



# ISO 27001 FOUNDATION

## I27001F



I27001F Versión 112022

**CertiProf**<sup>®</sup>

## 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



### Certified ISO 27001 Foundation - I27001F

Issued by [CertiProf](#)

Holders of this certification have demonstrated an understanding of the Principles, concepts and the requirements of ISO/IEC 27001:2013, its understanding and how it can be used. They know the fundamental requirements for the implementation of an ISMS and the great importance of maintaining continuous process improvement.

Certification

Paid

#### Skills

Compliance

Continual Improvement

Customer Confidence

Data Protection

Frameworks

Information Management & Analysis

ISMS

ISO27001 Certification

Risk Management

<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



# COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#I27001F #CertiProf



# ISO 27001 FOUNDATION

## I27001F



# Agenda



I127001F Versión 112022

**CertiProf**<sup>®</sup>

## 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

<b>1. Introducción y Antecedentes</b>	<b>13</b>
Introducción	14
Historia de la Norma	14
ISO/IEC 27001:2022 Estructura	15
ISO 27000 Familia de Normas	15
<b>2. Conceptos Claves</b>	<b>17</b>
<b>¿Qué es un SGSI?</b>	<b>18</b>
Información y Principios Generales	19
La Seguridad de la Información	20
El Sistema de Gestión	20
Factores Críticos de Éxito de una SGSI	21
Beneficios de la Familia de Normas SGSI	22
<b>3. Términos y Definiciones</b>	<b>23</b>
<b>Estructura de la Norma</b>	<b>24</b>
Estructura de ISO/IEC 27001	25
Ciclo Deming PHVA Y SGSI	26
<b>4. Contexto de la Organización</b>	<b>27</b>
4.1 Comprensión de la Organización y de su Contexto	28
<b>Taller 25 minutos</b>	<b>33</b>
<b>5. Liderazgo</b>	<b>34</b>
5.1 Liderazgo y Compromiso	35
5.2 Política	36
5.3 Roles, Responsabilidades y Autoridades en la Organización	37
<b>6. Planificación</b>	<b>39</b>
6.1 Acciones para Tratar los Riesgos y Oportunidades	40
Plan de Tratamiento de Riesgos	45
6.1 Acciones para Tratar los Riesgos y Oportunidades	45
Estructura de la Norma ISO 31000 Gestión de Riesgos – Directrices	46
<b>Taller 25 Minutos</b>	<b>47</b>
6.2 Objetivos de Seguridad de la Información y Planificación para su Consecución	48
6.3 Planificación de Cambios	48
<b>Taller 25 Minutos</b>	<b>49</b>
<b>7. Soporte</b>	<b>50</b>
7.1 Recursos	51
7.2 Competencia	51
7.3 Concienciación	51
7.4 Comunicación	52
7.5 Información Documentada	52
<b>8. Operación</b>	<b>55</b>
8.1 Planificación y Control Operacional	56
8.2 Apreciación de los Riesgos de Seguridad de la Información	56

8.3 Tratamiento de los Riesgos de Seguridad de la Información	59
Evaluación y Tratamiento de Riesgos	59
<b>9. Evaluación del Desempeño</b>	<b>60</b>
9.1 Seguimiento, Medición, Análisis y Evaluación	61
9.2 Auditoría Interna	62
Auditoría	62
9.3 Revisión por la Dirección	63
<b>10. Mejora</b>	<b>65</b>
10.1 Mejora continua 10.2 No conformidad y acciones correctivas	66
10.2 No Conformidad y Acciones Correctivas	66
<b>Anexo 1: Términos y Definiciones</b>	<b>67</b>
<b>Taller 25 Minutos</b>	<b>68</b>
3.1 Control de Acceso	69
3.2 Modelo Analítico	69
3.3 Ataque	69
3.4 Atributo	69
3.5 Auditoría	69
3.6 Alcance de la Auditoría	69
3.7 Autenticación	70
3.8 Autenticidad	70
3.9 Disponibilidad	70
3.10 Medida Básica	70
3.11 Competencia	70
3.12 Confidencialidad	70
3.13 Conformidad	70
3.14 Consecuencia	71
3.15 Mejora Continua	71
3.16 Control	71
3.17 Objetivo de Control	71
3.18 Corrección	71
3.19 Acción Correctiva	72
3.20 Datos	72
3.21 Criterios de Decisión	72
3.22 Medida Derivada	72
3.23 Información Documentada	72
3.24 Eficacia	73
3.25 Evento	73
3.26 Dirección Ejecutiva	73
3.27 Contexto Externo	73
3.28 Gobernanza de la Seguridad de la Información	74
3.29 Órgano de Gobierno	74
3.30 Indicador	74

