DELTA PROTECT®

La Biblia del ISO 27001

En este *e-book* encontrarás una amigable guía y beneficios de contar con la Certificación ISO 27001. Así como, un *checklist* que te guiará paso a paso en cómo certificar a tu empresa con los estándares internacionales de seguridad de la información.

Tabla de Contenidos

01. Introducción

Con la llegada y desarrollo de la tecnología se ha visto un aumento considerable en los riesgos de seguridad de la información para las empresas y organizaciones. Esto trae como consecuencia la pérdida de los servicios esenciales de red, decaimiento de la reputación y confianza de los clientes y graves problemas a nivel financiero.

En la búsqueda de soluciones a esta problemática surge la norma ISO 27001, durante todo el ***e-book*** te estaremos brindando información relevante sobre su implementación, beneficios y cómo obtener la certificación para la mejora de tu organización.

02. ¿Qué es ISO?

La ISO *(International Organization for Standardization)* es una organización internacional no gubernamental que cuenta actualmente con 167 países miembros y reúne expertos para compartir conocimientos y desarrollar normas internacionales que ayuden a adoptar las mejores prácticas para asegurar productos y servicios de calidad óptima, de forma homogénea en todo el mundo.

La organización tuvo sus inicios en el año 1946 en Londres y estuvo conformada por delegados de 25 países que fundaron los primeros comités técnicos con expertos enfocados en temas específicos y recursos necesarios en fabricación de productos y tecnologías que garanticen la satisfacción de los consumidores.

La ISO cuenta con una larga lista de normas publicadas, como la ISO 9001, ISO 22301 y una de las más reconocidas a nivel mundial, **la norma ISO 27001**: Sistemas de Gestión de la Seguridad de la Información (SGSI). La misma se basa en la política de seguridad de la información.

03. ¿Qué es la norma ISO 27001?

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO). Esta se basa en la teoría de gestión de calidad, o por sus siglas en inglés PDCA (Plan, Do, Check, Act. Planificar, Hacer, Verificar, Actuar en español) y **describe cómo gestionar la seguridad de la información en una empresa para la mejora continua de los sistemas de información** y garantizar la ciberseguridad de los activos de información. La filosofía que rige a esta norma es la investigación de los riesgos para la futura creación de un plan de tratamiento adecuado.

Es una norma que especifica los controles necesarios para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, o ISMS por sus siglas en inglés *(Information Security Management System)*, dentro del contexto de la organización. Los requisitos de la norma son de carácter genérico y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

Al igual que otros estándares de sistemas de gestión ISO, la certificación ISO/IEC 27001 es posible pero no obligatoria y puede ser implementada por cualquier tipo de organización, con o sin fines de lucro. Algunas organizaciones eligen implementar el estándar para beneficiarse de las mejores prácticas que contiene, mientras que otras deciden que también desean obtener la certificación para asegurar a los clientes que se han seguido sus recomendaciones, pues esto conlleva ciertos beneficios de los que se hablará más adelante.

Nota curiosa: *Debido a que 'Organización Internacional para la Estandarización' tendría diferentes acrónimos en diferentes idiomas (IOS en inglés, OIN en francés para Organización Internacional de Normalización), sus fundadores decidieron darle la forma abreviada ISO. ISO se deriva del griego 'isos', que significa igual. Sea cual sea el país, sea cual sea el idioma, siempre se podrá reconocer como ISO.*

¿Cómo funciona la norma 27001?

La ISO 27001 es una forma de seguridad de información. Entendiendo esto último como las medidas preventivas de resguardo de información de sistemas. Esto quiere decir que **busca mantener la confidencialidad y la integridad de los datos**, independientemente de su formato.

Esto lo hace mediante la investigación de posibles problemas, vulnerabilidades y riesgos que pueda presentar la organización. Para ello se utiliza la evaluación de riesgos y luego se define la mitigación o tratamiento de riesgos a través de políticas y procedimientos.

En muchos casos ya se cuenta con las herramientas técnicas como *software* y *hardware*, pero por desconocimiento no se saca el suficiente provecho. Es de allí que surgen los requisitos de la gestión de la seguridad de la información en las organizaciones propuestas por la ISO, donde el correcto cumplimiento de requisitos garantizará la obtención del certificado.

Es importante resaltar que ISO no realiza la certificación, sino que propone los controles adecuados para lograr obtenerla. Todo esto bajo reglas de estándar internacional y requisitos generales. Esta última información la ampliaremos más adelante.

04. Beneficios de la norma ISO 27001

Las buenas prácticas de gestión de seguridad de la información y cumplimiento de los controles establecidos por la ISO 27001 produce ventajas esenciales para una empresa. Los mismos los veremos a continuación:

Minimización de riesgos

Se disminuye la posibilidad de sufrir un incidente que comprometa la información de la organización. Esto mediante la evaluación de riesgos que permite conocer las vulnerabilidades y a partir de allí, tomar las acciones correctivas para dar paso a la continuidad del negocio.

