
SEGURIDAD
CERO
Curso Gratis
ISO 27001 De Cero a Lead Auditor

SEGURIDAD CERO

CURSO GRATIS

ISO 27001 DE CERO A LEAD AUDITOR

CLASE #1
FUNDAMENTOS
LUN 26 OCT

CLASE #2
IMPLEMENTADOR
MIE 28 OCT

CLASE #3
AUDITOR INTERNO
VIE 30 OCT

CLASE #4
AUDITOR LÍDER
LUN 02 NOV

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM
				

COL	ECU	PAN	PRY	DOM
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM
				

BOL	VEN	CHL	ARG	URY
8:00 PM	8:00 PM	9:00 PM	9:00 PM	9:00 PM
				

SEGURIDAD CERO

Fernando Conislla
Cybersecurity Expert

- Años de experiencia en servicios de ciberseguridad para entidades gubernamentales, bancarias, medios de pago, etc.
- Instructor SEGURIDAD CERO e instructor oficial ISO 27001
- Expositor en eventos internacionales
- Master en gestión y dirección de la ciberseguridad
- Certificaciones internacionales CEH, ISO 27001 LA, LCSPC.

SEGURIDAD CERO

Jaime Moya
ISO 27001 Lead Auditor

- Especialista en Seguridad de la Información, con más de 10 años de experiencia en ciberseguridad y seguridad de la información para clientes de los sectores energético, consumo masivo, telecomunicaciones, educativo, petróleo & gas.
- Instructor en SEGURIDAD CERO e instructor ISO 27001.
- Certificado internacionalmente ISO 27001 LA, CISM, LCSPC, etc

SEGURIDAD CERO

CLASE #1

ISO 27001 Fundamentos

LUNES 26 OCTUBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	9:00 PM

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM

SEGURIDAD CERO

¿Qué es ISO 27001?

¿Qué es ISO 27001?

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”.

SEGURIDAD CERO

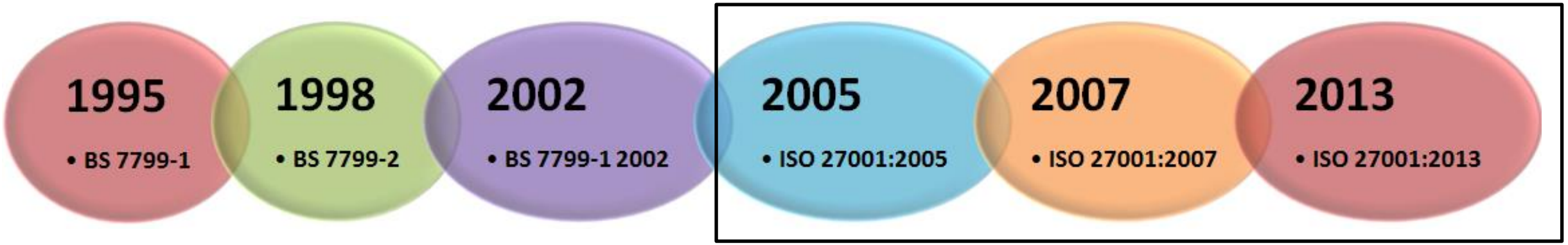
Historia de la Norma

ISO 27001

Historia de la Norma ISO 27001

- ✓ La norma BS 7799-1 de BSI apareció por primera vez en 1995“ y fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación.
- ✓ Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.
- ✓ Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO/IEC 17799 en el año 2000.