3.31 Necesidades de Información	74
3.32 Recursos (instalaciones) de Tratamiento de Información	74
3.33 Seguridad de la Información	74
3.34 Continuidad de la Seguridad de la Información	74
3.35 Evento o Suceso de Seguridad de la Información	75
3.36 Incidente de Seguridad de la Información	75
3.37 Gestión de Incidentes de Seguridad de la Información	75
3.38 Colectivo que Comparte Información	75
3.39 Sistema de Información	75
3.40 Integridad	75
3.41 Parte Interesada	75
3.42 Contexto Interno	76
3.43 Proyecto del SGSI	76
3.44 Nivel de Riesgo	76
3.45 Probabilidad (likelihood)	76
3.46 Sistema de Gestión	77
3.47 Medida	77
3.48 Medición	77
3.49 Función de Medición	78
3.50 Método de Medición	78
3.51 Resultados de las Mediciones	78
3.52 Supervisión, Seguimiento o Monitorización (monitoring)	78
3.53 No Conformidad	78
3.54 No Repudio	78
3.55 Objeto	79
3.56 Objetivo	79
3.57 Organización	79
3.58 Contratar Externamente (verbo)	79
3.59 Desempeño	80
3.60 Política	80
3.61 Proceso	80
3.62 Fiabilidad	80
3.63 Requisito	80
3.64 Riesgo Residual	80
3.65 Revisión	81
3.66 Objeto en Revisión	81
3.67 Objetivo de la Revisión	81
3.68 Riesgo	81
3.69 Aceptación del Riesgo	82

3.70	Análisis del Riesgo	82
3.71	Apreciación del Riesgo	82
3.72	Comunicación y Consulta del Riesgo	82
3.73	Criterios de Riesgo	83
3.74	Evaluación del Riesgo	83
3.75	Identificación del Riesgo	83
3.76	Gestión del Riesgo	84
3.77	Proceso de Gestión del Riesgo	84
3.78	Dueño del Riesgo	84
3.79	Tratamiento del Riesgo	84
3.80	Escala	85
3.81	Norma de Implementación de la Seguridad	85
3.82	Parte Interesada	85
3.83	Amenaza	86
3.84	Alta Dirección	86
3.85	Entidad de Confianza para la Comunicación de la Información	86
3.86	Unidad de Medida	86
3.87	Validación	86
3.88	Verificación	86
3.89	Vulnerabilidad	87
3.90	Información	87
3.91	Activo	87
<b>Conclusiones</b>		<b>88</b>
	Conclusiones	89

