
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

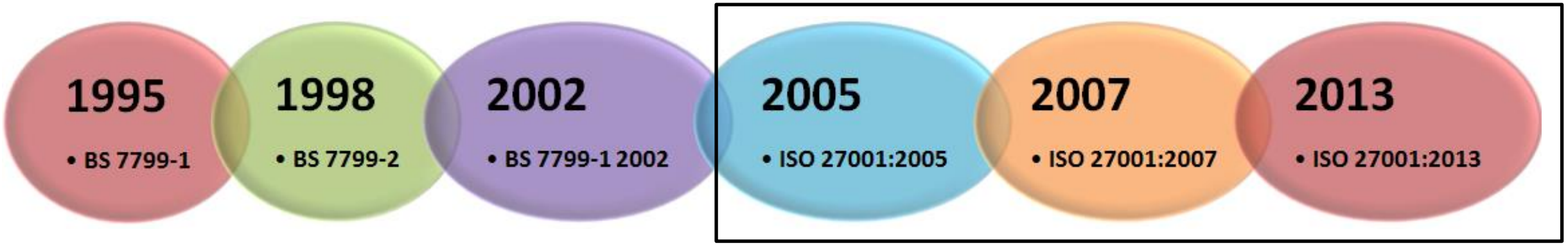
Historia de la Norma

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.

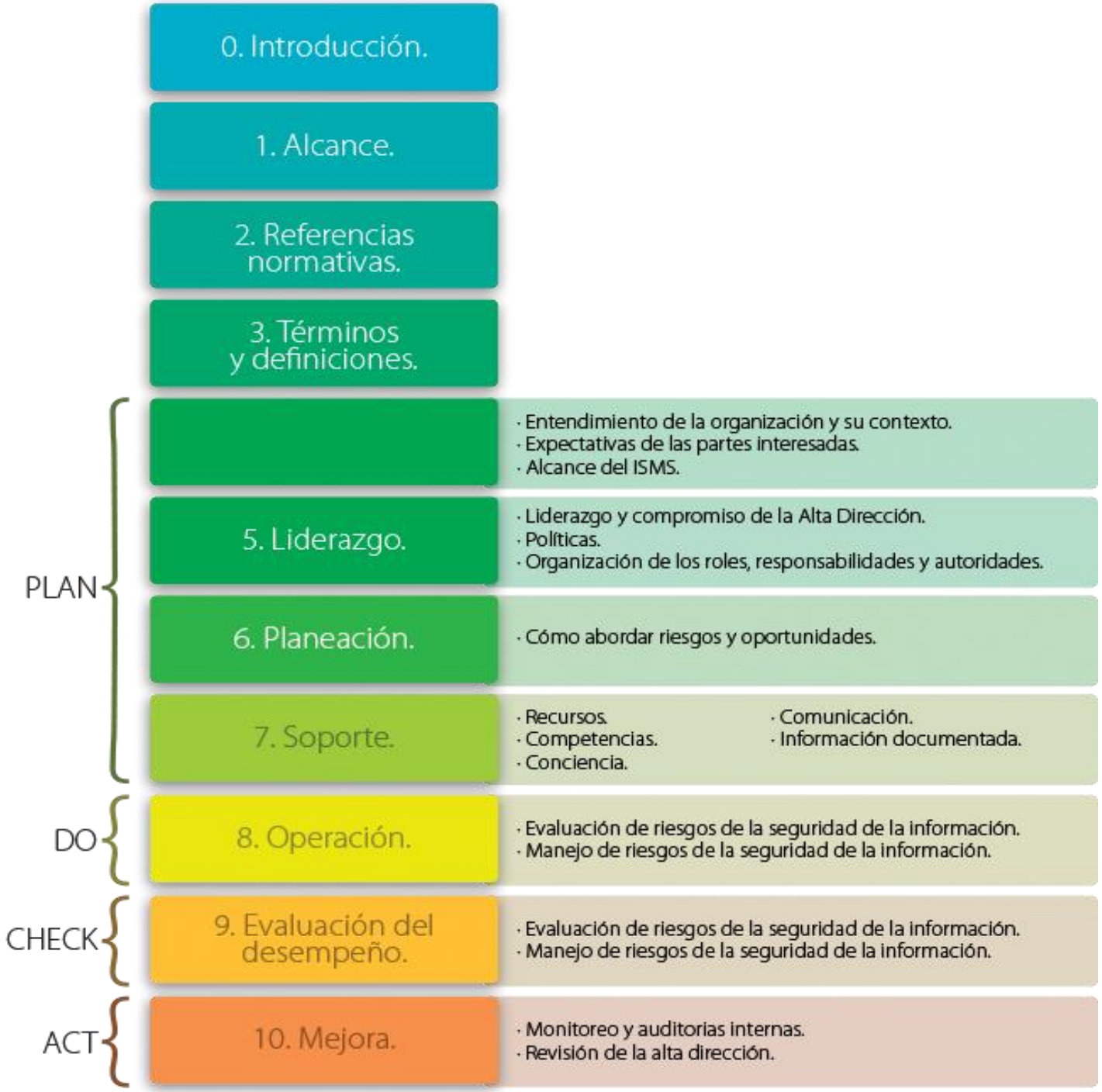
Historia de la Norma ISO 27001



- ✓ 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

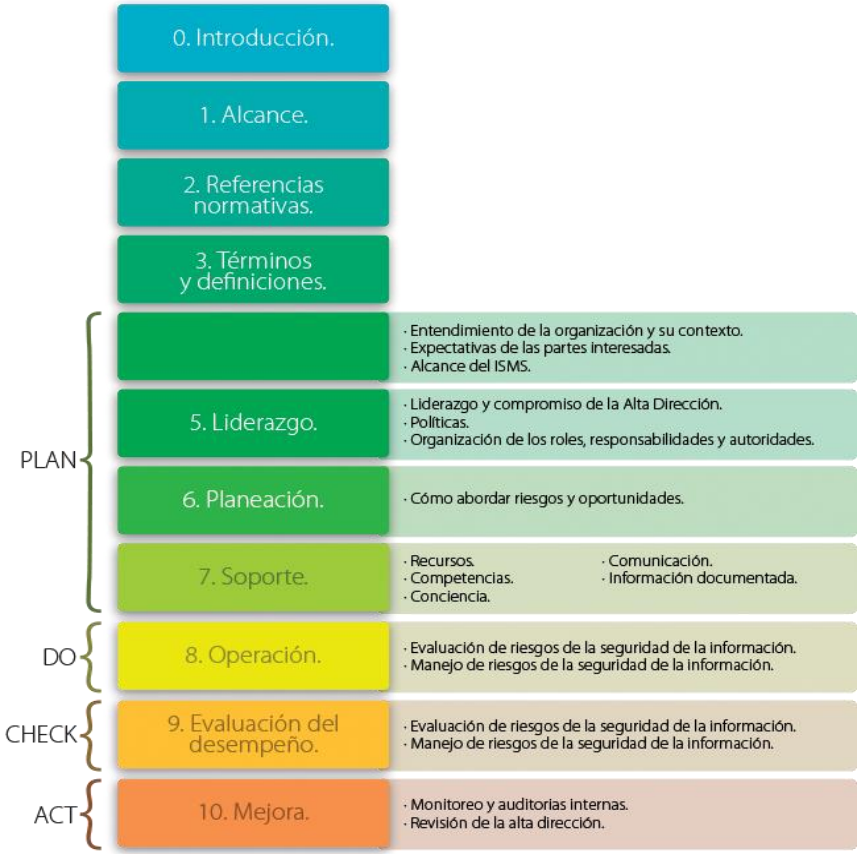
Los Anexos B y C del 27001:2005 han sido eliminados

