

Controles de la ISO 27001 y cómo cumplirlos con ET Seguridad

A continuación, recopilamos qué **controles de la ISO 27001** (recogidos en la guía de implementación del anexo A de dicha norma) puedes cumplir únicamente con la ayuda de ET Seguridad. Sus múltiples funciones otorgan cumplimiento en **32 controles distribuidos en 9 de los 14 apartados que componen la ISO 27001**.

Ten en cuenta que la planificación y posterior implementación del SGSI de una organización debe ajustarse a sus necesidades y objetivos particulares de seguridad, procesos de producción, tamaño y estructura. Asimismo, no es obligatorio cumplir con todos y cada uno de los controles para obtener la certificación con ISO 27001, aunque **implementar tantos como sea posible asegurará certificarse** con éxito.

Apartado 6: Organización de la seguridad de la información

Control	Implementación con ET Seguridad
<p>6.2.1 Política de dispositivos móviles</p> <p>Adoptar políticas para reducir el riesgo que representa el uso de dispositivos remotos en una empresa.</p>	<ul style="list-style-type: none"> » Monitoriza cualquier equipo informático a través de internet, sin necesidad de conexión a una red empresarial. » En caso de perder la conexión a internet, se seguirá monitorizando localmente hasta recuperar la conexión.
<p>6.2.2 Teletrabajo</p> <p>Las medidas de seguridad que se aplican en el sitio de trabajo deberán aplicarse también en caso de teletrabajo.</p>	<ul style="list-style-type: none"> » Monitoriza cualquier equipo informático a través de internet, sin necesidad de conexión a una red empresarial. » En caso de perder la conexión a internet, se seguirá monitorizando localmente hasta recuperar la conexión.

Apartado 8: Gestión de activos

Control	Implementación con ET Seguridad
<p>8.2.2 Etiquetado de la información</p> <p>La información debe ser etiquetada según su clasificación por confidencialidad.</p>	<ul style="list-style-type: none"> » Selecciona los directorios del equipo informático a monitorizar en función del etiquetado.

Control

Implementación con ET Seguridad

8.2.3 Manejo de los activos

Desarrollar procedimientos para el uso, procesamiento, almacenamiento y comunicación de los datos según su clasificación por confidencialidad.

- » Protege con contraseña el acceso a ciertos archivos y aplicaciones del equipo.
- » La monitorización de actividad mantiene un registro de cualquier operación realizada en el equipo.

8.3.1 Gestión de soportes extraíbles

Medidas de control específicas para soportes extraíbles USB. Además de hacer copias de seguridad y mantener un registro de soportes, hay que controlar la transferencia de datos hacia ellos.

- » El registro de actividad monitoriza la información que se copia a cualquier dispositivo extraíble USB conectado al equipo.

8.3.3 Traslado de soportes físicos

Proteger la información almacenada en soportes extraíbles en caso de traslado entre distintas ubicaciones.

- » Usa la herramienta de cifrado para proteger preventivamente los dispositivos USB que vayan a salir de la oficina. Así, en caso de pérdida o robo, evitarás que accedan a su contenido.

Apartado 9: Control de acceso

Control

Implementación con ET Seguridad

9.1.2 Acceso a las redes y a los servicios de red

Determinar las conexiones de red permitidas y cómo se supervisa el uso de los servicios de red.

- » Limita el acceso a las páginas web que tú decidas.
- » Monitoriza y revisa el historial de navegación, aunque se use la navegación privada.

9.2.1 Registro de usuarios y cancelación del registro

Controlar el proceso para realizar altas y bajas de los usuarios.

- » Gestiona los usuarios autorizados y sus permisos en cualquier momento y lugar, mediante el panel de administración en la nube.

9.2.2 Gestión de acceso a los usuarios

Controlar el proceso para asignar y revocar accesos de los usuarios.

- » Controla qué derechos de acceso posee cada usuario desde el panel de administración en la nube.
- » Protege con contraseña el acceso a ciertos archivos y aplicaciones del equipo.