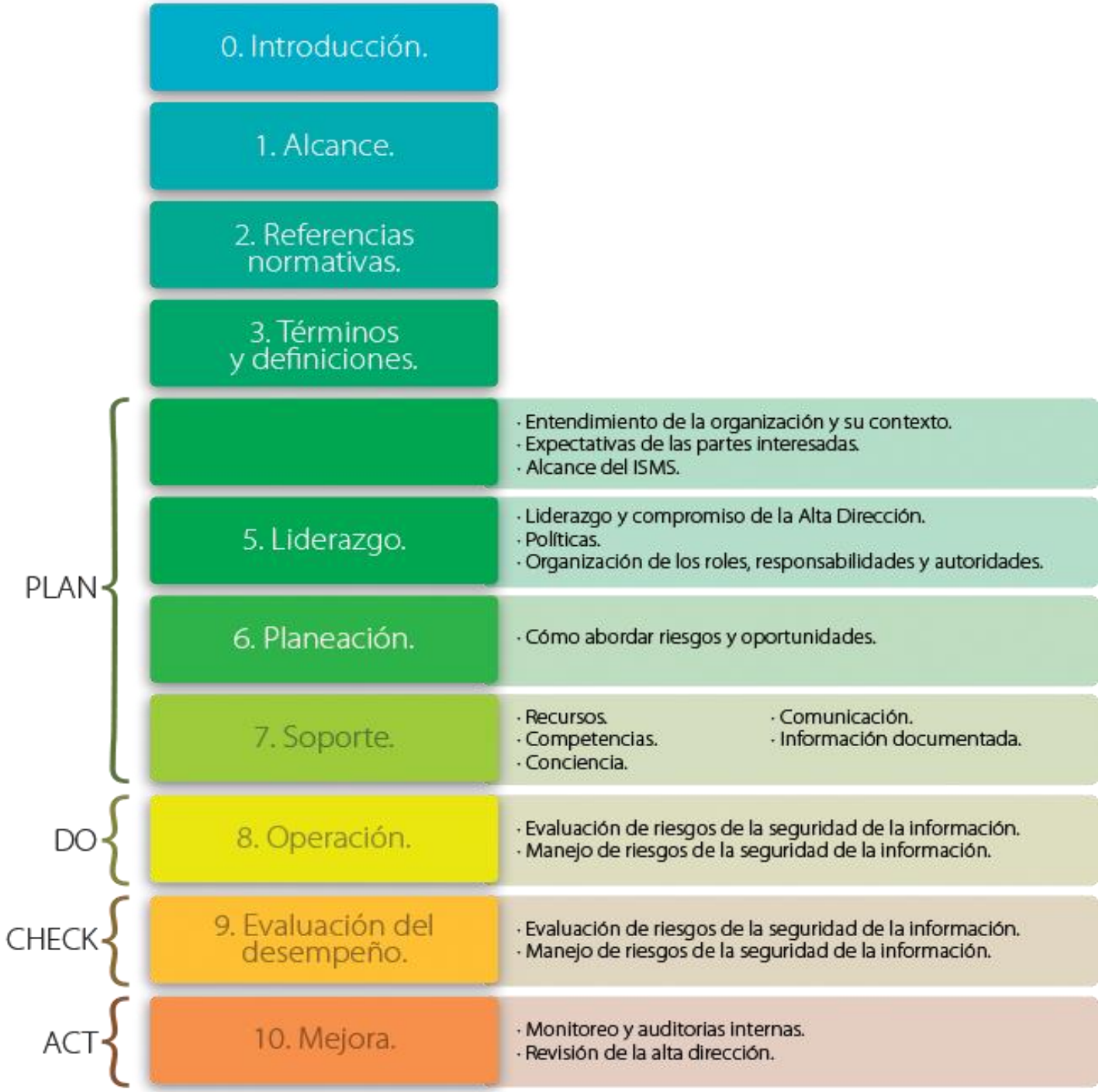
Historia de la Norma ISO 27001



- ✓ En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.
- ✓ En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar internacional ISO/IEC 27001. Al tiempo se revisó y actualizó ISO/IEC 17799. Esta última norma se renombró como ISO/IEC 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.
- ✓ Dentro de los periodos habituales de actualización de contenidos la última publicación que se ha realizado (segunda versión) de las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 ha sido en la misma fecha del 25 de Septiembre de 2013