# ISO 27001 FOUNDATION

## I27001F



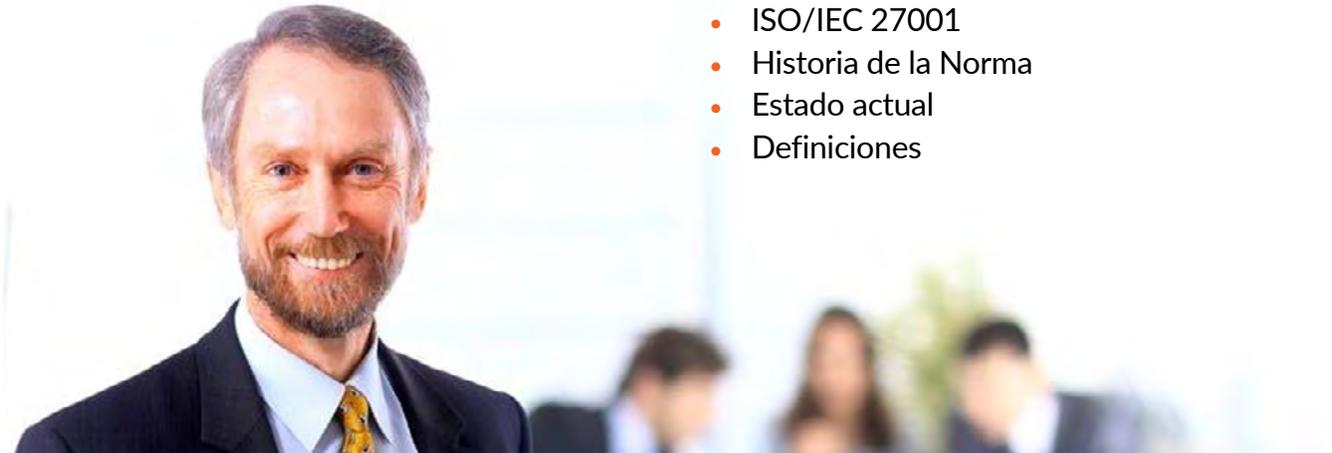
# 1. Introducción y Antecedentes



I127001F Versión 112022

**CertiProf**<sup>®</sup>

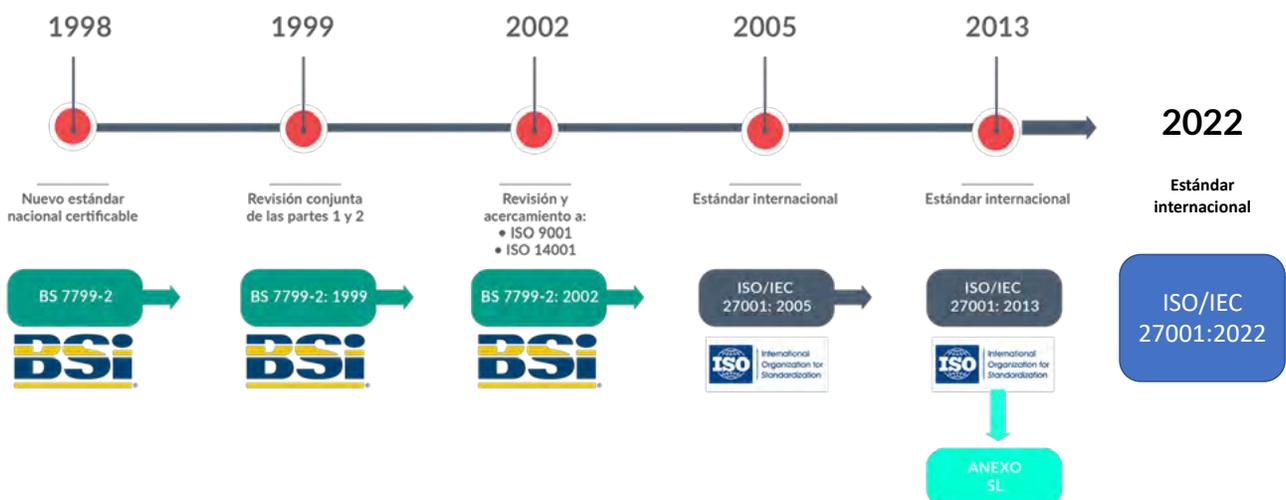
## Introducción



- 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

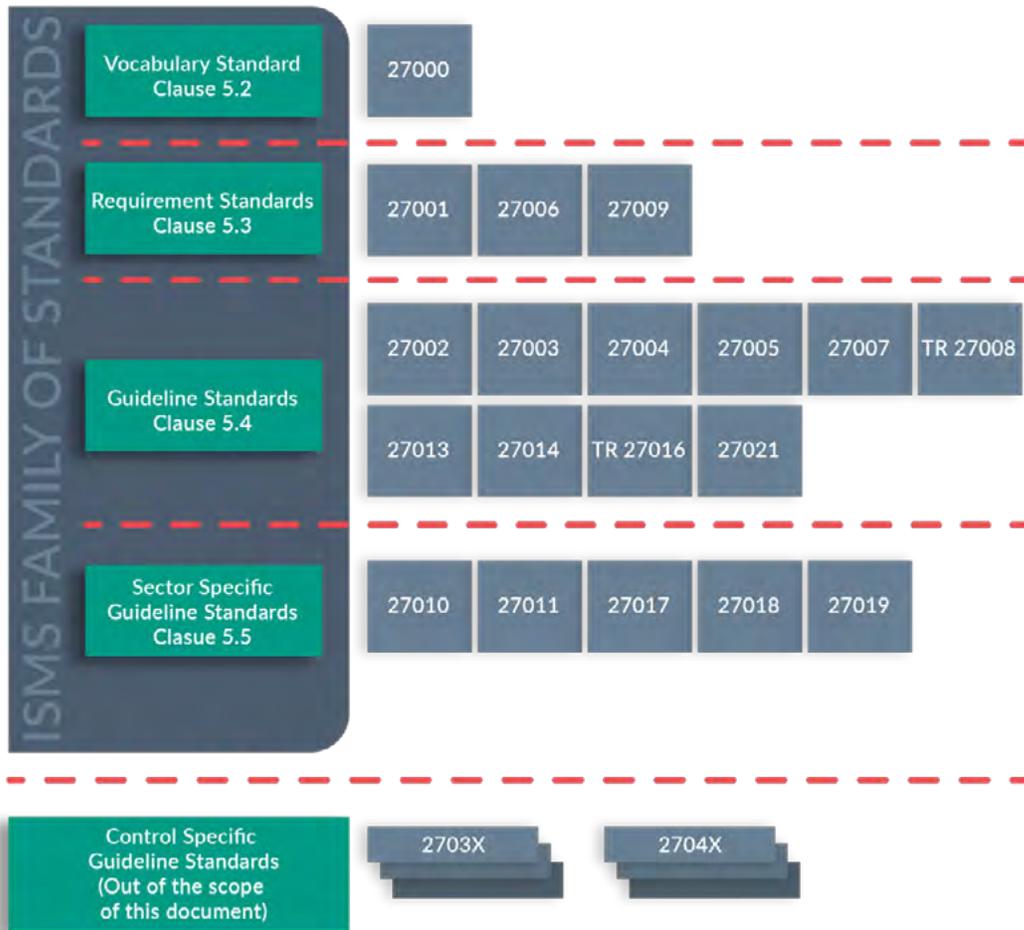
24 controles fusionados

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**<sup>®</sup>

# ISO 27001 FOUNDATION

## I27001F



# ¿Qué es un SGSI?



I127001F Versión 112022

**CertiProf**<sup>®</sup>

## 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.

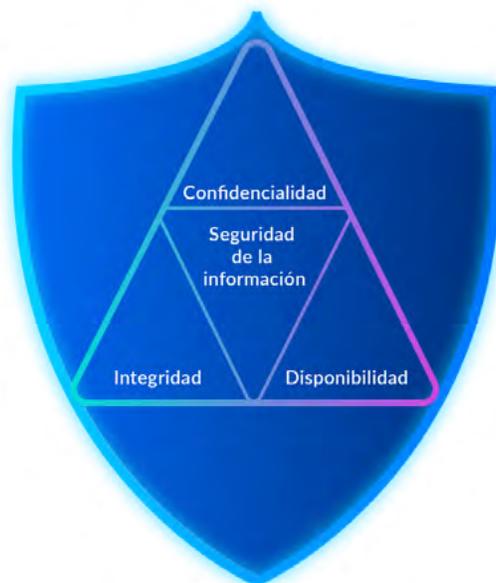
Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos.

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**<sup>®</sup>

# ISO 27001 FOUNDATION

## I27001F



# Estructura de la Norma



I127001F Versión 112022

**CertiProf**<sup>®</sup>

## 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**<sup>®</sup>

## 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**



I27001F 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](http://www.certiprof.com)

CERTIPROF® is a registered trademark of CertiProf, LLC in the United States and/or other countries.

**CertiProf®**