GRCForce

Lista de comprobación del modelo de preparación para auditorías

1 de julio de 2026

grcforce.com/es/#contact

Practical governance, risk and compliance guidance for European organisations.

Utilice esta matriz para comprobar si el alcance, las evidencias, la responsabilidad, la cadencia y la cultura son suficientemente sólidos antes de que llegue la presión de una auditoría.

Página 1 — Matriz del modelo de preparación para auditorías

Capa	Qué significa	Comprobación ISO 27001	Comprobación TISAX	Responsable de la evidencia	Estado
Alcance	Los límites están claros y coinciden con la realidad	La declaración de alcance está actualizada y refleja servicios, ubicaciones y sistemas	El alcance de la evaluación coincide con las necesidades de protección de datos de los clientes	Responsable del SGSI / GRC	Verde / Ámbar / Rojo
Evidencias	Las pruebas se generan mediante la operación normal, no en situación de urgencia	Las revisiones de acceso, las decisiones de riesgo y las aprobaciones tienen fecha y están almacenadas	Las evidencias de cada objetivo de control están actualizadas y son verificables	Responsables de controles	Verde / Ámbar / Rojo
Responsabilidad	Cada control tiene una persona responsable identificada	Existe una lista actualizada de responsables de controles	Cada control TISAX tiene una persona responsable	Responsable de GRC / Riesgos	Verde / Ámbar / Rojo
Cadencia	Las revisiones se realizan de forma previsible, no aleatoria	Las revisiones de riesgos, las revisiones por la dirección y las auditorías internas están programadas y se realizan	La preparación TISAX se revisa a intervalos definidos	Responsable del programa	Verde / Ámbar / Rojo
Cultura	La organización eleva los problemas en lugar de ocultarlos	Las conclusiones se comunican y corrigen con transparencia	Las sorpresas se reducen mediante una comunicación abierta	Equipo directivo	Verde / Ámbar / Rojo

Página 2 — 10 comprobaciones críticas de salud

1. La evaluación de riesgos está actualizada

La evaluación de riesgos se ha completado en los últimos 12 meses o después de un cambio significativo. Las decisiones de tratamiento tienen responsables y fechas.

Estado: Preparado / Necesita trabajo / No preparado

2. La Declaración de Aplicabilidad refleja la realidad

La SoA se revisa, justifica y aprueba, y está respaldada por evidencias de implantación.

Estado: Preparado / Necesita trabajo / No preparado

3. El programa de auditoría interna está en funcionamiento

Existe un calendario anual de auditoría interna, se cumple y las conclusiones anteriores se cierran con evidencias.

Estado: Preparado / Necesita trabajo / No preparado

4. Se ha realizado la revisión por la dirección

Las actas formales, las decisiones y las acciones de la revisión por la dirección están documentadas y almacenadas.

Estado: Preparado / Necesita trabajo / No preparado

5. Las políticas están conectadas con la práctica
Las políticas principales se revisan con la periodicidad establecida y coinciden con la forma en que se trabaja realmente en la actualidad.

Estado: Preparado / Necesita trabajo / No preparado

6. Las revisiones de acceso disponen de evidencias
Se realizan revisiones formales de acceso para los sistemas críticos y las evidencias se almacenan en el origen.

Estado: Preparado / Necesita trabajo / No preparado

7. Los controles de proveedores se mantienen
Los proveedores críticos se evalúan dentro del ciclo requerido y se documenta la exposición a subencargados o subprocesadores.

Estado: Preparado / Necesita trabajo / No preparado

8. Los registros de incidentes son exactos y completos
El registro de incidentes está actualizado y revisado, y se han probado las vías de escalado.

Estado: Preparado / Necesita trabajo / No preparado

9. Los objetivos son relevantes y se supervisan
Los objetivos de seguridad tienen metas medibles y son revisados por la dirección.

Estado: Preparado / Necesita trabajo / No preparado

10. Las acciones correctivas están cerradas
Los elementos abiertos tienen responsables identificados, causa raíz, fechas objetivo y condiciones de evidencia para el cierre.

Estado: Preparado / Necesita trabajo / No preparado

Página 3 — Cómo utilizar esta lista

Puntúe su situación actual
Revise de forma honesta la matriz y la lista de 10 puntos con el equipo responsable del alcance del SGSI o de TISAX.

Priorice los puntos débiles
Centre primero la atención en las carencias que puedan provocar una no conformidad mayor, una preocupación del cliente o una trazabilidad de evidencias insuficiente.

Asigne responsables y plazos

Cada elemento abierto necesita una persona responsable, una fecha de cierre realista y una expectativa de evidencia.

Realice una revisión 30 días antes de la auditoría

Vuelva a puntuar la situación 30 días antes de la auditoría. Los elementos que sigan sin estar preparados requieren una decisión de escalado.

Mantenga la lista activa trimestralmente

Utilícela entre auditorías para que la preparación siga formando parte del modelo operativo.

Fallos habituales

Fallo	Cómo se manifiesta	Acción correctiva
Desviación de políticas	Las políticas ya no coinciden con la forma de trabajar	Asignar responsables y revisar trimestralmente
Evidencias creadas solo para la auditoría	Se crean capturas y carpetas durante la preparación	Integrar la generación de evidencias en los flujos normales
Acciones correctivas abiertas	Las conclusiones se reconocen pero no se cierran	Asignar responsables, fechas y condiciones de evidencia
Desajuste del alcance	El alcance del certificado ya no coincide con las operaciones	Revisar anualmente y después de cambios importantes

Siguiente paso con GRCForce

Para evaluar su programa mediante esta lista, solicite una Revisión de Preparación para Auditorías de 30 minutos en https://grcforce.com/es/#contact.