SEGURIDAD CERO

Estructura ISO 27001


0. Introducción.
1. Alcance.
2. Referencias normativas.
3. Términos y definiciones.
PLAN
· Entendimiento de la organización y su contexto.
· Expectativas de las partes interesadas.
· Alcance del ISMS.
5. Liderazgo.
· Liderazgo y compromiso de la Alta Dirección.
· Políticas.
· Organización de los roles, responsabilidades y autoridades.
6. Planeación.
· Cómo abordar riesgos y oportunidades.
7. Soporte.
· Recursos.
· Competencias.
· Conciencia.
· Comunicación.
· Información documentada.
DO
8. Operación.
· Evaluación de riesgos de la seguridad de la información.
· Manejo de riesgos de la seguridad de la información.
CHECK
9. Evaluación del desempeño.
· Evaluación de riesgos de la seguridad de la información.
· Manejo de riesgos de la seguridad de la información.
ACT
10. Mejora.
· Monitoreo y auditorias internas.
· Revisión de la alta dirección.

Estructura ISO 27001

La nueva estructura refleja la estructura de otras normas nuevas de gestión, tales como ISO9000, ISO20000 e ISO22301,que ayudan a las organizaciones a cumplir con varias normas

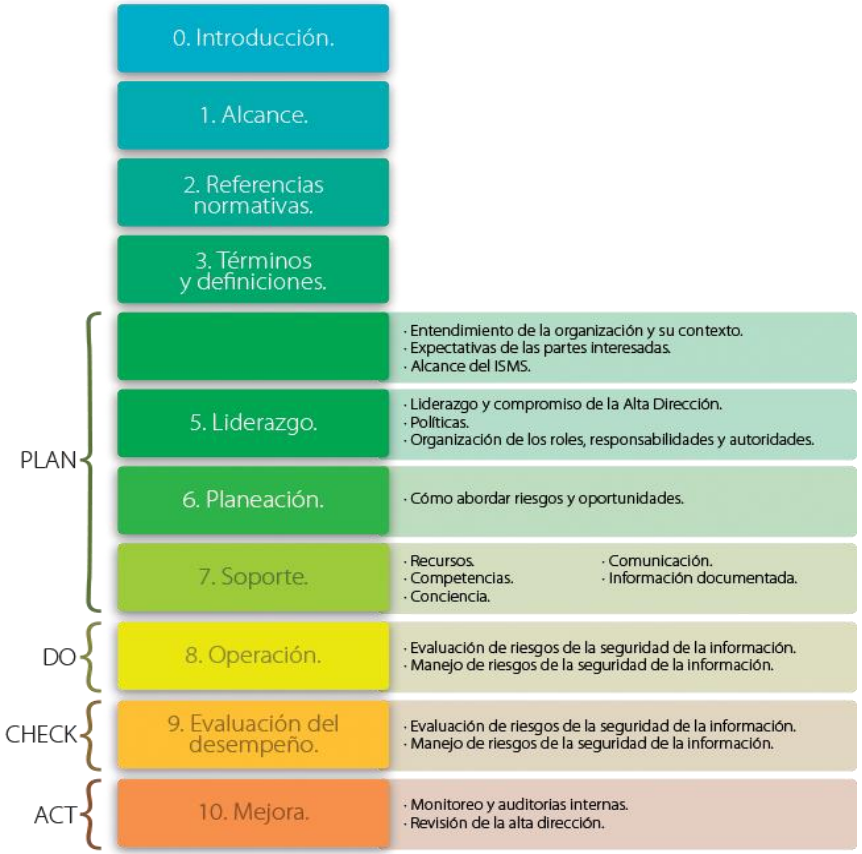
Los Anexos B y C del 27001:2005 han sido eliminados

Hay una sección adicional sobre la subcontratación

El ciclo PDCA de mejora continua ya no es central

La evaluación del riesgo más importante del contexto organizacional cambió

Hay 114 controles en 14 grupos en comparación con los 133 controles en 11 grupos en la versión de 2005.



