Checklist ISO 27001 – Gestión de Seguridad IT

DEKRA
Con toda confianza.

Con nuestra lista de verificación, puede averiguar rápida y fácilmente si su empresa está debidamente preparada para la certificación según ISO / IEC 27001 para un sistema integrado de gestión de 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 de acuerdo con la estructura básica de los estándares del sistema de gestión. Si puede responder una pregunta con un sí, márquela con una marca de verificación. De esa forma, puede ver instantáneamente qué áreas de su empresa ya cumplen con los requisitos y qué áreas requieren más trabajo.

Contexto de la organización

- [ ] Ha desglosado la organización precisa de su negocio (por ejemplo, como un diagrama organizativo).
- [ ] Ha definido el área de aplicación de su SGSI (especialmente para las partes interesadas).
- [ ] Ha elaborado una declaración de aplicabilidad (SoA), que documenta las decisiones sobre la implementación de medidas y las razones de esas decisiones.
- [ ] Ha realizado un análisis de entorno para la integración del SGSI en la empresa.
- [ ] Ha realizado un análisis de requisitos sobre los diferentes grupos de interés (stakeholders).
- [ ] Ha compilado una descripción general de todos los requisitos legales, reglamentarios y contractuales relevantes que tienen un efecto en su estrategia de seguridad de la información y el SGSI.

Gestión

- [ ] Ha definido y documentado claramente los objetivos y requisitos comerciales relacionados con la política de seguridad de la información de su empresa.
- [ ] Ha definido una estrategia de seguridad de la información concreta.
- [ ] Ha definido su "alta dirección"; este grupo es responsable de controlar el SGSI de la organización a proteger y decide cómo se despliegan los recursos.
- [ ] Ha implementado una política de seguridad de la información.

Planificación

- [ ] Tiene un procedimiento de evaluación de riesgos documentado.
- [ ] Tiene documentación completa del proceso de evaluación de riesgos y el proceso / plan de manejo de riesgos.
- [ ] Tiene todos los registros y resultados de las evaluaciones y análisis de riesgos.
- [ ] Ha documentado todos los registros y resultados del manejo de riesgos.
- [ ] Ha definido todos los objetivos de seguridad para su empresa y las partes interesadas.

Apoyo

- [ ] Tiene un plan o matriz de comunicación para documentar todas las comunicaciones dentro de la empresa que se relacionan con la seguridad de la información.
- [ ] Puede proporcionar el personal y la infraestructura necesarios para la implementación y el control del SGSI.
- [ ] Tiene una estrategia para manejar la información documentada.
- [ ] Ha creado descripciones detalladas de funciones para los empleados que se ven afectados por el SGSI (por ejemplo, ISB y / o CISO o DSB) y ha documentado toda la verificación de sus competencias.
- [ ] Ha creado documentación para el concepto de sensibilización y formación sobre el SGSI.

Dispone de documentación de formación para el SGSI y prueba de que sus empleados han participado en las acciones formativas pertinentes. ☐

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

Funcionamiento

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

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

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

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

Su documentación comprende reglas de comportamiento en caso de irregularidades relevantes para la seguridad, descripciones de procesos e instrucciones de trabajo para asegurar pruebas e informes sobre incidentes de seguridad de la información. ☐

Tiene pruebas de los tipos de incumplimiento, de todas las medidas reactivas implementadas y de los resultados de todas las medidas correctoras. ☐

Tiene una descripción general de los resultados de la evaluación de riesgos (por ejemplo, informes de evaluación de riesgos, cifras clave de riesgos) y la gestión de riesgos (por ejemplo, informes de pruebas de control, informes de pruebas de penetración). ☐

Le ayudamos a certificar con éxito su sistema de seguridad de la información según ISO / IEC 27001. ¡Póngase en contacto con nuestros expertos hoy mismo!

DEKRA Audits

Tel. +34.93.4792269
E-mail comercial.es@dekra.com
Web www.dekra.es/es/audits/