CERTIFIED

CertiProf

Professional Knowledge

ISO 27001 FOUNDATION

ISO 27001 FOUNDATION

I27001F

I127001F Versión 112022

CertiProf®

Objetivos

- Alcance, propósito, términos y definiciones claves de la norma ISO/IEC 27001 y cómo puede ser utilizada
- Requisitos de definición del alcance y aplicabilidad

¿Quién es CertiProf®?

CertiProf® es un Instituto de Exámenes fundado en los Estados Unidos en 2015. Ubicada en Sunrise, Florida.
Nuestra filosofía se basa en la creación de conocimiento en comunidad y para ello su red colaborativa está formada por:

- **CLL's (CertiProf Lifelong Learners)** los candidatos a la certificación se identifican como Continuing Learners, lo que demuestra su compromiso inquebrantable con el continuo aprendizaje, el cual es de vital importancia en el mundo actual, digitalizado y en constante cambio. Independientemente de si aprueban o no el examen
- **ATP's (Accredited Trainer Partners)** universidades, centros de formación y facilitadores de todo el mundo conforman nuestra red de socios
- **Autores (co-creadores)** son expertos o practicantes de la industria que, con su conocimiento, desarrollan contenidos para la creación de nuevas certificaciones que respondan a las necesidades de la industria
- **Equipo Interno:** Nuestro equipo distribuido con operaciones en India, Brasil, Colombia y Estados Unidos está a cargo de superar obstáculos, encontrar soluciones y entregar resultados excepcionales

¿Quién debe atender este taller de certificación?

Cualquier persona que esté interesada en ampliar sus conocimientos en la Norma ISO/IEC 27001.

Nuestras Acreditaciones y Afiliaciones

Memberships

Digital badges issued by Accreditation

Agile Alliance

CertiProf® es un miembro corporativo de la Agile Alliance.

Al unirnos al programa corporativo Agile Alliance, continuamos empoderando a las personas ayudándolas a alcanzar su potencial a través de la educación. Cada día, brindamos más herramientas y recursos que permiten a nuestros socios capacitar a profesionales que buscan mejorar su desarrollo profesional y sus habilidades.

https://www.agilealliance.org/organizations/certiprof/

IT Certification Council - ITCC

CertiProf® es un miembro activo de la ITCC.

El propósito fundamental del ITCC es brindar apoyo a la industria y sus empresas miembros mediante la comercialización del valor de la certificación, la promoción de la seguridad de los exámenes, el fomento de la innovación y el establecimiento y el intercambio de las mejores prácticas de la industria.

Credly

CertiProf® es un socio de Credly.

Esta alianza permite que las personas y empresas certificadas o acreditadas con CertiProf® cuenten con una distinción a nivel mundial a través de un distintivo digital.

Credly es el repositorio de insignias más grande del mundo y empresas líderes en el área de tecnología como IBM, Microsoft, PMI, Scrum.org, Nokia, la Universidad de Stanford, entre otras, emiten sus insignias con Credly.

Insignia

https://www.credly.com/org/certiprof/badge/certified-iso-27001-foundation-i27001f

Lifelong Learning

Quienes obtienen esta insignia han demostrado su compromiso inquebrantable con el aprendizaje constante, el cual es de vital importancia en el mundo digital actual en constante cambio y expansión. También identifica las cualidades de una mente abierta, disciplinada y en constante evolución, capaz de utilizar y aportar sus conocimientos para desarrollar un mundo más igualitario y mejor.

Criterios de obtención:

- Ser un candidato a la certificación CertiProf®
- Ser un estudiante continuo y enfocado
- Identificarse con el concepto de Lifelong Learning
- Creer verdaderamente e identificarse con el concepto de que el conocimiento y la educación pueden y deben cambiar el mundo.
- Querer impulsar tu crecimiento profesional

CertiProf®
certiprof.com

COMPARTE Y VERIFICA

TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#I27001F #CertiProf

ISO 27001 FOUNDATION

I27001F

Agenda

I127001F Versión 112022

CertiProf®

Agenda

Fundamentos de la Norma ISO 27001

- Introducción a la Norma.
- Términos y definiciones.
- Entendimiento de numerales de la Norma.
- Identificación de requisitos.
- Qué son los objetivos de control.
- Conclusiones y preguntas de apoyo.