SEGURIDAD CERO

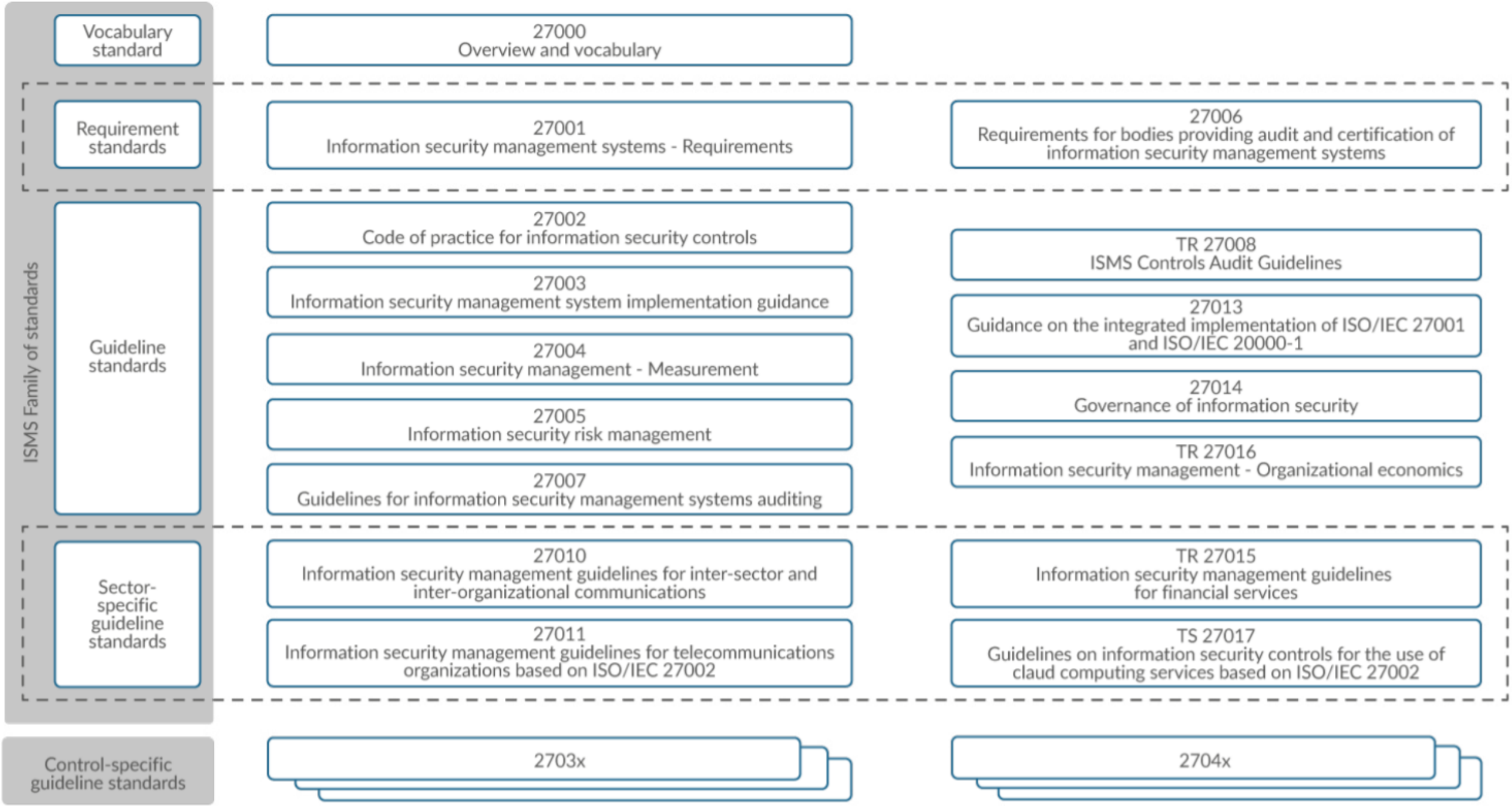
Controles ISO 27001

Controles ISO 27001

01. Políticas de seguridad de la información
02. Organización de la seguridad de información
03. Seguridad de los recursos humanos
04. Gestión de Activos
05. Controles de accesos
06. Criptografía
07. Seguridad física y ambiental
08. Seguridad de la operaciones
09. Seguridad de las comunicaciones
10. Adquisición y mantenimiento de sistemas
11. Relación con los proveedores
12. Gestión de los incidentes de seguridad
13. Gestión de la continuidad de negocios
14. Cumplimiento

