práctica: Activar el cifrado de disco en todas las laptops de la empresa. Si un empleado olvida su computadora en un taxi, los datos serán solo ruido ilegible para quien la encuentre.

27001:2022 Gestión y Protección de la Información

Link del artículo complete en:

Ingrid Mora Consultora

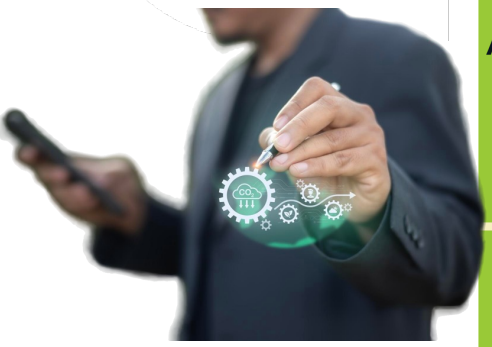
Controles Tecnológicos

Código	Control	Descripción	Ejemplo práctico Tip de implementación
A.8.25	**Borrado de información**	Eliminación definitiva de datos que ya no son necesarios para evitar su recuperación.	El borrado "simple" no existe. Práctica: Usar herramientas de sobreescritura (Wiping) antes de dar de baja un equipo, para que los archivos no sean recuperables con software forense.
A.8.26	**Enmascara-miento de datos**	Ocultar datos sensibles (como nombres o tarjetas) para que solo sean visibles si es estrictamente necesario.	Ver sin tocar". Práctica: Que en tu base de datos de pruebas, los correos reales se conviertan en usuario123@ejemplo.com, protegiendo la identidad real de tus clientes.
A.8.27	**Prevención de fuga de datos (DLP - El Bloqueo)**	Herramientas técnicas que impiden físicamente que un dato sensible salga de la red.	El "Muro" automático. Práctica: Configurar el sistema para que bloquee automáticamente cualquier correo que intente enviar un archivo adjunto con la palabra "Nómina".
A.8.28	**Prevención de la fuga de datos (Monitoreo - La Vigilancia)**	Sistemas que observan y alertan sobre comportamientos sospechosos en la salida de datos.	El "Ojo" supervisor. Práctica: Recibir una alerta si un usuario empieza a copiar archivos masivamente a las 3 AM, aunque el contenido no esté marcado como prohibido.

27001:2022 Ciclo de Vida y Gestión de Cambios

Link del artículo complete en:

Ingrid Mora Consultora



Controles Tecnológicos

Código	Control	Descripción	Ejemplo práctico Tip de implementación
A.8.29	**Seguridad en el ciclo de vida de desarrollo**	Establecer y aplicar reglas de seguridad para el desarrollo de software y sistemas.	Seguridad por diseño. Práctica: Incluir una fase de "Revisión de Seguridad" antes de que cualquier código pase a producción. Si no es seguro, no se publica.
A.8.30	**Seguridad en el desarrollo de software**	Definir requisitos de seguridad para el software desarrollado internamente o por terceros.	Estándares claros. Práctica: Obligar a los programadores a seguir guías como OWASP para evitar errores comunes que permiten a los hackers robar datos fácilmente.
A.8.31	**Separación de entornos de desarrollo, prueba y producción**	Los entornos donde se crea, se prueba y se usa el software deben estar totalmente separados.	Muros lógicos. Práctica: Que un programador nunca tenga acceso a la base de datos real de clientes. Lo que se hace en el "laboratorio" se queda en el laboratorio.
A.8.32	**Gestión de cambios**	Cualquier cambio en los sistemas debe ser planeado, aprobado, ejecutado y revisado.	Nada "al vuelo". Práctica: Usar un sistema de tickets donde cada cambio en un servidor deba ser aprobado por un superior y tener un plan de "marcha atrás" por si algo falla.