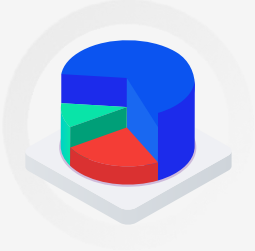
Algunos riesgos que se evitan o minimizan con la ISO 27001 son: obtención de datos privados del usuario o la organización, hackeo a sistemas y ataques financieros. Dicho de otra forma, promueve la ciberseguridad.

Aumento de confianza

El contar con esta certificación genera mayor confianza en clientes, proveedores y otras entidades. Además de proteger a la organización de ciberataques, al seguir los pasos de certificación, se demuestra que la misma es confiable, responsable y capaz.

Incremento de reputación

El cumplimiento de esta norma proyecta una imagen de profesionalidad que genera cada vez mayor y mejor reputación.



Reducción de costos

El cumplimiento de esta norma evita multas muy costosas de incumplimiento de leyes de protección de información personal y datos personales. De esta misma forma reduce la necesidad de realizar auditorías constantes, generando una única auditoría de certificación.

05. Estructura de la norma ISO 27001

La norma ISO 27001 se estructura de la siguiente manera:

06. Proceso de certificación

Si bien ISO no realiza la certificación, se apoya de organismos de certificación externos para cumplir con este propósito. A grandes rasgos se puede considerar el siguiente listado de pasos del proceso para obtener la certificación:

Listado de "To Do's" para lograr la Certificación de ISO 27001

1. Haz un equipo que tenga la misión de obtener la ISO 27001

- [ ] Establece roles y responsabilidades
- [ ] Si es necesario contrata a un tercero que ayude y oriente en el proceso de certificación

2. Construye tu Sistema de Gestión de Seguridad de la Información (SGSI)

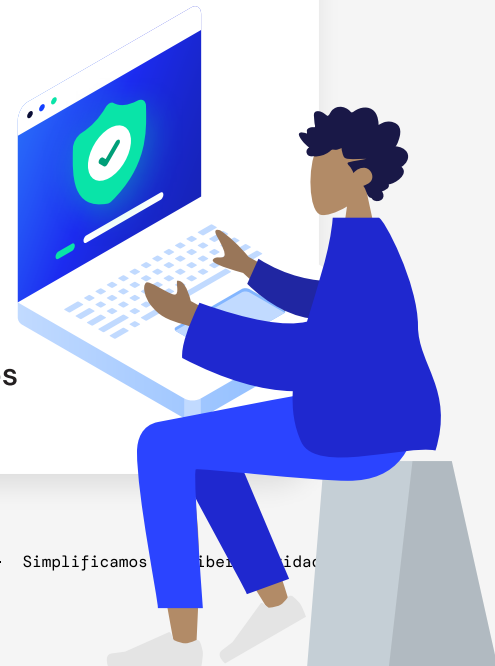
- [ ] Define el alcance de tu SGSI
- [ ] Informa a la Dirección y equipo de liderazgo de tu empresa sobre el alcance de SGSI

3. Crea y publica las políticas, documentos y reportes de SGSI

- [ ] Construye un marco para establecer, implementar, mantener y mejorar continuamente el SGSI
- [ ] Personaliza las plantillas de políticas con los procesos, políticas actuales y lenguaje de la organización
- [ ] Termina y publica las políticas

4. Realiza una evaluación de riesgos

- [ ] Establece un marco de gestión de riesgos
- [ ] Identifica riesgos potenciales
- [ ] Determina qué tan probable es que estos riesgos puedan ocurrir
- [ ] Evalúa el impacto potencial de los riesgos identificados



- [ ] Clasifica los riesgos en función del riesgo general para los objetivos de la organización
- [ ] Crea un plan de respuesta para cada riesgo

5. Completa un documento de Declaración de Aplicabilidad (DA)

- [ ] Revisa los 114 controles el Anexo A de la Norma ISO 27001
- [ ] Selecciona controles para abordar los riesgos identificados
- [ ] Completa la DA, enumerando todos los controles del Anexo A y justificando la inclusión o exclusión de cada control en la implementación el SGSI

6. Implementa políticas y controles del SGSI

- [ ] Crea un plan de comunicación para informar a los usuarios
- [ ] Comparte políticas y realiza un seguimiento de las revisiones de los empleados
- [ ] Realiza un seguimiento continuo de la eficacia del control

