**Evidencia No 7.1**

**ISO 27001 (Controles) & Calidad**

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

**PARTE 1.**

La ISO (*International Organization for Standardization*) es la Organización Internacional de Normalización, cuya principal actividad es la elaboración de normas técnicas internacionales, tanto de productos como de servicios, a través de normas voluntarias que usan las empresas para su eficiencia y rentabilidad.

La norma ISO/IEC 27001 es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 y busca cumplir con principios de la tríada de la seguridad: confidencialidad, integridad y disponibilidad de la información. Su objetivo es identificar los riesgos, definiciones de estrategias para evitarlos e implementar salvaguardas.

En ese sentido, ayuda a las organizaciones a establecer la política y los objetivos de gestión de la seguridad de la información y a comprender cómo se pueden gestionar los aspectos importantes, aplicar los controles necesarios y establecer objetivos claros para mejorar la seguridad de la información.

Los controles deben aplicarse para gestionar o reducir los riesgos reales una vez finalizada la evaluación de riesgos. La norma ISO 27001 requiere que se comparen los controles contra su propia lista de controles de buenas prácticas enumerados en el Anexo A.

La declaración de aplicabilidad (SoA) establece una lista de todos los controles del Anexo A de la norma ISO/IEC 27001:2013, junto con una declaración de si se ha aplicado el control o no y la justificación de su inclusión o exclusion.

En la presente actividad cooperativa con equipos de proyectos, realizaremos la revisión del ***Anexo A*** para asegurarse que ningún control necesario se pasó por alto. El ***Anexo A*** de la NCh-ISO 27001:2013 contiene una completa lista de objetivos de control y controles.

Se debe generar una declaración de aplicabilidad que contenga los controles necesarios para implementar (o que fueron implementados) en su proyecto formativo además de la justificación de inclusiones o exclusiones.

# Controles ISO 27001 Anexo A

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Objetivos de control | Nombre / descripción de control | Control | Justificación de aplicabilidad a su proyecto formativo | Tipo | Descripción requisito |
| A.5 Política de Seguridad | Política de Seguridad de la Información | Definir una política de seguridad de la información aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas relevantes. | Garantiza que todos los empleados entiendan y cumplan con las políticas de seguridad para proteger la información sensible del software. | Funcional | La política debe ser clara y accesible, detallando las responsabilidades y procedimientos de seguridad. |
| A.6 Organización de la seguridad de la información | Roles y Responsabilidades | Asignar responsabilidades de seguridad de la información dentro de la organización. | Permite definir quién es responsable de la seguridad de la información dentro del proyecto 'Imperial Inventory'. | Funcional | Cada rol debe tener claramente definidas sus responsabilidades de seguridad. |
| A.7 Seguridad en los recursos humanos | Proceso de Selección | Asegurar que los candidatos a empleo comprendan sus responsabilidades en seguridad de la información. | Previene que empleados sin formación en seguridad manejen información sensible del software. | No funcional | Realizar evaluaciones de seguridad durante el proceso de contratación. |
| A.8 Gestión de activos | Inventario de Activos | Identificar y gestionar los activos de la organización para asegurar una adecuada protección. | Gestionar correctamente los activos (datos, hardware) utilizados en el software 'Imperial Inventory'. | Funcional | Mantener un inventario actualizado de todos los activos relacionados con la información. |
| A.9 Control de acceso | Control de acceso a la red y a los sistemas de información | Implementar políticas para el control de acceso a la información y sistemas de la organización. | Protege el acceso no autorizado a la información sensible gestionada por el software. | Funcional | Establecer políticas de contraseñas y accesos basados en roles. |
| A.10 Criptografía | Uso de Controles Criptográficos | Proteger la confidencialidad, autenticidad e integridad de la información. | Asegura que la información almacenada y transmitida sea inaccesible a usuarios no autorizados. | Funcional | Implementar cifrado en almacenamiento y transmisión de datos. |
| A.11 Seguridad física y del entorno | Seguridad de áreas críticas | Prevenir el acceso no autorizado, daños e interferencias en las instalaciones de la organización. | Protege los equipos y datos físicos del proyecto 'Imperial Inventory'. | No funcional | Establecer controles de acceso físico y medidas de vigilancia. |
| A.12 Seguridad de las operaciones | Procedimientos de operación segura | Definir y seguir procedimientos operativos para gestionar las operaciones de manera segura. | Garantiza que las operaciones del software se realicen de forma segura y consistente. | Funcional | Documentar y seguir procedimientos para la gestión de la seguridad en las operaciones. |
| A.13 Seguridad en las comunicaciones | Gestión de Redes | Asegurar la protección de la información en las redes de comunicación. | Protege la transmisión de datos del software 'Imperial Inventory'. | Funcional | Implementar firewalls, IDS/IPS y cifrado en las comunicaciones. |
| A.14 Adquisición, desarrollo y mantenimiento de sistemas | Seguridad en el ciclo de vida del sistema | Integrar la seguridad de la información en el ciclo de vida de los sistemas de información. | Asegura que el desarrollo del software 'Imperial Inventory' considere la seguridad en todas sus fases. | Funcional | Realizar revisiones de seguridad en cada fase de desarrollo. |