Mihai Lucian

Cumplimiento ISO 27001

Checklist de Auditoría. Auditoría Integral para empresas en la nueva era digital.

Cómo usar este checklist?

Marca cada control como **Cumplido (✔), En proceso (⚠) o No cumplido (❌).**
Para cada control, anota evidencias o acciones correctivas.

🔹 Gobierno y Gestión de Seguridad

☐ **¿Existe una política de seguridad de la información documentada y aprobada por la dirección?**
Confirmar que la política esté formalmente documentada, aprobada por la alta dirección y alineada con los objetivos estratégicos de la organización.

☐ **¿Se ha definido un comité o responsable de seguridad de la información?**
Verificar que exista un comité o un CISO encargado de la implementación y supervisión de la seguridad de la información.

🔹 Gestión de Riesgos y Cumplimiento

☐ **¿Se ha implementado un proceso de gestión de riesgos de seguridad de la información?**
Asegurar que la organización cuenta con una metodología de evaluación de riesgos (ISO 27005, OCTAVE, FAIR) para identificar, analizar y mitigar amenazas.

☐ **¿Se realiza una revisión periódica de los controles de seguridad en función del análisis de riesgos?**
Confirmar que los controles de seguridad son revisados y ajustados periódicamente para mitigar nuevas amenazas emergentes.

☐ **¿Se cumple con las normativas aplicables (ISO 27001, GDPR, NIS2, ENS, etc.)?**
Verificar que la organización cumple con los requisitos legales y regulatorios en materia de seguridad de la información.

🔹 Seguridad en Infraestructura y Redes

☐ **¿Se han implementado medidas de segmentación de red y control de tráfico?**
Asegurar que existen segmentaciones adecuadas en la red para minimizar la superficie de ataque y evitar movimientos laterales de amenazas.

☐ **¿Se emplean herramientas SIEM/XDR para la monitorización de eventos de seguridad?**
Verificar que se utilicen soluciones avanzadas de monitoreo y correlación de eventos para la detección temprana de incidentes.

☐ **¿Se aplican configuraciones seguras en dispositivos de red y servidores?**
Confirmar que los sistemas cuentan con configuraciones reforzadas (hardening), incluyendo control de acceso y eliminación de servicios innecesarios.

🔹 Seguridad en la Nube y Aplicaciones

☐ **¿Se realizan auditorías periódicas en entornos cloud (AWS, Azure, Google Cloud)?**
Asegurar que los entornos cloud cumplen con las mejores prácticas de seguridad y configuración según CIS Benchmarks.

☐ **¿Se aplican controles de acceso granular y autenticación multifactor (MFA)?**
Verificar que todos los accesos críticos están protegidos con autenticación multifactor y roles de acceso mínimo necesario (principio de privilegio mínimo).

☐ **¿Se han implementado análisis de seguridad en el desarrollo de software (SAST, DAST, IAST)?**
Confirmar que se realizan pruebas de seguridad en el ciclo de vida del desarrollo de software para prevenir vulnerabilidades en las aplicaciones.

🔹 Protección de Identidad y Control de Accesos

☐ **¿Se gestionan adecuadamente los accesos privilegiados (PAM)?**
Verificar que las cuentas con privilegios elevados están bajo control mediante soluciones de gestión de accesos privilegiados.

☐ **¿Se han implementado políticas de cambio y almacenamiento seguro de credenciales?**
Asegurar que las credenciales están cifradas, almacenadas de forma segura y sujetas a políticas de rotación.

☐ **¿Se auditan los intentos de acceso no autorizados y se aplican respuestas automatizadas?**
Confirmar que se monitorizan los accesos sospechosos y se aplican bloqueos y alertas ante intentos de intrusión.

🔹 Respuesta a Incidentes y Continuidad del Negocio

☐ **¿Existe un plan de respuesta a incidentes documentado y probado regularmente?**
Verificar que la organización cuenta con un procedimiento de respuesta a incidentes y realiza simulacros periódicos.

☐ **¿Se dispone de copias de seguridad protegidas contra ransomware (modelo 3-2-1)?**
Asegurar que existen backups con redundancia y medidas de protección frente a cifrado malicioso.

☐ **¿Se han definido RTO y RPO para garantizar la continuidad del negocio?**
Confirmar que la organización ha establecido tiempos de recuperación adecuados para minimizar el impacto de un incidente.

🔹 Evaluación Final y Priorización de Riesgos

- **100%-80%** → Cumple con los estándares de seguridad, mejoras mínimas necesarias.
- **79%-50%** → Cumple parcialmente, requiere correcciones urgentes en áreas clave.
- **49%-0%** → Alto riesgo, incumplimiento crítico, necesita una estrategia de remediación inmediata.