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

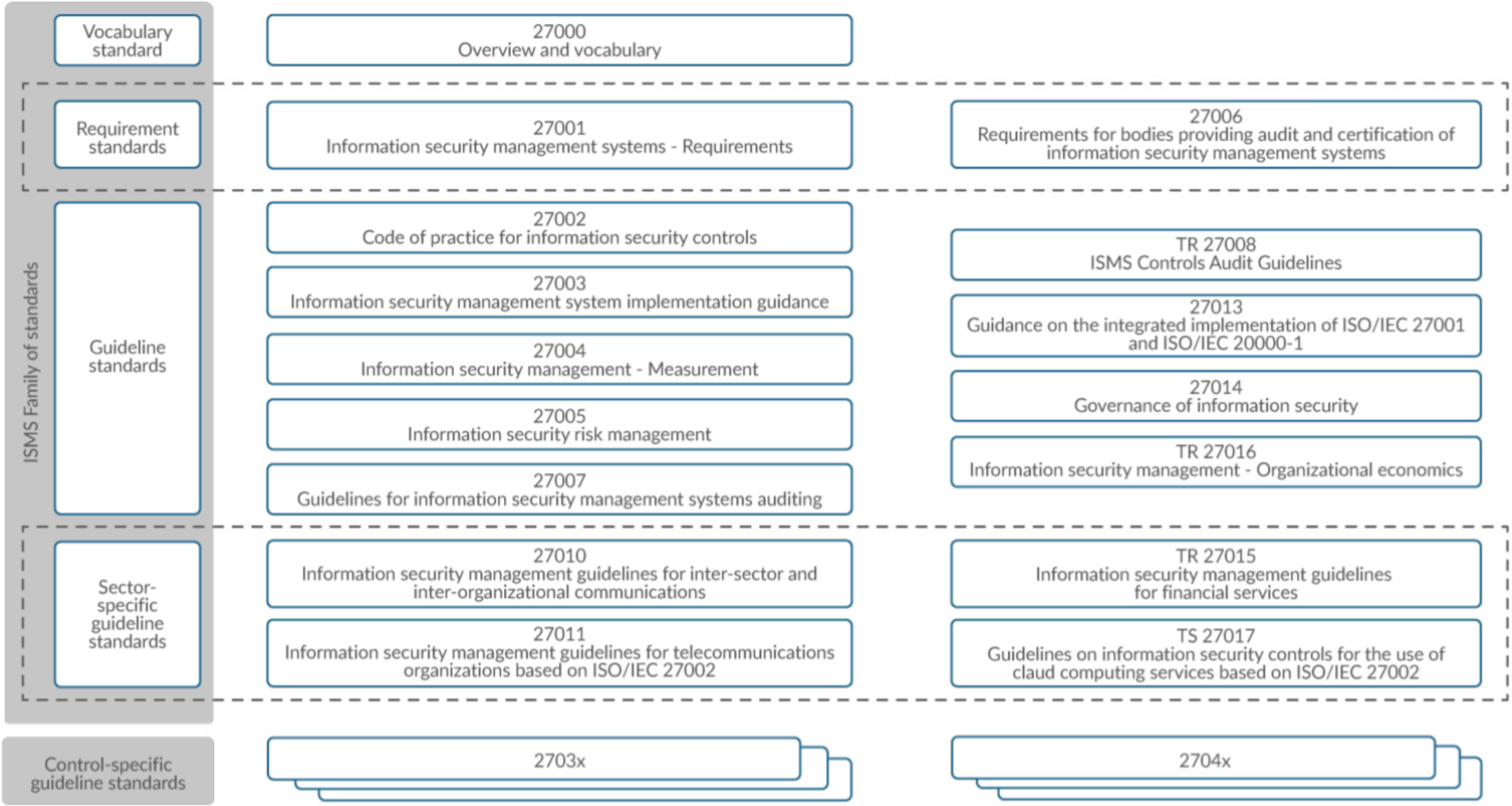
Controles ISO 27001

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

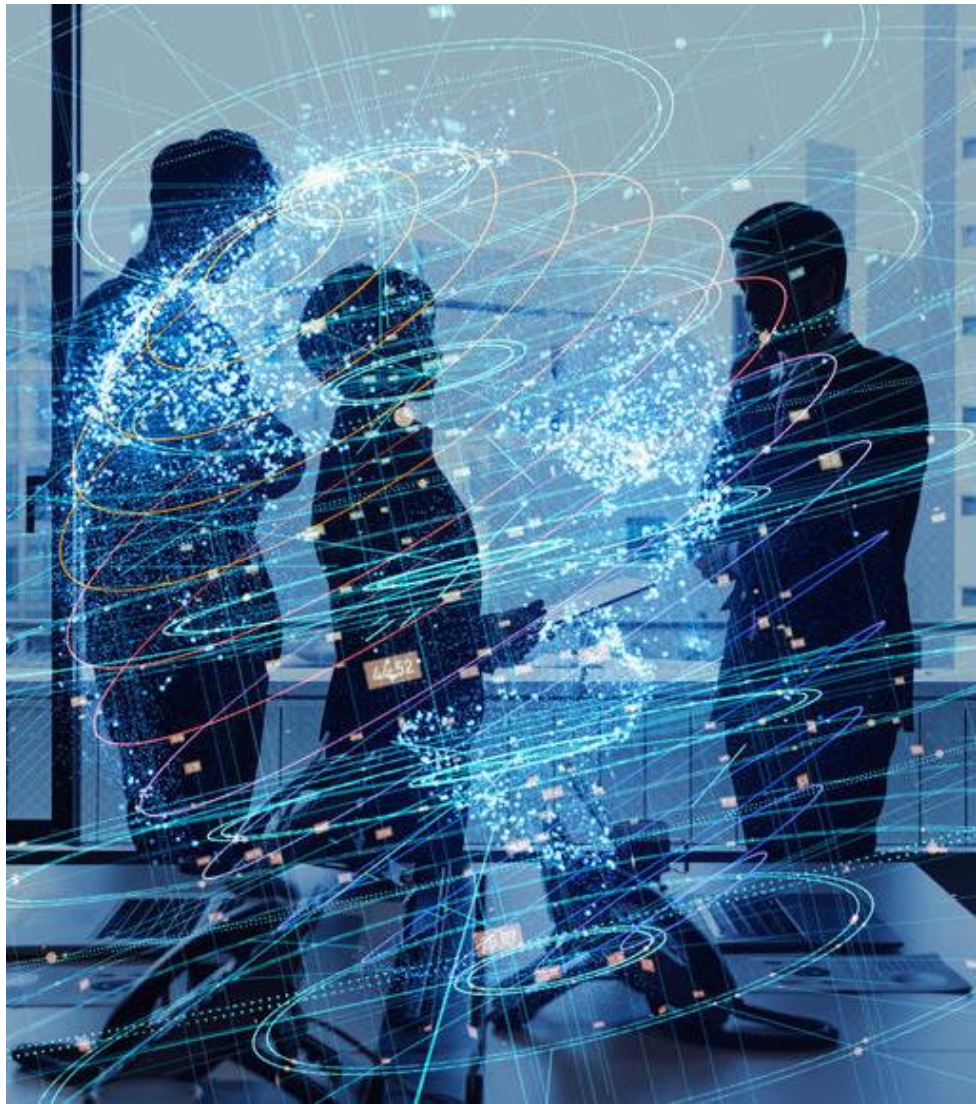
Integridad:
Propiedad de exactitud y completitud – ISO 27000