**La agenda es una recomendación general, cada entrenador puede desarrollar el material bajo su experiencia.*

AGENDA

ISO 27001 FOUNDATION

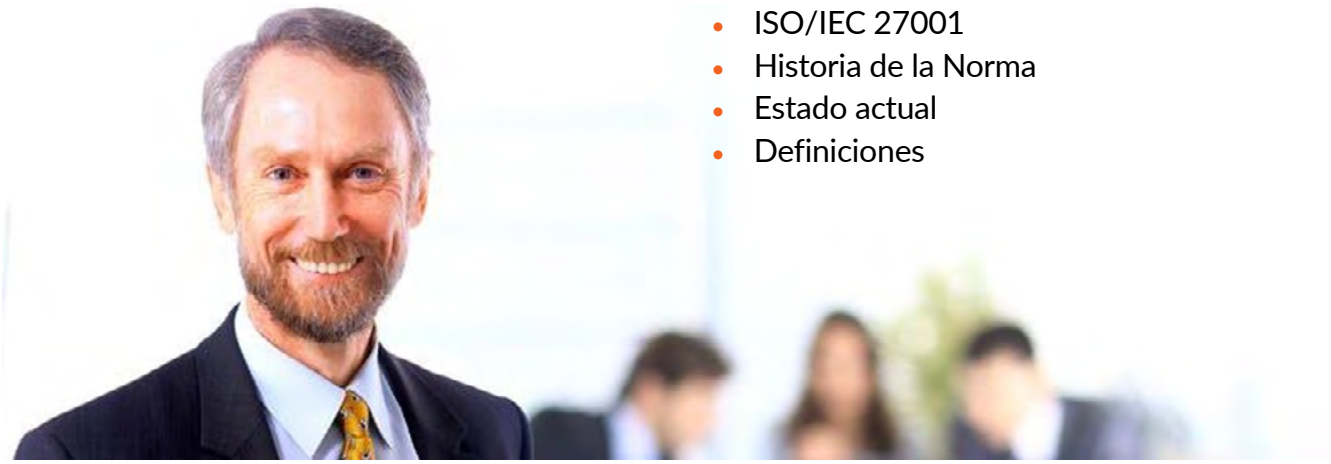
I27001F

1. Introducción y Antecedentes

I127001F Versión 112022

CertiProf®

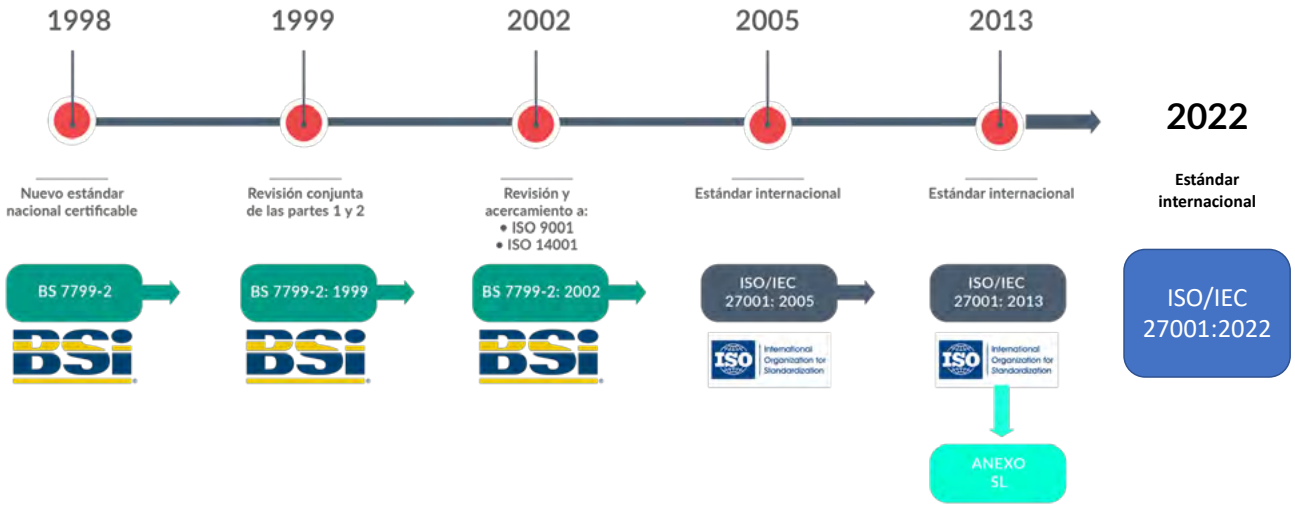
Introducción



- ISO/IEC 27001
- Historia de la Norma
- Estado actual
- Definiciones

- La Norma ha sido diseñada para "proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información".
- La Norma "puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización para cumplir con sus propios requisitos de seguridad de la información".
- La Norma también incluye "requisitos para la evaluación y el tratamiento de los riesgos en la seguridad de la información a la medida de las necesidades de la organización. Los requisitos establecidos en esta Norma Internacional son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza".