9.2.3 Gestión de derechos de acceso privilegiados

Los derechos de acceso privilegiados deben gestionarse de forma independiente a los otros accesos.

- » Protege con contraseña el acceso a ciertos archivos y aplicaciones del equipo.
- » Limita funciones del equipo informático según el usuario que inicie el software.

9.2.4 Gestión de la información de autenticación secreta de los usuarios

Garantizar que las contraseñas y accesos están protegidas y son confidenciales.

- » Usa la herramienta de cifrado para encriptar con contraseña cualquier documento que contenga información confidencial.

9.2.5 Revisión de derechos de acceso de usuario

Revisar periódicamente los permisos de acceso comunes y privilegiados.

- » Obtén una visión global de todos los dispositivos de la organización desde el panel de administración en la nube.

9.2.6 Remoción o ajuste de los derechos de acceso

Garantizar que se revisan los accesos en caso de promoción o cese de un contrato.

- » Gestiona los usuarios autorizados y sus permisos en cualquier momento y lugar, mediante el panel de administración en la nube.

9.4.1 Restricción del acceso a la información

Restricción selectiva de los derechos de lectura, escritura, eliminación y ejecución según el usuario. Limitación de determinadas funciones del equipo informático y cifrado adicional para datos confidenciales.

- » Protege con contraseña el acceso a ciertos archivos y aplicaciones del equipo.
- » Limita funciones del equipo informático según el usuario que inicie el software.

9.4.2 Procedimientos de conexión (log-on) seguros

El inicio de sesión debe ser capaz de corroborar la identidad del usuario, registrando los intentos fallidos para la detección de posibles ataques.

- » Configura un usuario para cada miembro del equipo con identificador y contraseña únicos.
- » Registra cualquier operación en el equipo informático, incluyendo intentos de acceso fallidos a los programas.
- » Los datos se transfieren a la nube mediante protocolo de conexión seguro. No es posible acceder al registro de forma local.

Control

Implementación con ET Seguridad

9.4.3 Sistema de gestión de contraseñas

Cambiar contraseñas periódicamente y almacenarlas por separado de los sistemas en los que se encuentran las aplicaciones.

- » Gestiona las contraseñas en cualquier momento y lugar, mediante el panel de administración en la nube.
- » Dicha información se almacena en la nube, y no en los equipos monitorizados.
- » Usa la herramienta de cifrado para encriptar con contraseña cualquier documento que contenga información confidencial.

Apartado 10: Criptografía - Cifrado y gestión de claves

Control

Implementación con ET Seguridad

10.1.1 Política sobre el empleo de controles criptográficos

Establecer en qué casos será necesario cifrar archivos y mediante qué herramientas.

- » Usa la herramienta de cifrado incluida en ET Seguridad, equipada con el algoritmo de encriptado de máximo nivel AES 256.

Apartado 12: Seguridad de las operaciones

Control

Implementación con ET Seguridad

12.4.1 Registro de eventos

Mantener un registro de eventos que determine las acciones ejecutadas, los intentos de acceso, la fecha y la hora.

- » Registra todas las operaciones con archivos (leer, escribir, eliminar, mover, renombrar...) e identifica el usuario, la fecha y la hora.

12.4.2 Protección de la información de registros (logs)

Dotar a los registros de un nivel adecuado de protección para evitar pérdidas, corrupción o cambios no autorizados.

- » Los datos se transfieren a la nube mediante protocolo de conexión seguro. No es posible acceder al registro de forma local.

Control

Implementación con ET Seguridad

12.4.3 Registros del administrador y operador

El registro debe realizarse tanto a usuarios como a la cuenta de administrador.

- » Una vez instalado el software en el equipo, no es posible desactivarlo localmente. Todo se gestiona desde el panel de administración en la nube.

12.5.1 Instalación de software en los sistemas operativos

Mantener procedimientos para cubrir las instalaciones de software en cualquier dispositivo dentro de una organización.

- » Registra cualquier operación en el equipo informático, incluyendo la instalación de software.

12.7.1 Controles de auditoría de sistemas de información

Implantar un sistema desde donde evaluar los privilegios de los usuarios, la capacidad de las infraestructuras, el monitoreo de la actividad y la infraestructura de seguridad.

- » Usa la herramienta *Auditoría de Ciberseguridad* para analizar el equipo (infraestructura, hardware y software) con la herramienta CLARA del CCN.
- » Obtén una visión global de todos los dispositivos de la organización desde el panel de administración en la nube.

Apartado 13: Seguridad de las comunicaciones

Control

Implementación con ET Seguridad

13.1.1 Controles de Red

Establecer controles adicionales para mantener las conexiones, la privacidad y la integridad de los datos.

- » Limita funciones del equipo informático según el usuario que inicie el software.
- » Limita el acceso a las páginas web que tú decidas.

13.2.1 Políticas y procedimientos de intercambio de información

Medidas de seguridad para proteger la información que se va a transmitir conforme a la GDPR.

- » Usa la herramienta de cifrado para proteger preventivamente los documentos que vayas a enviar por internet. Así, en caso de interceptación o destinatario erróneo, evitarás que accedan al contenido.

Apartado 14: Adquisición, desarrollo y mantenimiento de los sistemas

Control

Implementación con ET Seguridad

14.2.2 Procedimiento de control de cambio del sistema

Controlar cambios desde la actualización de los navegadores a las actualizaciones de los sistemas operativos.

- » Usa la herramienta *Auditoría de Ciberseguridad* para analizar el equipo (infraestructura, hardware y software) con la herramienta CLARA del CCN.

Apartado 16: Gestión de incidentes de seguridad de la información

Control

Implementación con ET Seguridad

16.1.2 Reporte de eventos de seguridad de la información

Establecer mecanismos de notificación ante cualquier evento, incidente, amenaza o vulnerabilidad en la seguridad de la información.

- » Obtén una visión global de todos los dispositivos de la organización desde el panel de administración en la nube.

16.1.4 Evaluación y decisión sobre los eventos de seguridad de información

Establecer parámetros para determinar la prioridad de cada incidente.

- » Usa la herramienta *Auditoría de Ciberseguridad* para analizar el equipo (infraestructura, hardware y software) con la herramienta CLARA del CCN.

16.1.5 Respuesta a incidentes de seguridad de la información

Controlar el proceso de resolución de incidentes.

- » La monitorización de actividad mantiene un registro de cualquier operación realizada en el equipo.

16.1.7 Recolección de evidencia

Implantar métodos para recuperar las evidencias de un incidente.

- » Consulta el registro de actividad para recabar evidencias del incidente, determinar qué ha ocurrido y cómo resolverlo.
- » Los registros se almacenan en la nube durante un mínimo de 48 meses, conforme dicta la ley.



Apartado 18: Cumplimiento

Control

Implementación con ET Seguridad

18.1.3 Protección de los registros

Clasificar los registros de información y aplicar los controles necesarios según los requisitos legales.

- » Los datos se transfieren a la nube mediante protocolo de conexión seguro. No es posible acceder al registro de forma local.
- » Los registros se almacenan en la nube durante un mínimo de 48 meses, conforme dicta la ley.

18.1.4 Protección de los datos y privacidad de la información personal

Los controles deben cumplir con la legislación vigente LOPD y RGPD.

- » Cada vez que un usuario inicia sesión en su equipo informático, se muestra y debe dar conformidad al aviso LOPD, que le informa sobre la monitorización de su actividad tal y como exige la ley.

18.1.5 Regulación de los controles criptográficos

En España existe obligatoriedad de conservar cifrados los datos personales especialmente sensibles.

- » Usa la herramienta de cifrado incluida en ET Seguridad, equipada con el algoritmo de encriptado de máximo nivel AES 256.



&edorteam
DESDE 1992

Madrid
C/ Isabel Colbrand 6, 5º
28050 Madrid
☎ 91 344 69 10

Lleida
Avenida Madrid 38, 2º-2ª
25002 Lleida
☎ 973 248 601

✉ info@edorteam.com

www.edorteam.com