SEGURIDAD CERO

Familia de Normas ISO 27000


ISMS Family of standards
Vocabulary standard
27000
Overview and vocabulary
Requirement standards
27001
Information security management systems - Requirements
27006
Requirements for bodies providing audit and certification of information security management systems
Guideline standards
27002
Code of practice for information security controls
27003
Information security management system implementation guidance
27004
Information security management - Measurement
27005
Information security risk management
27007
Guidelines for information security management systems auditing
TR 27008
ISMS Controls Audit Guidelines
27013
Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
27014
Governance of information security
TR 27016
Information security management - Organizational economics
Sector-specific guideline standards
27010
Information security management guidelines for inter-sector and inter-organizational communications
27011
Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
TR 27015
Information security management guidelines for financial services
TS 27017
Guidelines on information security controls for the use of claud computing services based on ISO/IEC 27002
Control-specific guideline standards
2703x
2704x

SEGURIDAD CERO

¿Qué es un SGSI?

¿Qué es un SGSI?

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

Un **SGSI** es un enfoque sistemático para establecer, implementar, operar, monitorizar, 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**

SEGURIDAD CERO

Propiedades de la Seguridad de la Información


CONFIDENCIALIDAD
INTEGRIDAD
INFORMACIÓN
DISPONIBILIDAD

Propiedades de la Seguridad de la Información

Confidencialidad:
Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados – ISO 27000

Disponibilidad:
Propiedad de ser accesible y estar listo para su uso o demanda de una entidad autorizada – ISO 27000

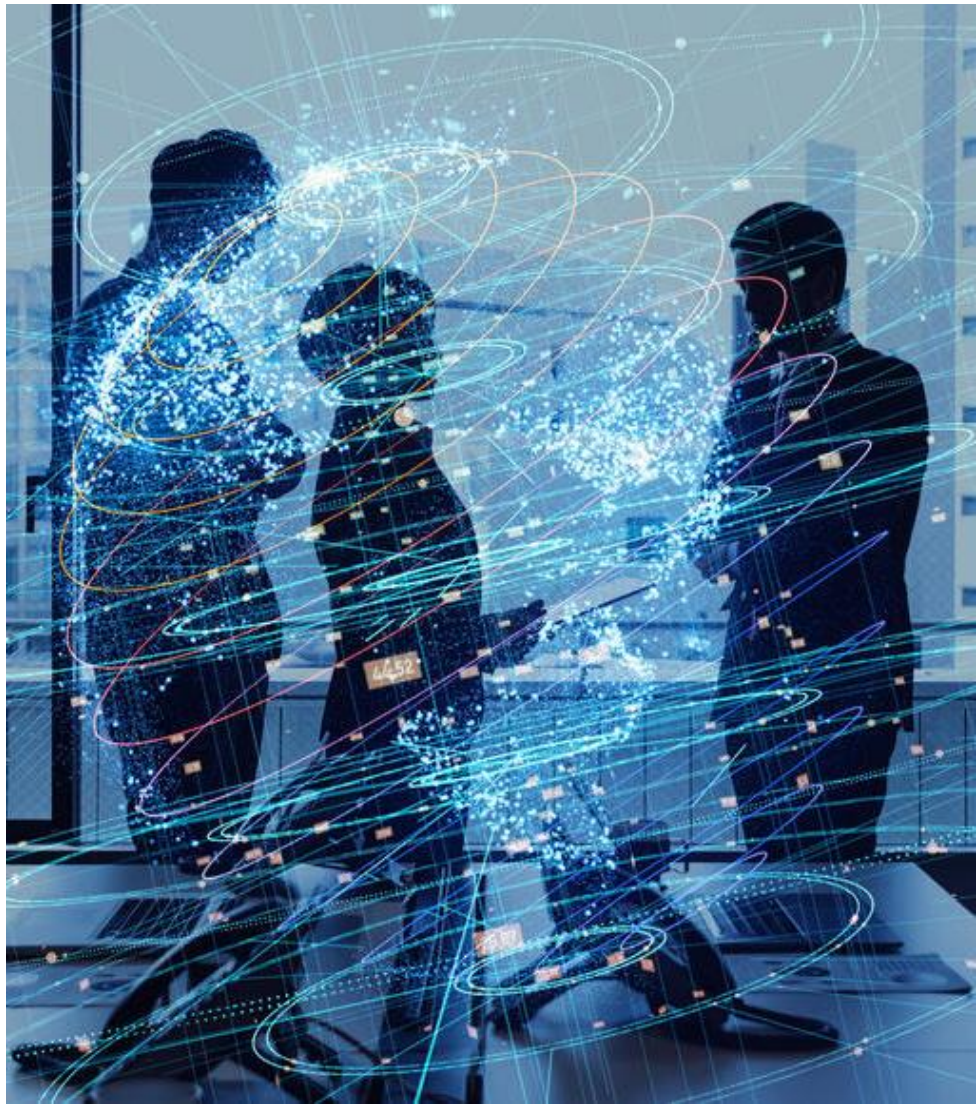
Integridad:
Propiedad de exactitud y completitud – ISO 27000

