LISTA DE CONTROL ISO 27001 (SEGURIDAD DE LA INFORMACIÓN)

1 CLAUSE 4 — Conozca su organización

Antes de empezar a diseñar sus controles de seguridad de la información, debe ser capaz de definir su organización. Una organización no se define sólo por lo que hace, sino también por lo que la conforma e influye en ella.

Habrá partes interesadas, leyes y reglamentos de seguridad de datos que tengan influencia en su organización. Podrían influir en su planificación.

- [ ] **Enumere los problemas internos y externos para la seguridad de la información.**
- [ ] **Enumere las partes interesadas y sus requisitos de seguridad de la información.**
- [ ] **Enumere la regulación pertinente en materia de seguridad de la información.**

2 CLAUSE 4 — Limite su sistema de gestión de la seguridad de la información a lo que realmente importa.

Conociendo su organización y con su misión u objetivos empresariales, puede establecer los límites de su Sistema de Gestión de la Seguridad de la Información (SGSI).

Puede que no necesite un SGSI para toda la organización; limite el alcance a las cosas que le importan a usted y a las partes interesadas.

- [ ] **Enumere las partes de la organización que deben estar en el alcance de certificación.**
- [ ] **Enumere las actividades internas, incluyendo cómo interactúan, a inlcuir en el alcance.**
- [ ] **Enumere las actividades que se llevan a cabo externamente (proveedores y subcontratas) que deben estar en el alcance.**

3 CLAUSE 5 — Asegúrese de que la gerencia está comprometida con la seguridad de la información y la mejora continua

Al igual que los altos cargos dirigen y dotan de recursos a la organización para que cumpla su objetivo, deben hacer lo mismo con la seguridad de la información.

Comience con una política que es una declaración de intenciones, que a su vez impulsa la necesidad, las actividades y los recursos.

- [ ] **Redacte una política de seguridad de la información. Esta es la política de alto nivel de la organización. Asegúrese de que cumple todos los requisitos de la norma.**
- [ ] **Difunda la política a todos los afectados (tanto internos como externos).**
- [ ] **Defina las funciones y responsabilidades en materia de seguridad de la información.**
- [ ] **Proporcionar recursos para la seguridad de la información y para el SGSI.**
- [ ] **Asegúrese de que alguien de la gerencia es responsable del SGSI y documente cuáles son sus responsabilidades. Se les entrevistará durante la auditoría.**

4 CLAUSE 6.1.1 Abordar los riesgos del SGSI y de la mejora continua

El SGSI es importante para la organización, por lo que debe enumerar los riesgos que podrían impedir que sea eficaz, y tener planes para mitigarlos. Tenga en cuenta los asuntos identificados durante la cláusula 4.

5 CLAUSE 6.1.2 Definir una evaluación de riesgos de seguridad de la información

La evaluación de los riesgos para la seguridad de la información es el núcleo de la norma (se trata de un proceso independiente de los riesgos identificados en el punto 6.1.1).

El proceso debe definirse para garantizar que produce resultados coherentes y repetibles.

Defina los criterios para aceptar los riesgos que identifique posteriormente. Esto supone su capacidad de riesgo.

Defina los criterios para saber cuándo debe realizar una evaluación de riesgos. Estos son eventos en Iso que deberá reevaluar sus riesgos de seguridad de la información.

El proceso debe asegurar que considera los riesgos de confidencialidad, integridad y disponibilidad de la información y que asigna un propietario a cada riesgo.

Los riesgos comprenden la probabilidad de que ocurra algo malo y el impacto cuando ocurre. Sus criterios para garantizar resultados repetibles y coherentes deben incluir criterios de impacto y probabilidad, y luego criterios para los niveles de riesgo.

El proceso debe garantizar que los criterios de aceptación del riesgo se utilicen para determinar el orden de tratamiento de los riesgos que considere inaceptables.

6 CLAUSE 6.1.3 Hacer algo con los riesgos que son inaceptables

El tratamiento de los riesgos de seguridad de la información consiste en reducir los riesgos a niveles aceptables mediante la definición de un plan de tratamiento de riesgos.

La norma ISO 27001 es inusual en el sentido de que enumera los controles de seguridad de la información de las mejores prácticas de la industria en el Anexo A. Estos constituirán la base del plan de tratamiento de riesgos.

Decida qué controles de seguridad son necesarios para tratar los riesgos y compárelos con los controles del Anexo A para asegurarse de que dispone de los necesarios.

Elabore una declaración de aplicabilidad (SoA), una lista de todos los controles del anexo A. Para cada control debe explicar por qué lo está implementando o no, y si está implementado. Puede añadir controles adicionales no incluídos en el Anexo A si son necesarios.