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

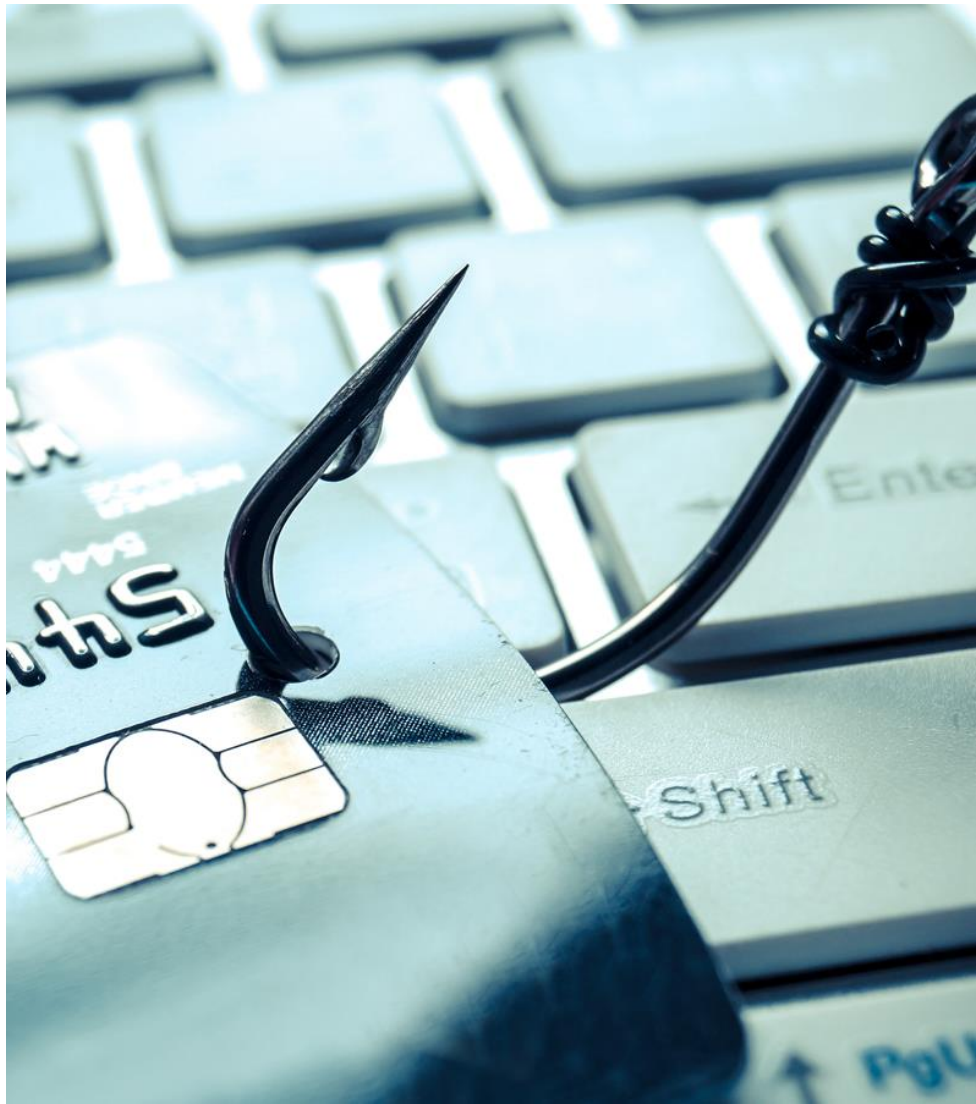
- ✓ Para hacer más sencillo el proceso de implementación, es bueno contar con la ayuda de una empresa especializada o un profesional especializado que asesore durante todo el proceso
- ✓ El tiempo de implementación del sistema de gestión de seguridad de la información varía en función del tamaño de la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

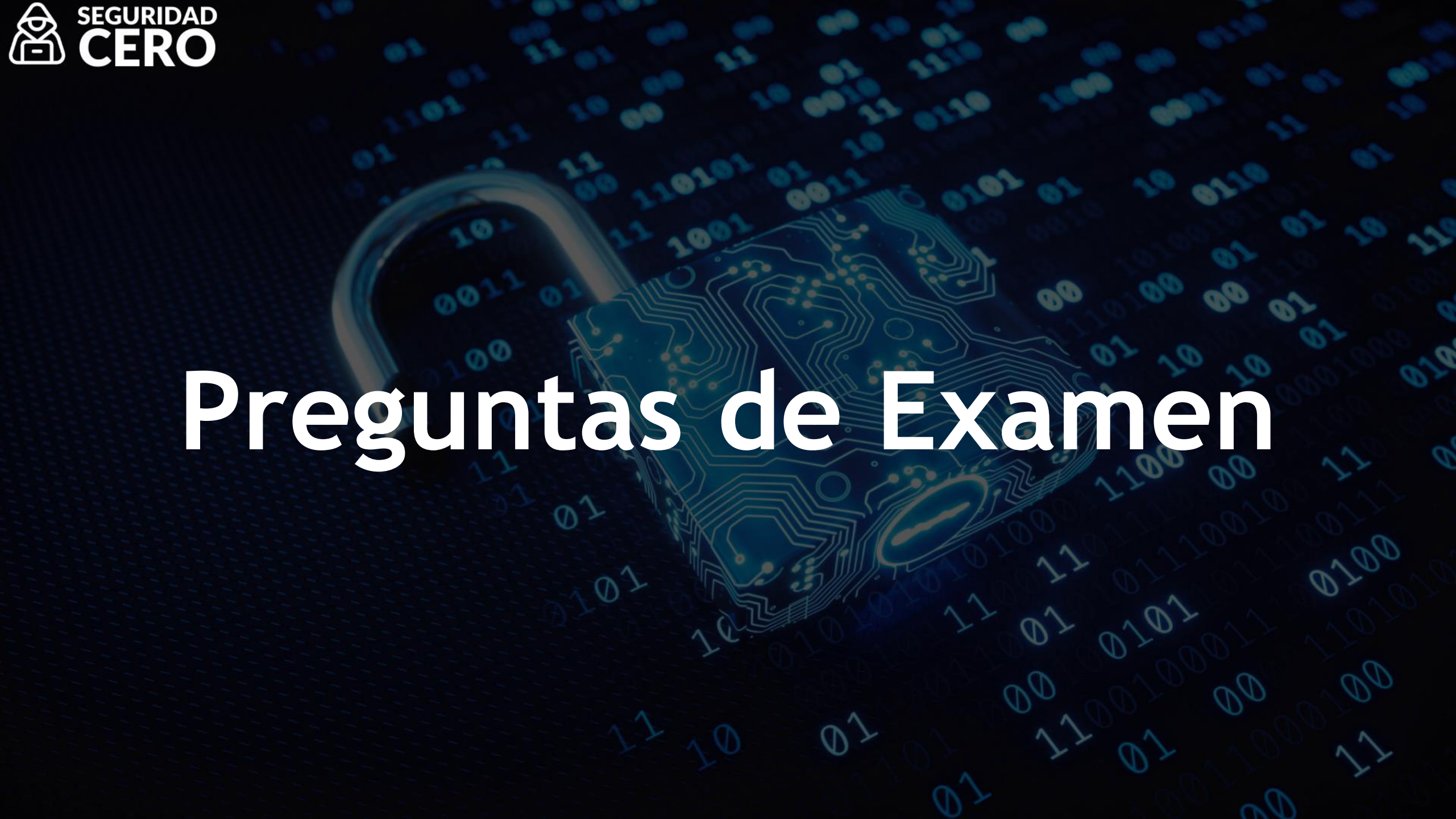
- ✓ La organización debe contar con una estructura organizacional así como de recursos necesarios, entre otras cosas, para llevar a cabo la implementación del SGSI
- ✓ Realizar un Análisis de Riesgos que valore los activos de información y vulnerabilidades a las que están expuestas. Así mismo, es necesario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