SEGURIDAD CERO

Principios para una exitosa implantación de un SGSI

Principios que contribuyen a una exitosa implantación de un SGSI

- ✓ Es una decisión estratégica que debe involucrar a toda la organización y que debe ser apoyada y dirigida desde la alta dirección
- ✓ Su diseño dependerá de los objetivos y necesidades de la organización, así como de su estructura organizacional



Principios que contribuyen a una exitosa implantación de un SGSI

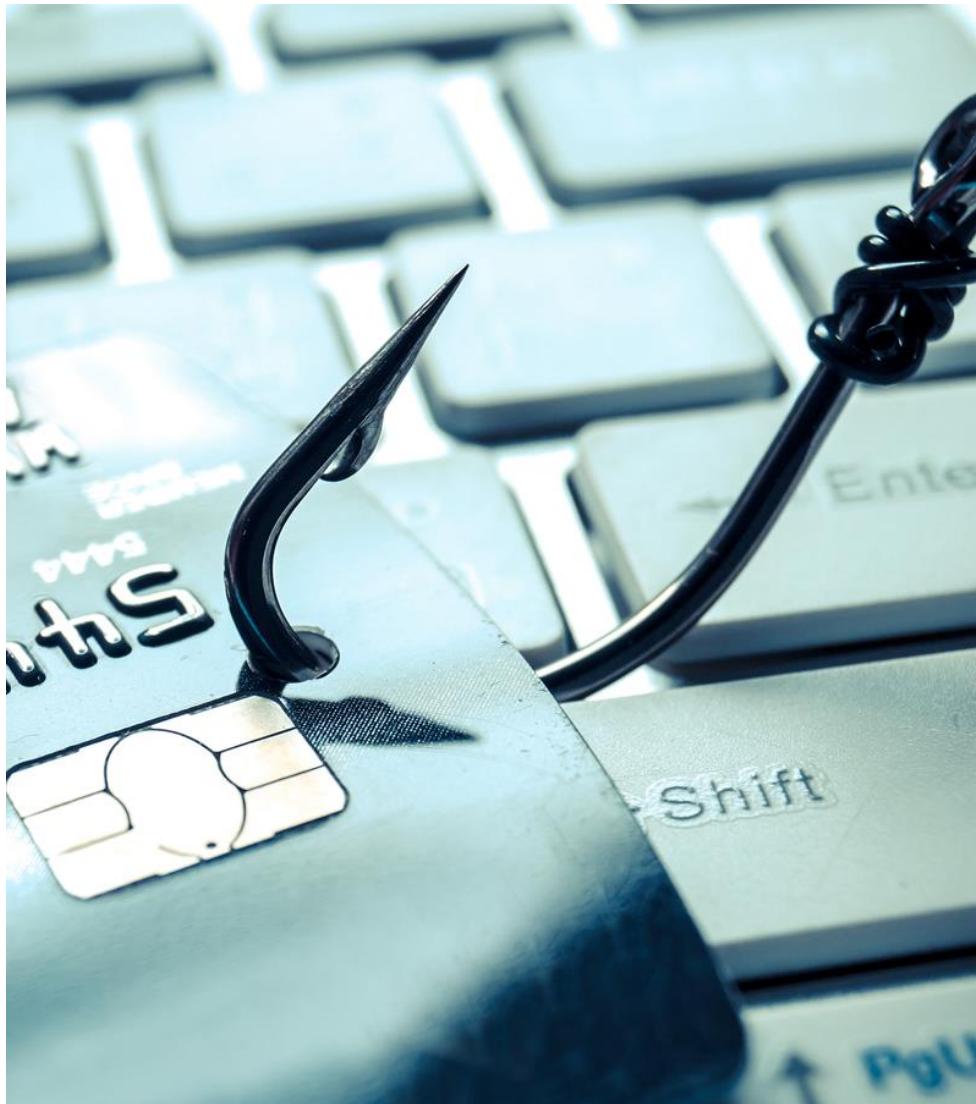
- ✓ Para hacer más sencillo el proceso de implementación, es bueno contar con la ayuda de una empresa especializada o un profesional especializado que asesore durante todo el proceso
- ✓ El tiempo de implementación del sistema de gestión de seguridad de la información varía en función del tamaño de la empresa, el estado inicial de la seguridad de la información y los recursos destinados a ello

