CHECKLIST ISO 27001 **SEGURIDAD EN LA GESTIÓN DE TI**

Con nuestra lista de verificación, puedes descubrir de manera rápida y fácil si tu negocio está adecuadamente preparado para la certificación según ISO/IEC 27001 para un sistema integrado de gestión de la seguridad de la información.

Certificación ISO/IEC 27001: ¡para una evaluación precisa de la gestión de la seguridad de la información!

Las siguientes preguntas están organizadas según la estructura básica de las normas de sistemas de gestión. Si puedes responder afirmativamente a una pregunta, indícalo con una marca de verificación.

De esta manera, podrás ver al instante qué áreas de tu empresa cumplen con los requisitos y cuáles necesitan más trabajo.

Contexto de la organización

- [x] Has desglosado la organización precisa de tu negocio (por ejemplo, en un diagrama organizacional).
- [ ] Has definido el ámbito de aplicación de tu SGSI (especialmente para las partes interesadas).
- [ ] Has elaborado una declaración de aplicabilidad (SoA), que documenta las decisiones sobre la implementación de medidas y las razones para esas decisiones.
- [ ] Has llevado a cabo un análisis del entorno para la integración del SGSI en la empresa.
- [ ] Has realizado un análisis de requisitos sobre los diferentes grupos de interés (partes interesadas).
- [ ] Has compilado una visión general de todos los requisitos legales, reglamentarios y contractuales relevantes que afectan a tu estrategia de seguridad de la información y al SGSI.

Gestión

- [ ] Has definido clara y documentadamente los objetivos y requisitos comerciales relacionados con la política de seguridad de la información en tu empresa.
- [ ] Has definido una estrategia concreta de seguridad de la información..
- [ ] Has definido tu 'alta dirección'; este grupo es responsable de controlar el SGSI de la organización a proteger y decide cómo se asignan los recursos.
- [ ] Has implementado una política de seguridad de la información.

Planificación

- [ ] Tienes un procedimiento de evaluación de riesgos documentado.
- [x] Tienes documentación completa del proceso de evaluación de riesgos y del proceso/plan de manejo de riesgos.
- [x] Tienes todos los registros y resultados de las evaluaciones de riesgos y análisis de riesgos.
- [ ] Tienes documentados todos los registros y resultados del manejo de riesgos.
- [ ] Has definido todos los objetivos de seguridad para tu empresa y partes interesadas.

Soporte

- [ ] Tienes un plan o matriz de comunicación para documentar todas las comunicaciones dentro de la empresa relacionadas con la seguridad de la información.
- [ ] Puedes proporcionar el personal y la infraestructura necesarios para la implementación y control del SGSI.
- [ ] Tienes una estrategia para manejar la información documentada.
- [ ] Has creado descripciones de roles detalladas para los empleados afectados por el SGSI (por ejemplo, ISB y/o CISO o DSB) y has documentado todas las verificaciones de sus competencias.
- [ ] Has creado documentación para el concepto de concienciación y capacitación con respecto al SGSI.
- [ ] Tienes documentos de capacitación para el SGSI y pruebas de que tus empleados han participado en las medidas de capacitación relevantes.

Has definido un procedimiento para las comunicaciones internas y externas. ☐

Operación

Tienes verificación de que los procesos del SGSI se ejecutaron correctamente y que el SGSI está controlado y su rendimiento medido. ☐

Tienes documentación sobre programas de auditoría interna y resultados de auditoría. ☐

Has definido un plan de respuesta a incidentes (IRP) que incluye listas de contactos actuales y planes de escalada. ☐

Tienes documentación completa sobre la estructura de medición para todos los KPI (indicadores clave de rendimiento), así como sobre los resultados de la medición y los informes de gestión resultantes para la escalada. ☐

Tu documentación comprende reglas de comportamiento en caso de irregularidades relacionadas con la seguridad, descripciones de procesos e instrucciones de trabajo para asegurar la prueba, e informes sobre incidentes de seguridad de la información. ☐

Tienes pruebas de los tipos de incumplimientos, de todas las medidas reactivas implementadas y de los resultados de todas las medidas correctivas. ☐

Tienes una visión general de los resultados de la evaluación de riesgos (por ejemplo, informes de evaluación de riesgos, cifras clave de riesgos) y del manejo de riesgos (por ejemplo, informes de pruebas de control, informes de pruebas de penetración). ☐