Historia de la Norma



ISO/IEC 27001:2022 Estructura

La nueva estructura refleja la estructura de otras normas nuevas de gestión, tales como ISO 9000, ISO 20000 e ISO 22301, que ayudan a las organizaciones a cumplir con varias normas.

Los cambios que se presentaron en la industria con la aparición del Marco de Ciberseguridad del NIST (CSF) cuyo enfoque era proteger la infraestructura crítica que soporta los servicios esenciales de los Estados Unidos, las propuestas de Ciberseguridad de la Unión Europea reflejados en diversos documentos de la ENISA y las actualizaciones que ocurrieron en otras mejores prácticas como ITIL y COBIT -durante 2019- y PCI, durante este año también han influido en la necesidad de refrescar el contenido de esta norma.

Hay 93 controles en 4 grupos en comparación con los 114 controles en 14 cláusulas en la versión de 2013.

Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos

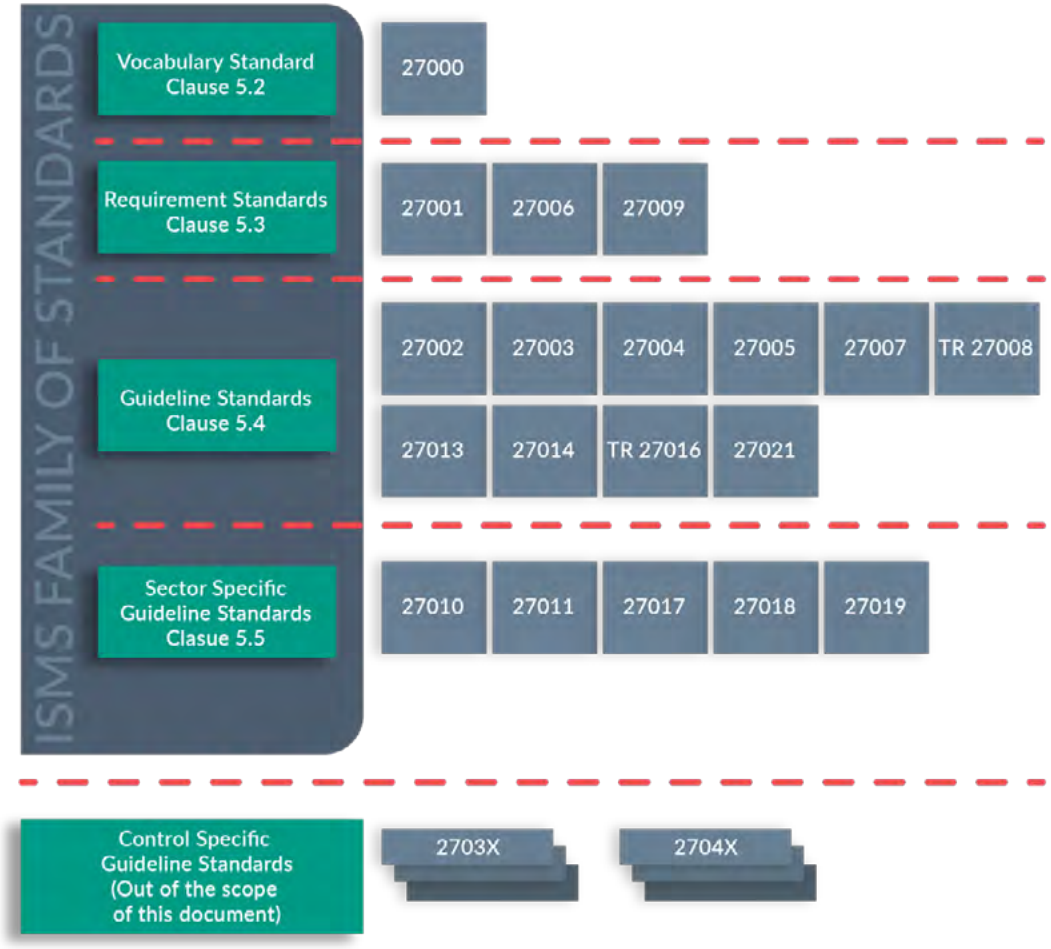
Se agregaron 11 nuevos controles (Inteligencia de amenazas, Seguridad de la información en la nube, continuidad del negocio, seguridad física y su supervisión, configuración, eliminación de la información, encriptación de datos, seguimiento y monitoreo, filtrado web, codificación segura)