Principios que contribuyen a una exitosa implantación de un SGSI

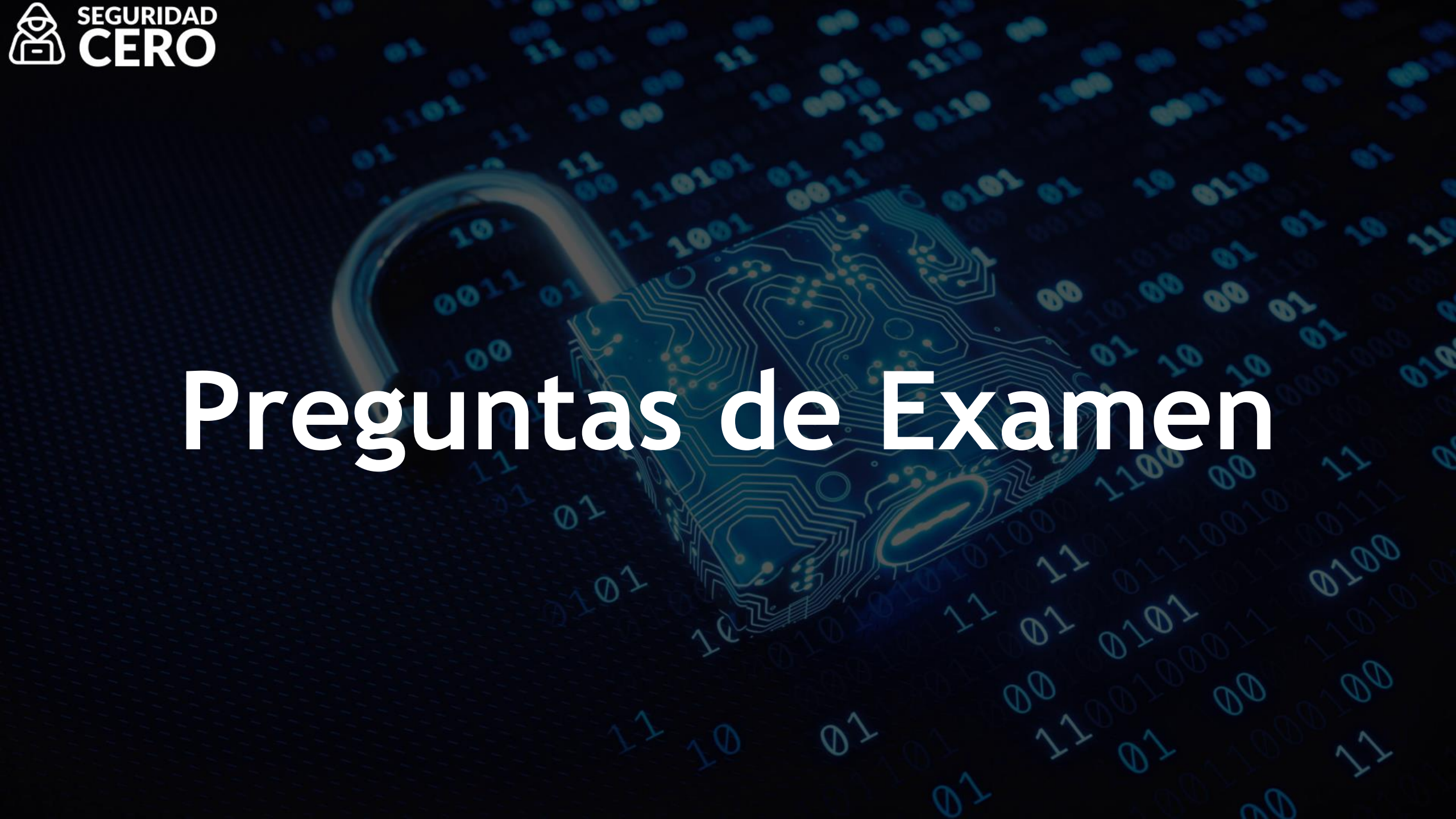
- ✓ La organización debe contar con una estructura organizacional así como de recursos necesarios, entre otras cosas, para llevar a cabo la implementación del SGSI
- ✓ Realizar un Análisis de Riesgos que valore los activos de información y vulnerabilidades a las que están expuestas. Así mismo, es necesario una Gestión de dichos riesgos para reducirlos en la medida de lo posible.

