Checklist de UNE-EN ISO/IEC 27001

Requisitos y preparación para la implementación de la ISO 27001	Descripción	Evidencia	Validación	CHK
1.1 Compromiso de la alta dirección	Establecer políticas y objetivos claros para la gestión de la seguridad de la información	Políticas y objetivos documentados	Revisión de documentación	
1.2 Asignación de recursos	Asegurarse de que se asignen recursos adecuados para la implementación	Presupuesto y asignación de recursos documentados	Revisión de documentación	
1.3 Establecimiento de un comité de seguridad de la información	Establecer un comité de seguridad de la información para supervisar la implementación	Acta de creación del comité y sus miembros	Revisión de documentación	
2.1 Identificación de los activos de información	Identificar los activos de información críticos para la organización	Registro de activos de información	Revisión de documentación	
2.2 Evaluación del riesgo asociado con cada activo	Evaluar el riesgo asociado con cada activo	Matriz de riesgos	Revisión de documentación	
2.3 Establecimiento de un registro de los activos de información	Establecer un registro de los activos de información	Registro de activos de información actualizado	Revisión de documentación	
3.1 Identificación de los riesgos y vulnerabilidades	Identificar los riesgos y vulnerabilidades asociados con los activos de información	Matriz de riesgos y vulnerabilidades	Revisión de documentación	
3.2 Evaluación de la probabilidad y el	Evaluar la probabilidad y el	Evaluación de riesgos	Revisión de documentación	

Requisitos y preparación para la implementación de la ISO 27001	Descripción	Evidencia	Validación	CHK
impacto de cada riesgo	impacto de cada riesgo	documentada		
3.3 Establecimiento de un plan para mitigar los riesgos identificados	Establecer un plan para mitigar los riesgos identificados	Plan de mitigación de riesgos	Revisión de documentación	
4.1 Establecimiento de políticas y procedimientos para el control de acceso	Establecer políticas y procedimientos para el control de acceso	Políticas y procedimientos documentados	Revisión de documentación	
4.2 Implementación de controles de acceso físico y lógico	Implementar controles de acceso físico y lógico	Evidencia de implementación de controles de acceso	Inspección visual	
4.3 Realización de auditorías y revisiones periódicas de los controles de acceso	Realizar auditorías y revisiones periódicas de los controles de acceso	Informe de auditoría y revisión	Revisión de documentación	
5.1 Implementación de métodos de autenticación seguros	Implementar métodos de autenticación seguros	Evidencia de implementación de métodos de autenticación	Inspección visual	
5.2 Establecimiento de políticas y procedimientos para la autorización	Establecer políticas y procedimientos para la autorización	Políticas y procedimientos documentados	Revisión de documentación	
5.3 Realización de auditorías y revisiones periódicas de la autenticación y la autorización	Realizar auditorías y revisiones periódicas de la autenticación y la autorización	Informe de auditoría y revisión	Revisión de documentación	
6.1 Implementación de	Implementar tecnologías de	Evidencia de implementación de	Inspección visual	

Requisitos y preparación para la implementación de la ISO 27001	Descripción	Evidencia	Validación	CHK
tecnologías de seguridad	seguridad como firewalls y sistemas de detección de intrusos	tecnologías de seguridad		
6.2 Establecimiento de políticas y procedimientos para la gestión de las tecnologías de seguridad	Establecer políticas y procedimientos para la gestión de las tecnologías de seguridad	Políticas y procedimientos documentados	Revisión de documentación	
6.3 Realización de auditorías y revisiones periódicas de las tecnologías de seguridad	Realizar auditorías y revisiones periódicas de las tecnologías de seguridad	Informe de auditoría y revisión	Revisión de documentación	
7.1 Establecimiento de un plan de gestión de incidentes y crisis	Establecer un plan de gestión de incidentes y crisis	Plan de gestión de incidentes y crisis	Revisión de documentación	
7.2 Identificación de los roles y responsabilidades de cada persona involucrada	Identificar los roles y responsabilidades de cada persona involucrada	Descripción de roles y responsabilidades	Revisión de documentación	
7.3 Realización de simulacros y ejercicios de gestión de crisis periódicos	Realizar simulacros y ejercicios de gestión de crisis periódicos	Informe de simulacro y ejercicio	Revisión de documentación	
8.1 Activación del plan de gestión de incidentes y crisis en caso de un incidente o crisis	Activar el plan de gestión de incidentes y crisis en caso de un incidente o crisis	Evidencia de activación del plan	Inspección visual	
8.2 Identificación y contención del incidente o crisis	Identificar y contener el incidente o crisis	Evidencia de identificación y contención del incidente o crisis	Inspección visual	
8.3 Realización de	Realizar	Informe de	Revisión de	

Requisitos y preparación para la implementación de la ISO 27001	Descripción	Evidencia	Validación	CHK
investigaciones y análisis de la causa raíz del incidente o crisis	investigaciones y análisis de la causa raíz del incidente o crisis	investigación y análisis	documentación	
9.1 Revisión periódica del plan de gestión de incidentes y crisis	Realizar revisiones periódicas del plan de gestión de incidentes y crisis	Informe de revisión	Revisión de documentación	
9.2 Identificación y corrección de los errores y debilidades del plan	Identificar y corregir los errores y debilidades del plan	Informe de corrección de errores y debilidades	Revisión de documentación	
9.3 Realización de ajustes y mejoras al plan de gestión de incidentes y crisis según sea necesario	Realizar ajustes y mejoras al plan de gestión de incidentes y crisis según sea necesario	Informe de ajustes y mejoras	Revisión de documentación	