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 #2

ISO 27001 Implementador

MIERCOLES 28 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 Gestión de Seguridad de la Información?

¿Qué es Gestión de Seguridad de la Información?

La gestión de seguridad de la información se puede entender como la adición de elementos de administración (actividades, recursos, responsabilidades) a temas técnicos, normativos, de cumplimiento legal, y todo lo relacionado con la seguridad.

Consiste en orquestar todos estos elementos para que se alineen de acuerdo a los objetivos de la organización, brinden valor y logran los objetivos de la seguridad frente al negocio.

SEGURIDAD CERO

¿Qué es un Sistema de Gestión de Seguridad de la Información?

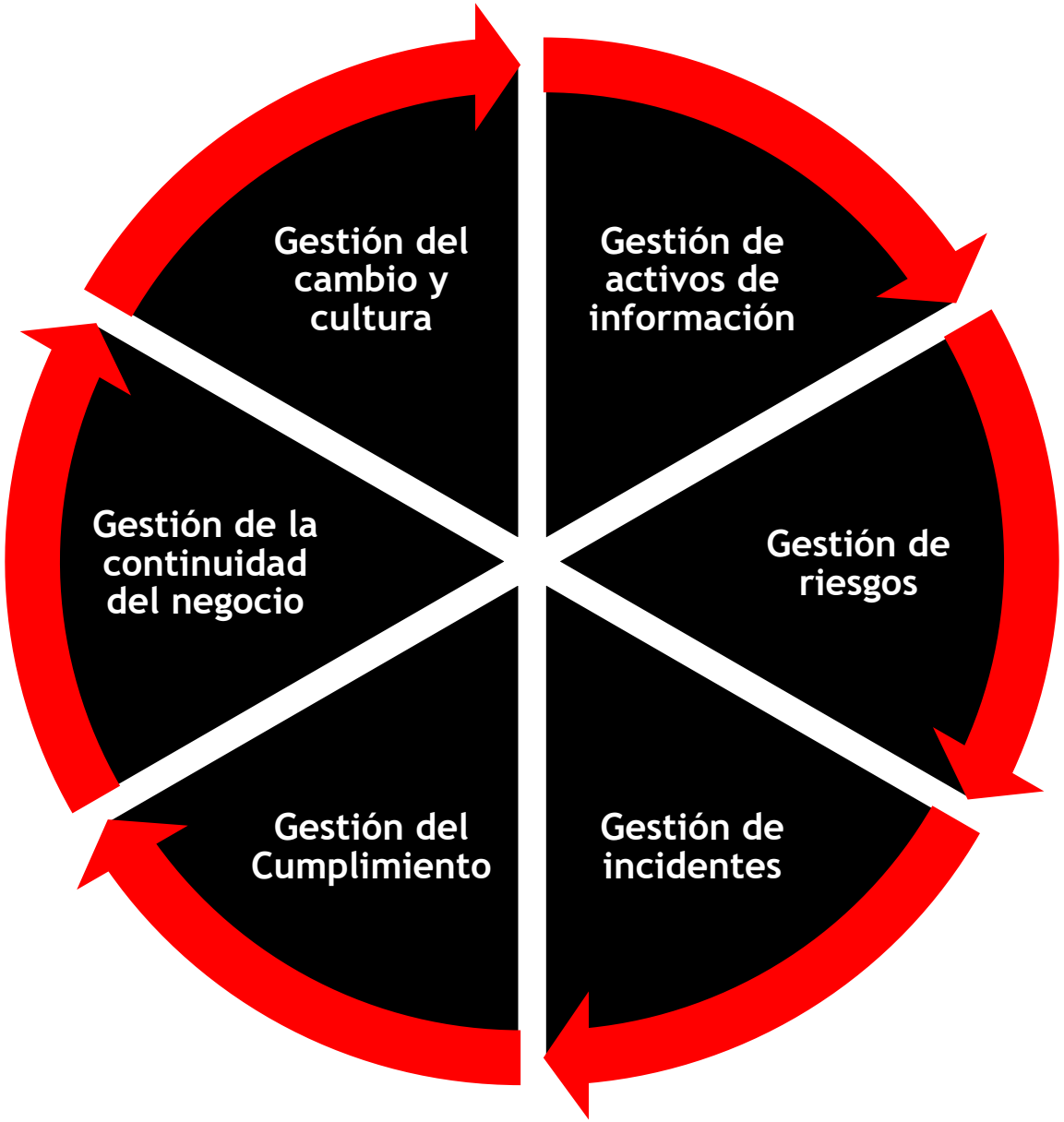
¿Qué es un Sistema de Gestión de Seguridad de la Información?

El sistema de gestión de seguridad de la información en adelante SGSI es un conjunto de elementos interrelacionados (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión de riesgos y mejora continua