1 control se eliminó (eliminación de activos)
58 controles se actualizaron
24 controles fusionados
4 grupos o tipos de controles: organizacional (37 controles), personas (8 controles), físico (14 controles), tecnológico (34 controles)

ISO 27000 Familia de Normas

La familia de normas de SGSI cuenta con normas para:

a) Definir los requisitos para un SGSI y para los organismos que certifiquen tales sistemas
b) Abordar la evaluación de la conformidad para el SGSI
c) Proporcionar apoyo directo, orientación detallada y/o interpretación para el proceso general a establecer, implementar, mantener y mejorar un SGSI
d) Abordar directrices sectoriales específicas para el SGSI



ISO 27001 FOUNDATION

I27001F

2. Conceptos Claves

I127001F Versión 112022

CertiProf®

ISO 27001 FOUNDATION

I27001F

¿Qué es un SGSI?

I127001F Versión 112022

CertiProf®

Información y Principios Generales

Un **SGSI** (*Sistema de Gestión de la Seguridad de la Información*) consiste en un conjunto de políticas, procedimientos, guías, recursos y actividades asociadas, que son gestionados de manera colectiva por una organización.

Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio.

Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos.

El análisis de los requisitos para la protección de los activos de la información y la aplicación de controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la exitosa implementación de un SGSI.

Los siguientes principios fundamentales también pueden contribuir a la implementación exitosa de un SGSI:

a) La conciencia de la necesidad de seguridad de la información.
b) La asignación de responsabilidades en seguridad de la información.
c) La incorporación del compromiso de la Dirección y los intereses de las partes interesadas.
d) La mejora de los valores sociales.
e) Apreciaciones de riesgo para determinar los controles adecuados para alcanzar niveles aceptables de riesgo.
f) La seguridad incorporada como un elemento esencial de los sistemas y redes de información.
g) La prevención y detección activas de incidentes de seguridad de la información.
h) El garantizar una aproximación exhaustiva a la gestión de la seguridad de la información.
i) La evaluación continua de la seguridad de la información y la realización de modificaciones cuando corresponda.

La Seguridad de la Información

La seguridad de la información incluye tres dimensiones principales: la confidencialidad, la disponibilidad y la integridad. Con el objetivo de garantizar el éxito empresarial sostenido, así como su continuidad y minimizar impactos, la seguridad de la información conlleva la aplicación y la gestión de medidas de seguridad adecuadas, que implican la consideración de una amplia gama de amenazas.

La seguridad de la información se consigue mediante la implementación de un conjunto de requisitos y controles aplicables, seleccionados a través del proceso de gestión de riesgo por medio de un SGSI, empleando políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados.

Estos controles necesitan ser especificados, implementados, monitorizados, revisados y mejorados cuando sea necesario, para garantizar que la seguridad y los objetivos de negocio y de seguridad específicos se cumplan. Estos controles de seguridad de la información deben integrarse de forma coherente con los procesos de negocio de una organización.

El Sistema de Gestión

Un sistema de gestión utiliza un marco de recursos para alcanzar los objetos de una organización.

El sistema de gestión incluye la estructura organizativa, las políticas, la planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

En términos de seguridad de la información, un sistema de gestión permite a una organización:

a) Satisfacer los requisitos de seguridad de los clientes y otras partes interesadas
b) Mejorar los planes y actividades de la organización
c) Cumplir con los objetivos de seguridad de información de la organización
d) Cumplir con las regulaciones, leyes y obligaciones sectoriales
e) Gestionar los activos de información de una manera organizada que facilita la mejora continua y la adaptación a las actuales metas de la organización y a su entorno