7. Capacita a los miembros del equipo en ISO 27001

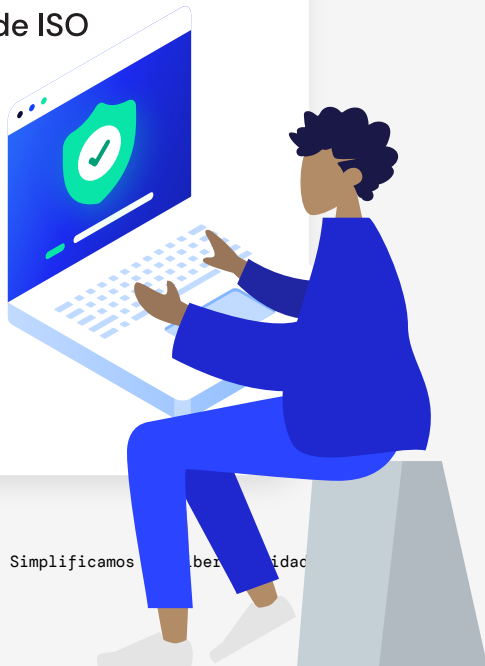
- [ ] Realiza capacitaciones periódicas para educar a los empleados sobre la norma ISO 27001 y el SGSI de la empresa
- [ ] Brinda capacitación sobre cómo responder a los riesgos más comunes que tu organización está enfrentando
- [ ] Educa a los empleados sobre las medidas disciplinarias que pueden tomar si no cumplen con los requisitos de seguridad de datos

8. Reúne documentación y pruebas

- [ ] Prepara la lista de documentos y registros requeridos de ISO 27001 para referencia durante la auditoría
- [ ] El equipo de Delta Protect te ayudará a tener todo en orden y listo

9. Haz una auditoría interna

- [ ] Identifica el alcance y la metodología de la auditoría interna (Cláusulas 4–10 y controles aplicables del Anexo A de ISO 27001)



- [ ] Elige un auditor independiente y objetivo para realizar la auditoría interna
- [ ] Produce y registra los resultados de la auditoría interna
- [ ] Remedia cualquier hallazgo de la auditoría interna

10. Somete a la empresa a la Etapa 1 de auditoría para la Certificación ISO 27001

- [ ] Selecciona un auditor ISO 27001 acreditado
- [ ] Lleva a acabo la Etapa 1 de auditoría, que consiste en una exhaustiva revisión de documentación
- [ ] Recibe retroalimentación sobre la preparación que se tiene hasta el momento para enfrentar la Etapa 2 de la auditoría

11. Implementa las correcciones de la Retroalimentación de la Etapa 1 de auditoría

- [ ] Asegúrate de que se cumplan todos los requisitos de la norma ISO 27001
- [ ] Asegúrate de que la organización siga los procesos que haz especificado y documentado
- [ ] Asegúrate de que la organización cumpla con los requisitos contractuales con terceros
- [ ] Aborda y registra las no conformidades específicas identificadas por el auditor de ISO 27001

12. Somete a la empresa a la Etapa 2 de Auditoría

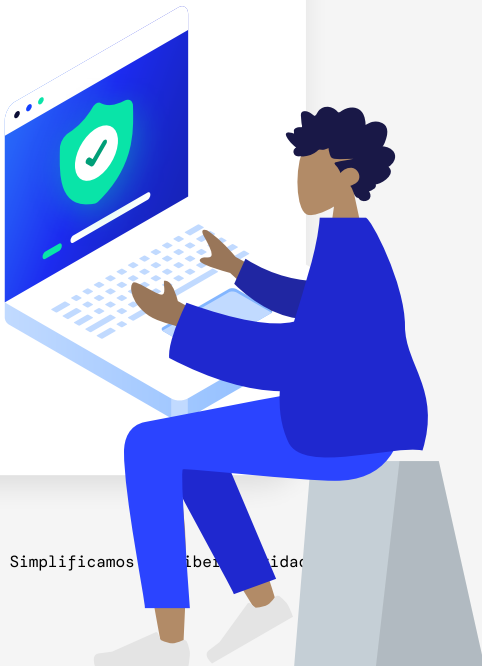
- [ ] Lleva a cabo la Etapa 2 de auditoría

13. Implementa las correcciones de la Retroalimentación de la Etapa 2 de Auditoría

- [ ] Aborda y registra las no conformidades específicas identificadas por el auditor de ISO 27001

14. Comprométete a realizar auditorías y evaluaciones posteriores

- [ ] Realizar revisiones de gestión anuales o trimestrales



- [ ] Prepárate para las auditorías de vigilancia del primer y segundo año
- [ ] Realiza evaluaciones de riesgo anuales
- [ ] Prepárate para la auditoría e renovación del tercer año
- [ ] Garantiza que el SGSI y tusobjetivos sigan siendo apropiados y efectivos
- [ ] Garantiza que la alta dirección se mantenga informada
- [ ] Asegúrate de que los ajustes para abordar los riesgos o las deficiencias se puedan implementar rápidamente