SEGURIDAD CERO

Gestión Integral de Seguridad de la Información

Gestión Integral de Seguridad de la Información



SEGURIDAD CERO

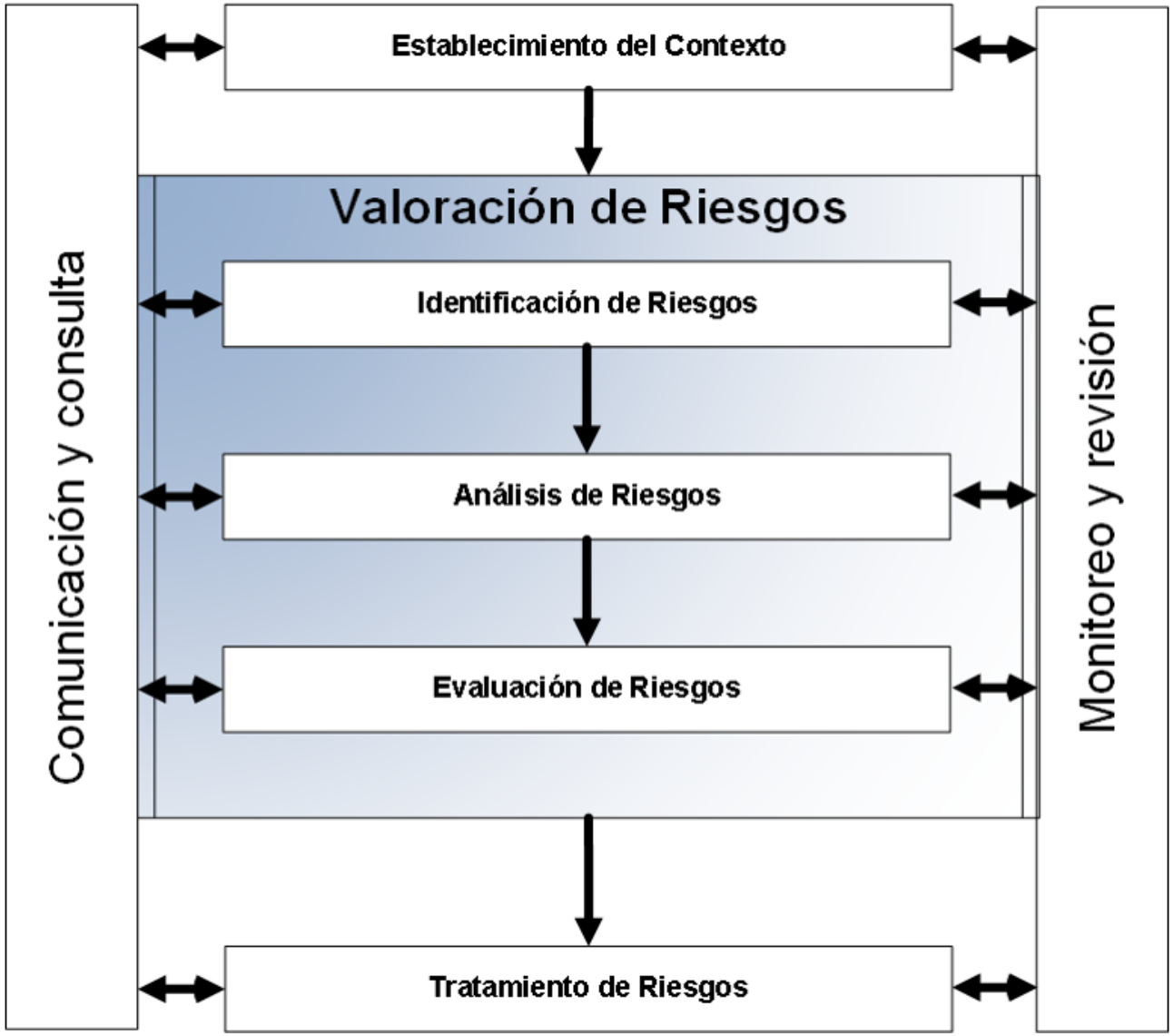
Gestión de Activos de Información

Gestión de Activos de Información

SEGURIDAD CERO

Gestión de Riesgos

Gestión de Riesgos



SEGURIDAD CERO

Gestión de Incidentes

Gestión de Incidentes

SEGURIDAD CERO

Gestión de Cumplimiento


return
COMPLIANCE

SEGURIDAD CERO

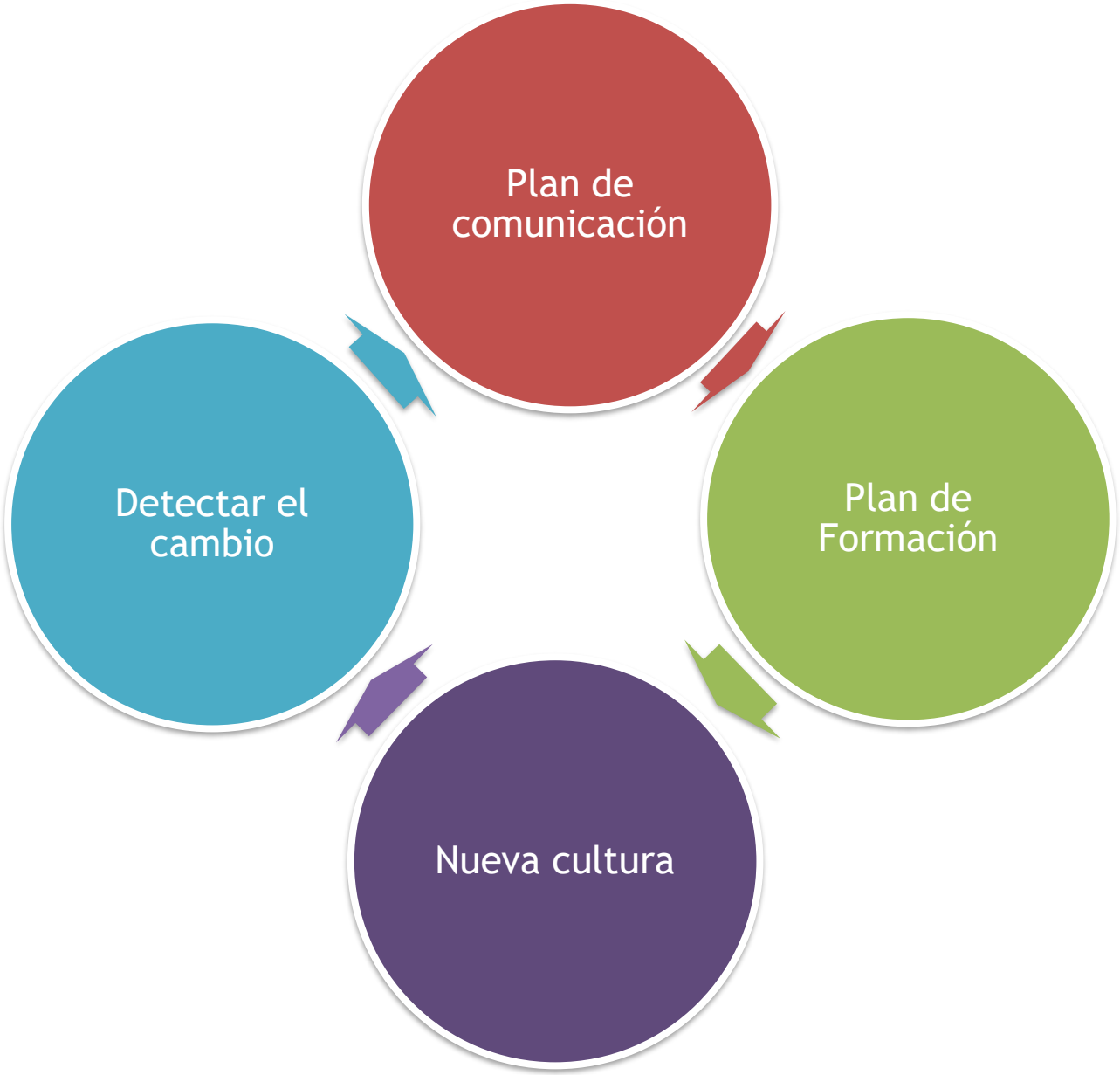
Gestión de la Continuidad

Gestión de Incidentes

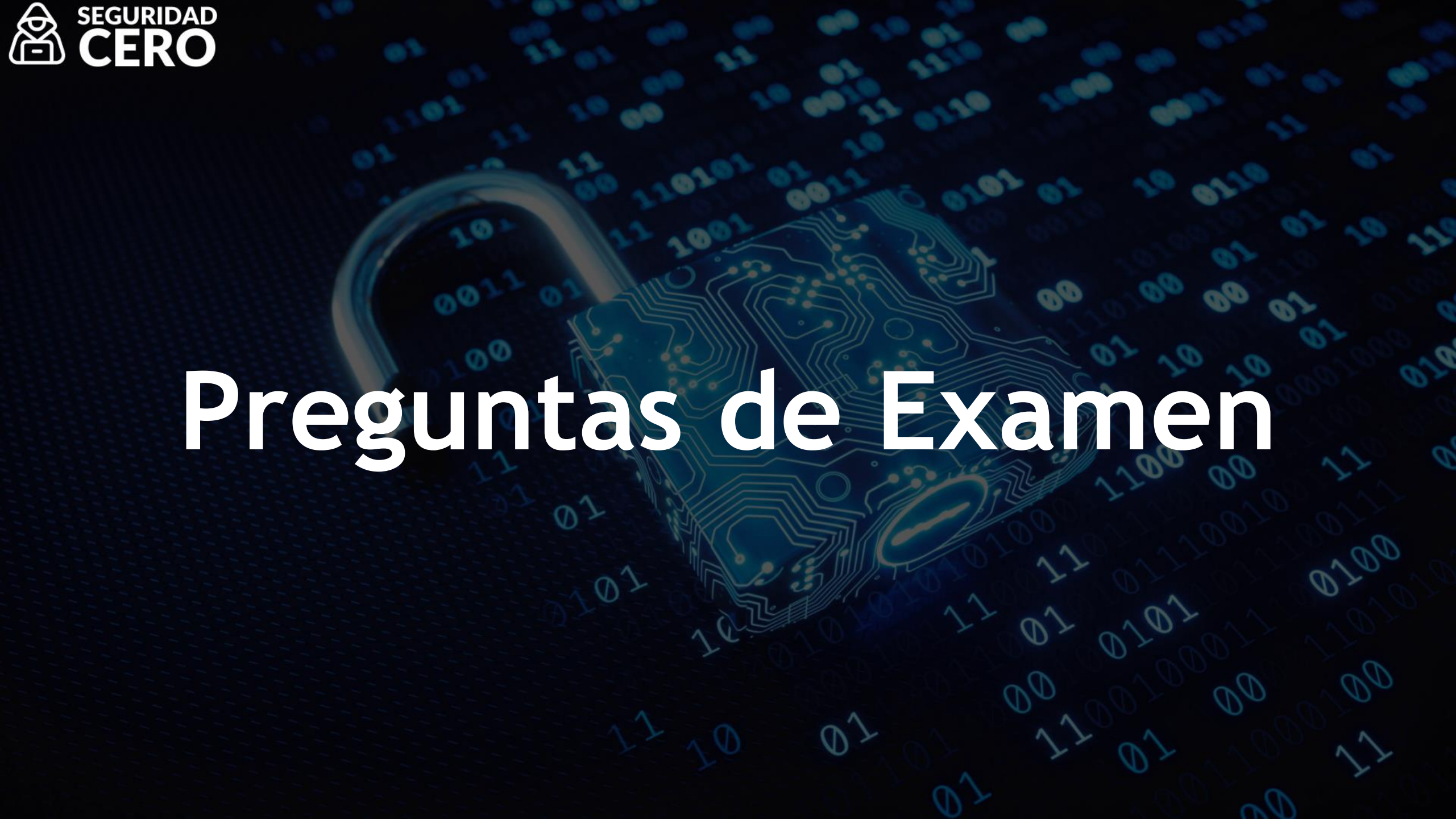
SEGURIDAD CERO

Gestión del Cambio y Cultura

Gestión de Incidentes



SEGURIDAD CERO



Preguntas de Examen

Pregunta #1

¿Qué es un Sistemas de Gestión de Seguridad de la Información?

a) Conjunto de políticas, procedimientos, guías, recursos y actividades asociadas, que son gestionados de manera colectiva por una organización.

b) Consta de todas la tecnologías de seguridad como WAF, Firewall, IDS/IPS, antivirus, EDR.

c) Es un servicio de un tercero para proteger a la organización de todo riesgo de seguridad

d) Ninguna de las anteriores

Pregunta #1

¿Qué es un Sistemas de Gestión de Seguridad de la Información?

a) Conjunto de políticas, procedimientos, guías, recursos y actividades asociadas, que son gestionados de manera colectiva por una organización.

b) Consta de todas la tecnologías de seguridad como WAF, Firewall, IDS/IPS, antivirus, EDR.

c) Es un servicio de un tercero para proteger a la organización de todo riesgo de seguridad

d) Ninguna de las anteriores

Pregunta #2

¿Qué es un sistema de gestión de incidentes de seguridad de la información ?

a) Enfoque estructurado y planificado que permita manejar adecuadamente los incidentes de seguridad de la información.

b) Tecnología que permite detectar los incidentes y abordarlos.

c) Equipo de personas encargadas de responder ante los incidentes de seguridad

d) b y c

Pregunta #2

¿Qué es un sistema de gestión de incidentes de seguridad de la información ?

a) Enfoque estructurado y planificado que permita manejar adecuadamente los incidentes de seguridad de la información.