Elabore un plan de tratamiento de riesgos basado en los planes y los controles de seguridad del SoA. Debe obtener la aprobación de los propietarios el tratamiento de los mismos.

Vuelva a realizar la evaluación de riesgos, teniendo en cuenta el plan de tratamiento, para calcular el riesgo residual, y conseguir la aceptación de los nuevos niveles de riesgo.

7 CLAUSE 6.2 Disponga algunos objetivos

Una vez que disponga de una política de seguridad de la información y de los planes de tratamiento de riesgos, podrá establecer objetivos de seguridad de la información.

- **Planifique lo que necesita para lograrlo y quién es el responsable.**
- **Decida cómo va a controlar y medir los resultados de los objetivos.**
- **Comuníquelos a todos los que deban saberlo.**

8 CLAUSE 7 ¿Son sus recursos conscientes, competentes y suficientes?

El SGSI y sus operaciones de seguridad de la información no funcionarán sin los recursos adecuados.

- **Decida qué recursos se necesitan (personal, tecnología e infraestructura) para operar el SGSI. En el caso del personal, determine los conocimientos y habilidades necesarios y confirme que dispone de dichos conocimientos entre su personal.**
- **Tenga un plan de comunicación para asegurarse de que el personal y los terceros son conscientes de su papel en el apoyo al SGSI y a su política de seguridad de la información.**
- **Documente todo lo que exige la norma (hay una lista al final) y cualquier otra cosa que considere necesario. Controla los cambios en el documento y manténgalo seguro.**

Documentos obligatorios en la ISO 27001

CLÁUSULAS	
cláusula 4.3	Alcance del SGSI
cláusulas 5.2 y 6.2	Política y objetivos de seguridad de la info.
cláusula 6.1.2	Metodología de evaluación y tratamiento de riesgos
cláusula 6.1.3 d	Declaración de aplicabilidad (SoA)
cláusulas 6.1.3 e y 6.2	Plan de tratamiento de riesgos
cláusula 8.2	Informe de evaluación de riesgos

REGISTROS OBLIGATORIOS:	
cláusula 7.2	Alcance del SGSI
cláusula 9.1	Política y objetivos de seguridad de la info
cláusula 9.2	Metodología de evaluación y tratamiento de riesgos
cláusula 9.2	Declaración de aplicabilidad (SoA)
cláusula 9.3	Plan de tratamiento de riesgos
cláusula 10.1	Informe de evaluación de riesgos
cláusulas A.12.4.1 y A.12.4.3	Registros de actividades de usuarios, excepciones y eventos de seguridad

ANEXO A	
cláusulas A.7.1.2 y A.13.2.4	Definición de las funciones y responsabilidades de seguridad
cláusula A.8.1.1	Inventario de activos
cláusula A.8.1.3	Uso aceptable de los activos
cláusula A.9.1.1	Política de control de acceso
cláusula A.10.1.1	Política de uso de controles criptográficos
cláusula A.10.1.2	Política de gestión de claves
cláusula A.12.1.1	Proced. operativos para gestión informática
cláusula A.14.2.5	Principios de ingeniería de sistemas seguros
cláusula A.15.1.1	Política de seguridad de los proveedores
cláusula A.16.1.5	Procedimiento de gestión de incidentes
cláusula A.17.1.2	Procedimientos de continuidad de la actividad
cláusula A.18.1.1	Requisitos legales, reglamentarios y contractuales

9 CLAUSE 8 Planifique y controle la seguridad de su información

La seguridad de la información es un tema amplio y complicado, por lo que necesitará planificación y seguimiento, y habrá que gestionar los cambios.

Apliquelos planes de los objetivos de seguridad de la información	☐
Documente todo lo que considere necesario para garantizar el funcionamiento de los procesos de seguridad de la información	☐
Implemente la gestión de cambios en sus controles de seguridad de la información y realice revisiones cuando las cosas no vayan como previsto (no olvide los proveedores).	☐
Realice el proceso de evaluación de riesgos que definió en el punto 6.1.2	☐
Aplique el plan de tratamiento de riesgos que definió en el punto 6.1.3	☐

10 CLAUSE 9 Supervisar continuamente el rendimiento de la seguridad de la info.

Teniendo en cuenta todo lo definido en las cláusulas anteriores, aquí es donde se mide el rendimiento de su SGSI. Necesita saber qué debe medir, por quién, cómo y cuándo. La norma afirma lo siguiente: Necesita un programa de auditoría interna continua y revisiones por la dirección continuas. ☐

11 CLAUSE 10 Mejora continua

A veces las cosas van mal (no conformidades) por lo que hay que tener un proceso para:

Controlarlas	☐
Arreglarlas	☐
Descubrir la causa	☐
Tomar medidas para evitar que se repitan	☐