15. Realiza mejoras continuas

- [ ] Asegúrate de que las debilidades y amenazas al SGSI sean identificadas y remediadas
- [ ] Documenta y rastrea las no conformidades y las acciones correctivas hasta el cierre

07. Delta Protect y el cumplimiento de ISO 27001

Desde que inició la pandemia, los ciberataques se han incrementado un 400%, resultando en altas pérdidas económicas para varias empresas en múltiples industrias, pero las más afectadas hoy en día son las pymes y startups en Latam. Por ello, Delta Protect nace para simplificar y automatizar la ciberseguridad y el cumplimiento de startups y pymes en México y Latam, desde Micro-Empresas hasta Unicornios, automatizando certificaciones como ISO 27001, PCI DSS, SOC 2, HIPPA acompañado de Pentesting, Análisis de Vulnerabilidades y Ciberinteligencia.

Cada servicio se complementa para lograr certificaciones y/o robustecer la ciberseguridad de la organización. Para el caso específico de ISO 27001, nuestra plataforma Apolo ayudará a alcanzar la certificación en tiempo récord, con pocos recursos económicos y sin necesitar de grandes conocimientos en ISO 27001, nosotros nos encargamos.

APOLO

La plataforma que simplifica y automatiza
tu ciberseguridad y cumplimiento.

Beneficios

20x más rápido
detectar vulnerabilidades

10x más rápido en
lograr una certificación

10x más económico
que contratar un equipo
de seguridad

1 suscripción para tus
vulnerabilidades en vez de
utilizar **múltiples** herramientas

¿Por qué Apolo?

Protege a tus clientes
y usuarios

Construye **confianza** con tus
inversionistas y clientes

Ventaja
competitiva

Visibilidad en el proceso
de **certificación**

Evita incidentes
de seguridad

Ahorra tiempo
y dinero

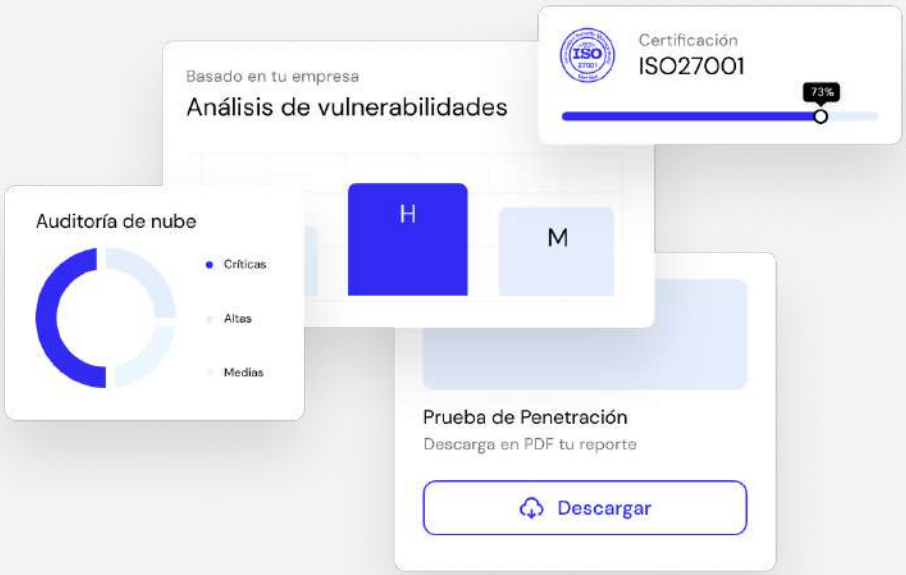
Lograr la certificación con Apolo simplifica el proceso de cumplimiento, ya que optimizamos la atención y cumplimiento de más de 150 puntos tanto documentales como de control que requieran la certificación.

Con Apolo podrás:

Crear e implementar **políticas** y **manuales** de ciberseguridad en tu empresa

Obtener **asesoramiento personalizado** en la **implementación** de controles y procedimientos

Visibilidad en el avance para el proceso de certificación en la norma ISO 27001



Quiero un demo de Apolo →

Conclusiones

Una vez más, reiteramos la importancia de la ciberseguridad y los requerimientos que hoy en día hacen posible esta oportunidad. Aunque no sea tarea sencilla, vale el esfuerzo por lograr las certificaciones necesarias, en este caso la certificación ISO 27001. Una herramienta clave para la continuidad de un negocio por todos los aportes positivos para la organización que la obtenga.

Si estás buscando certificar tu organización, en Delta Protect trabajamos con organismos certificadores y apoyamos a nuestros clientes en el cumplimiento de la norma para lograr la certificación. Contáctanos y logra la mejora continua de tu organización en materia de seguridad de información.

DELTA PROTECT®

Simplifica tu cumplimiento

¡Adelante! Agenda una demo con nuestro equipo

Agenda una demo con un especialista →

Delta Protect @delta.protect @DeltaProtect www.deltaprotect.com