b) Tecnología que permite detectar los incidentes y abordarlos.

c) Equipo de personas encargadas de responder ante los incidentes de seguridad

d) b y c

Pregunta #3

¿Qué proceso no forma parte de la gestión integral de la seguridad de la información?

a) Gestión de Incidentes

b) Gestión de la Continuidad

c) Gestión de Riesgos

d) Gestión de Datos Personales

Pregunta #3

¿Qué proceso no forma parte de la gestión integral de la seguridad de la información?

a) Gestión de Incidentes

b) Gestión de la Continuidad

c) Gestión de Riesgos

d) Gestión de Datos Personales

SEGURIDAD CERO

CLASE #2

ISO 27001 Implementador

MIERCOLES 28 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
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 #3

ISO 27001 Auditor

SEGURIDAD CERO

¿Qué es la ISO 19011?

¿Qué es la ISO 19011?

Esta norma proporciona una guía para todos los tamaños y tipos de organizaciones y auditorías de diferentes alcances y escalas.

Esto incluye aquellas realizadas por grandes equipos de auditoría, generalmente de organizaciones más grandes, y aquellas realizadas por auditores individuales, ya sea en organizaciones grandes o pequeñas.

Esta orientación debería adaptarse según corresponda al alcance, la complejidad y la escala del programa de auditoría.

SEGURIDAD CERO

Alcance ISO 19011

Alcance ISO 19011

Este documento proporciona orientación sobre auditoría a sistemas de gestión, incluidos los principios de auditoría, la gestión de un programa de auditoría y la realización de auditorías del sistema de gestión, así como orientación sobre la evaluación de la competencia de las personas involucradas en el proceso de auditoría.

Estas actividades incluyen las personas que administran el programa de auditoría, los auditores y los equipos de auditoría.

Es aplicable a todas las organizaciones que necesitan planificar y llevar cabo auditorías internas o externas de los sistemas de gestión o administrar un programa de auditoría. La aplicación de este documento a otros tipos de auditorías es posible, siempre que se otorgue una consideración especial a la competencia específica necesaria.

SEGURIDAD CERO

¿Qué es Auditoria?

¿Qué es Auditoria?

Proceso sistemático, independiente y documentado para obtener evidencia objetiva y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría.

Nota 1: las auditorías internas, a veces llamadas auditorías de primera parte, son realizadas por, o en nombre de, la organización misma.

Nota 2: Las auditorías externas incluyen aquellas generalmente llamadas auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por las partes que tienen un interés en la organización, como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte son llevadas a cabo por organizaciones de auditoría independientes, como aquellas que proporcionan certificación / registro de conformidad o agencias gubernamentales.

SEGURIDAD CERO

Tipos de Auditoria

Tipos de Auditoria

Auditoria de primera parte	Auditoria de segunda parte	Auditoria de tercera parte
Auditoria Interna	Auditoria de proveedor externo	Auditoria de certificación y/o acreditación
	Otra auditoria de parte interesada externa	Auditoria legal, regulatoria y similar

SEGURIDAD CERO

Principios de Auditoria

Principios de Auditoria

1. **Integridad:** la base del profesionalismo
2. **Presentación justa:** la obligación de informar veraz y exactamente
3. **Debido cuidado profesional:** la aplicación de la diligencia y el juicio en la auditoría
4. **Confidencialidad:** seguridad de la información
5. **Independencia:** la base para la imparcialidad de la auditoría y la objetividad de las conclusiones de la auditoría
6. **Enfoque basado en la evidencia:** el método racional para llegar a conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático
7. **Enfoque basado en el riesgo:** un enfoque de auditoría que considera riesgos y oportunidades

SEGURIDAD CERO

Competencia y Evaluación de los Auditores

Competencia y Evaluación de los Auditores

Poseer cualidades personales, tales como diplomacia, sinceridad, percepción, persistencia, etc. Para que la auditoría se realice en forma profesional y correcta a la vez.

Poseer conocimientos genéricos y habilidades tales como:

- Aplicar principios, procedimientos y técnicas de auditoría
- Planificar y organizar el trabajo en forma eficaz
- Conocer los códigos, leyes y normativas locales, regionales y nacionales

Poseer un adecuado nivel de educación, experiencia laboral, capacitación como auditor y experiencia en auditorías.

Mantener y mejorar en forma continua sus habilidades y competencias.


SEGURIDAD
CERO
Atributos Personales de los
Auditores

Atributos Personales de los Auditores

A. **Ético,** es decir, justo, veraz, sincero, honesto y discreto
B. **De mente abierta,** es decir, dispuesto a considerar ideas o puntos de vista alternativos
C. **Diplomático,** es decir, discreto al tratar con individuos
D. **Observador,** es decir, observando activamente el entorno físico y las actividades
E. **Perceptivo,** es decir, consciente de y capaz de comprender situaciones
F. **Versátil,** es decir, capaz de adaptarse fácilmente a diferentes situaciones.
G. **Tenaz,** es decir persistente y enfocado en alcanzar objetivos.

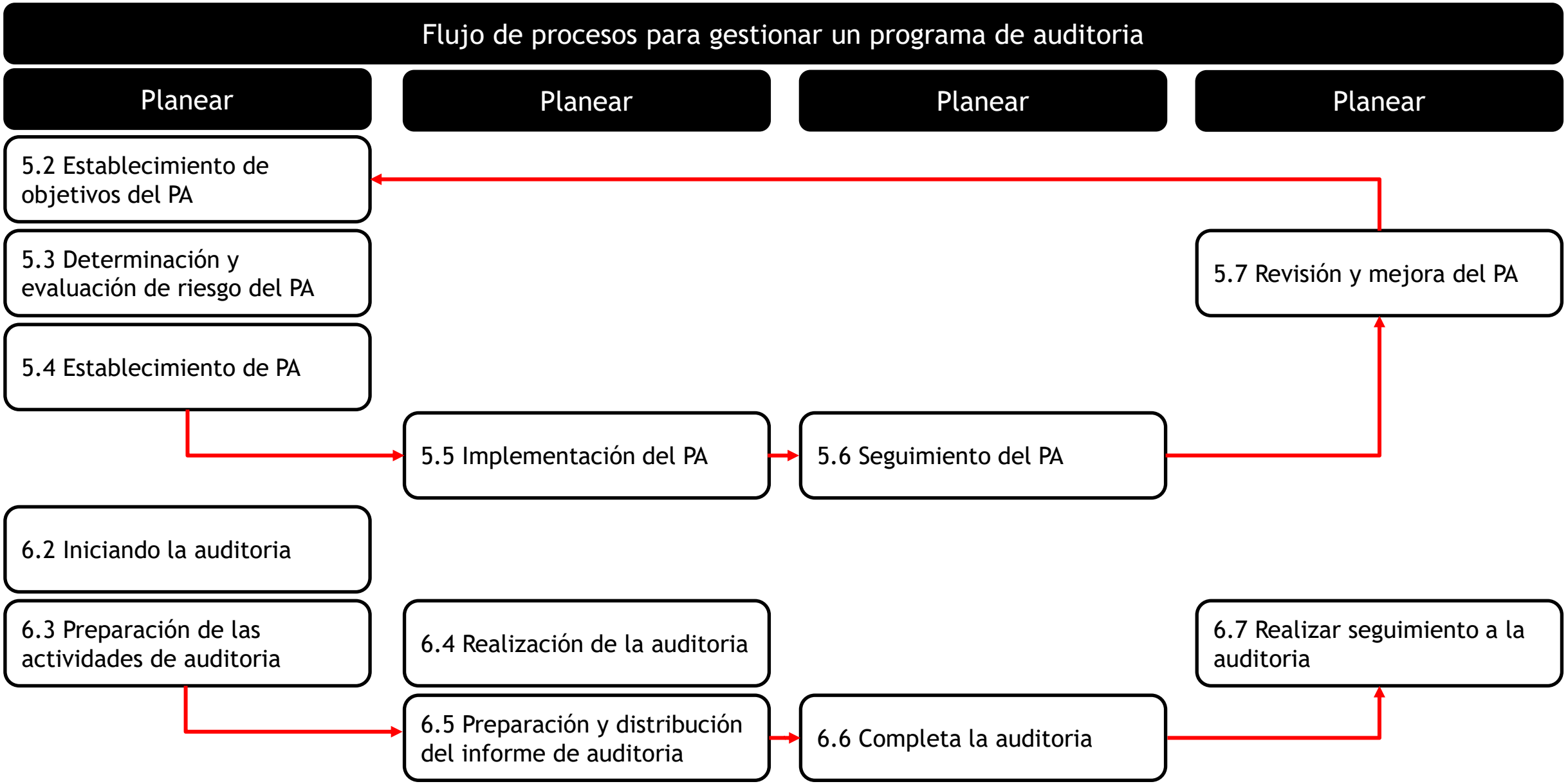
Atributos Personales de los Auditores

H. Decisivo, es decir, capaz de llegar a conclusiones oportunas basadas en el razonamiento lógico y el análisis;
I. Autosuficiente, es decir, capaz de actuar y funcionar independientemente mientras interactúa efectivamente con otros
J. Capaz de actuar con fortaleza, es decir, capaz de actuar de manera responsable y ética, aunque estas acciones no siempre sean populares y en ocasiones pueden dar lugar a desacuerdos o confrontaciones;
K. Abierto a la mejora, es decir, dispuesto a aprender de las situaciones
L. Culturalmente sensible, es decir, atento y respetuoso con la cultura del auditado
M. Colaborador, es decir, interacción efectiva con otros, incluidos los miembros del equipo de auditoría y el personal del auditado.