Factores Críticos de Éxito de una SGSI

Un gran número de factores son fundamentales para la implementación exitosa de un SGSI que permite a una organización cumplir con sus objetivos de negocio. Algunos ejemplos de factores críticos de éxito son:

a) Que la política, los objetivos y actividades de seguridad de la información estén alineadas con los objetivos del negocio
b) Un enfoque y un marco para el diseño, ejecución, seguimiento, mantenimiento y mejora de la seguridad de la información en consonancia de la cultura de la organización
c) El apoyo visible y el compromiso de todos los niveles de la Dirección, especialmente de alta Dirección
d) El conocimiento y entendimiento de los requisitos de protección de los activos de información obtenido mediante la aplicación de la gestión del riesgo de la seguridad de la información (véase la Norma ISO/IEC 27005)
e) Un programa efectivo de concienciación, formación y educación sobre seguridad de la información, informando a todos los empleados y otras partes interesadas de sus responsabilidades en seguridad de la información establecidas en las políticas de seguridad de la información, normas, etc
f) Un proceso eficaz de gestión de incidentes de seguridad de la información
g) Un enfoque efectivo de gestión de la continuidad del negocio
h) Un sistema de medición utilizado para evaluar el desempeño en la gestión de la seguridad de la información y para proporcionar sugerencias de mejora

Un **SGSI** aumenta la probabilidad de que una organización alcance de forma coherente los factores críticos de éxito para proteger sus activos de información.

Beneficios de la Familia de Normas SGSI

Los beneficios de implementar un SGSI producirán principalmente una reducción de los riesgos asociados a la seguridad de la información (es decir, reduciendo la probabilidad y/o el impacto causado por los incidentes de seguridad de la información). De una forma más específica los beneficios que para una organización produce la adopción exitosa de la familia de normas SGSI son:

a) Un apoyo al proceso de especificar, implementar, operar y mantener un SGSI, global, eficiente en costes, integrado y alineado que satisfaga las necesidades de la organización en diferentes operaciones y lugares.
b) Una ayuda para la dirección en la estructura de su enfoque hacia la gestión de la seguridad de la información, en el contexto de la gestión y gobierno del riesgo corporativo, incluidas las acciones de educación y formación en una gestión holística de la seguridad de la información a los propietarios del negocio y del sistema.
c) La promoción de buenas prácticas de seguridad de la información, aceptadas a nivel mundial, de una manera no preceptiva, dando a las organizaciones la flexibilidad para adoptar y mejorar los controles aplicables, respetando sus circunstancias específicas y para mantenerlos de cara a futuros cambios internos y externos.
d) Disponer de un lenguaje común y una base conceptual para la seguridad de la información, haciendo más fácil confiar a los socios de un negocio que esté en conforme a un SGSI, especialmente si requieren la certificación conforme a la Norma ISO/IEC 27001 por un organismo de certificación acreditado.
e) Aumentar la confianza en la organización por las partes interesadas.
f) Satisfacer necesidades y expectativas sociales.
g) Una más eficaz gestión desde un punto de vista económico de las inversiones en seguridad de la información.

ISO 27001 FOUNDATION

I27001F

3. Términos y Definiciones

(Ver anexo)

I127001F Versión 112022

CertiProf®

ISO 27001 FOUNDATION

I27001F

Estructura de la Norma

I127001F Versión 112022

CertiProf®

Estructura de ISO/IEC 27001

0.Introducción
1.Alcance
2.Referencias normativas
3.Términos y definiciones

4. Contexto de la organización
5.Liderazgo
6.Planificación
7.Soporte
8.Operación
9.Evaluación del desempeño
10.Mejora

Ciclo Deming PHVA Y SGSI

ISO 27001 FOUNDATION

I27001F

4. Contexto de la Organización

I127001F Versión 112022

CertiProf®

4.1 Comprensión de la Organización y de su Contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.

NOTA: La determinación de estas cuestiones se refiere al establecimiento del contexto externo e interno de la organización considerando el apartado 5.3 de la Norma ISO 31000.

- **Contexto Externo:** Es el entorno externo en el que la organización busca alcanzar sus objetivos
- **Contexto Interno:** Es el entorno interno, en el que la organización busca alcanzar sus objetivos

ISO 27001 FOUNDATION

I27001F

Taller 25 minutos

Determinar el Contexto de la Organización

haciendo uso de una matriz de análisis FODA

I127001F Versión 112022

CertiProf®

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas

La organización debe determinar:

a) Las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información
b) Los requisitos de estas partes interesadas que son relevantes para la seguridad de la información

NOTA: Los requisitos de las partes interesadas pueden incluir requisitos legales y regulatorios, así como obligaciones contractuales.

Parte Interesada es una persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.

Algunos ejemplos de partes interesadas:

ISO 27001 FOUNDATION

I27001F

¡Síguenos, contáctanos!

www.certiprof.com

CertiProf®