Principios que contribuyen a una exitosa implantación de un SGSI

- ✓ Concienciación y formación al personal de la organización para dar a conocer qué se está haciendo y por qué
- ✓ La asignación de responsabilidades en seguridad de la información



SEGURIDAD CERO



Preguntas de Examen

Pregunta #1

El anexo A de la ISO/IEC 27001:2013 consta de:

a) 05 funciones, 23 categorías y 108 subcategorías

b) 14 clausulas de control, 35 objetivos de control y 114 controles

c) 11 clausulas de control, 35 objetivos de control y 133 controles

d) Ninguna de las anteriores

Pregunta #1

El anexo A de la ISO/IEC 27001:2013 consta de:

a) 05 funciones, 23 categorías y 108 subcategorías

b) 14 clausulas de control, 35 objetivos de control y 114 controles

c) 11 clausulas de control, 35 objetivos de control y 133 controles

d) Ninguna de las anteriores

Pregunta #2

¿Cual es la finalidad de la ISO/IEC 27002?

a) Contiene requisitos obligatorios para el SGSI

b) Proporciona requisitos obligatorios para la gestión de riesgos

c) Proporciona orientación en los controles de seguridad de la información

d) Proporciona capacidades para la medición del SGSI

Pregunta #2

¿Cual es la finalidad de la ISO/IEC 27002?

a) Contiene requisitos obligatorios para el SGSI

b) Proporciona requisitos obligatorios para la gestión de riesgos

c) Proporciona orientación en los controles de seguridad de la información

d) Proporciona capacidades para la medición del SGSI

Pregunta #3

¿Cómo la alta dirección debe proporcionar evidencia de su compromiso con el SGSI?

a) Comprando tecnología de primera

b) Definiendo el enfoque de gestión de riesgos

c) Comunicando la importancia de cumplir los requisitos

d) Realizando una auditoria interna anual del sistema de gestión de seguridad de la información

Pregunta #3

¿Cómo la alta dirección debe proporcionar evidencia de su compromiso con el SGSI?

a) Comprando tecnología de primera

b) Definiendo el enfoque de gestión de riesgos

c) Comunicando la importancia de cumplir los norma a la organización

d) Realizando una auditoria interna anual del sistema de gestión de seguridad de la información

SEGURIDAD CERO

CLASE #1

ISO 27001 Fundamentos

LUNES 26 OCTUBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	9:00 PM

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM