

# LOS 11 NUEVOS CONTROLES DE ISO27001 VERSIÓN 22

La norma ISO27001 a través de su anexo A desarrollado en la ISO27002 presenta 11 nuevos controles que pasamos a comentar.



**A 5.7 Inteligencia de amenazas**  
Identificación y análisis de factores que incrementan el riesgo de la seguridad.  
Registros: ampliación de la gestión de riesgos.

**A 5.23 Seguridad de la información para el uso de servicios en la nube**  
Identificación de requisitos de seguridad para los servicios en la nube  
Registros: mapa de red, tabla de servicios.

**A 5.30 Preparación para las TIC para la continuidad del negocio**  
Establecer elementos TIC en la gestión de la continuidad.  
Registros: BIA, Plan de continuidad de negocio, simulacros.

**A 7.4 Monitorización de la seguridad física**  
Disponer de indicadores que permitan la toma de decisiones en base a datos.  
Registros: archivos CCTV, BBDD de control de acceso, inspecciones antintrusión,...

**A 8.9 Gestión de la configuración**  
Procedimiento para la gestión de la configuración de hardware, software, servicios y redes.  
Registros: Checking de configuración, banco de pruebas.

**A 8.10 Eliminación de la información**  
Control de plazos de almacenamiento de información física y digital  
Registros: certificados de borrado, logs de eliminación.

**A 8.11 Enmascaramiento de datos**  
Política específica de limitación de exposición de datos.  
Registros: logs de software de enmascaramiento, tickets de ejecución de acciones

**A 8.12 Prevención de fuga de datos**  
Implantación de herramientas que reduzcan el riesgo de fuga de datos. Concienciación.  
Registros: software de monitorización, test de vulnerabilidad, gestión de riesgos, plan de formación.

**A 8.16 Seguimiento de actividades**  
Monitorización de redes, sistemas y aplicaciones orientados a la detección de anomalías.  
Registros: Logs de redes, sistemas, aplicaciones, gestión de riesgos, acciones correctivas

**A 8.23 Filtrado de webs**  
Política de acceso restringido a webs externas y herramientas de limitación de acceso.  
Registros: relación de webs autorizadas, software de gestión de accesos, gestión de incidentes...

**A 8.28 Codificación segura**  
Política de codificación de software identificando potenciales vulnerabilidades del proceso.  
Registros: Tickets de desarrollo que incluya requisitos de seguridad, análisis de vulnerabilidades,...