SEGURIDAD CERO

Programa de la Auditoria

Programa de Auditoria



SEGURIDAD CERO

Actividades de Auditoria

Actividades de Auditoria

01

6.2 Inicio de Auditoria
6.2.1 Generalidades
6.2.2 Establecer el contacto con el auditado
6.2.3 Determinación de la viabilidad de la auditoria

02

6.3 Preparación de Actividades de Auditoria
6.3.1 Realizar revisión de información documentada
6.3.2 Planificación de auditoria
6.3.3 Asignación del trabajo al equipo de auditoria
6.3.4 Preparación de información documentada para la auditoria

03

6.4 Realización de las actividades de auditoria
6.4.1 Generalidades
6.4.2 Asignación de roles y responsabilidades de guías y observadores
6.4.3 Realización de las reuniones de apertura
6.4.4 Comunicación durante la auditoria
6.4.5 Disponibilidad y acceso a la información de auditoria
6.4.6 Revisión de información documentada durante la realización de la auditoria
6.4.7 Recopilación y verificación de información
6.4.8 Generalidades de hallazgos de auditoria
6.4.9 Determinación de conclusiones de auditoria
6.4,10 Realización de la reunión de cierre

Actividades de Auditoria

04

6.5 Preparación y distribución del informe de auditoria
6.5.1 Preparación del informe de auditoria
6.5.2 Distribuir el informe de auditoria

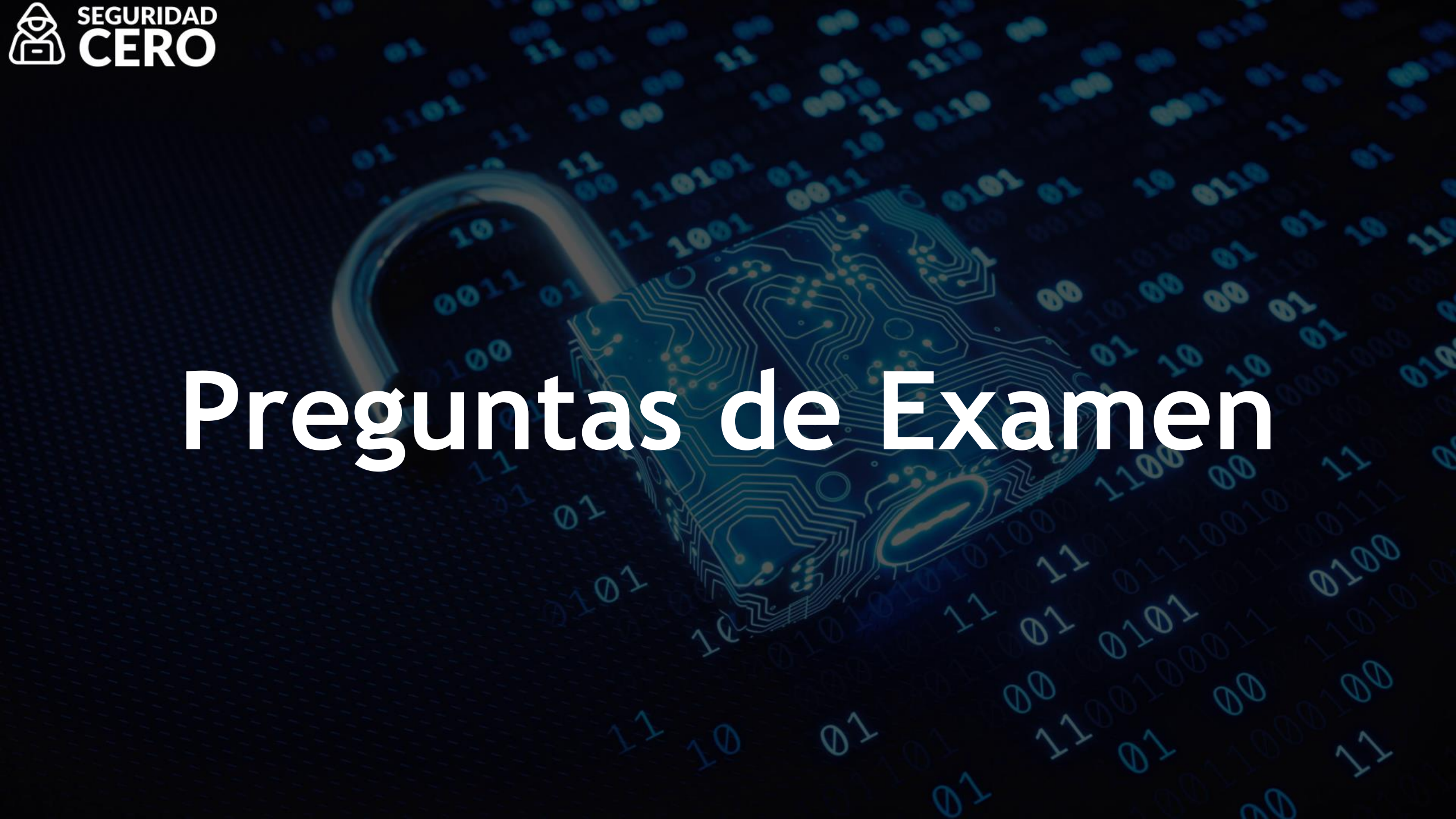
05

6.6 Completar la auditoria

06

6.7 Seguimiento de la auditoria
(Si se aplica en el seguimiento de la auditoria)

SEGURIDAD CERO



Preguntas de Examen

Pregunta #1

¿Basados en la ISO 19011, actividades dentro de la preparación de la auditoría incluyen?

a) Revisar la documentación

b) Preparar el plan de auditoria

c) Asignar el trabajo al equipo auditor

d) Todas las anteriores

Pregunta #1

¿Basados en la ISO 19011, actividades dentro de la preparación de la auditoría incluyen?

a) Revisar la documentación

b) Preparar el plan de auditoria

c) Asignar el trabajo al equipo auditor

d) Todas las anteriores

Pregunta #2

¿Son principios del auditor?

a) Discreción como parte de su comportamiento ético

b) Exactitud en los informes de auditoría

c) Debido cuidado profesional

d) Todas los anteriores

Pregunta #2

¿Son principios del auditor?

a) Discreción como parte de su comportamiento ético

b) Exactitud en los informes de auditoría

c) Debido cuidado profesional

d) Todas los anteriores

Pregunta #3

¿Conjunto de una o más auditorías planificadas en un periodo?

a) Plan de auditoría

b) Programa de auditoría

c) Lista de chequeo general

d) Sistema de gestión

Pregunta #3

¿Conjunto de una o más auditorías planificadas en un periodo?

a) Plan de auditoría

b) Programa de auditoría

c) Lista de chequeo general

d) Sistema de gestión

SEGURIDAD CERO

CLASE #3

ISO 27001 Auditor

SEGURIDAD CERO

Preguntas y Respuestas


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 #4

ISO 27001 Auditor Líder

LUNES 02 NOVIEMBRE

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 una Auditoria de Tercera Parte?

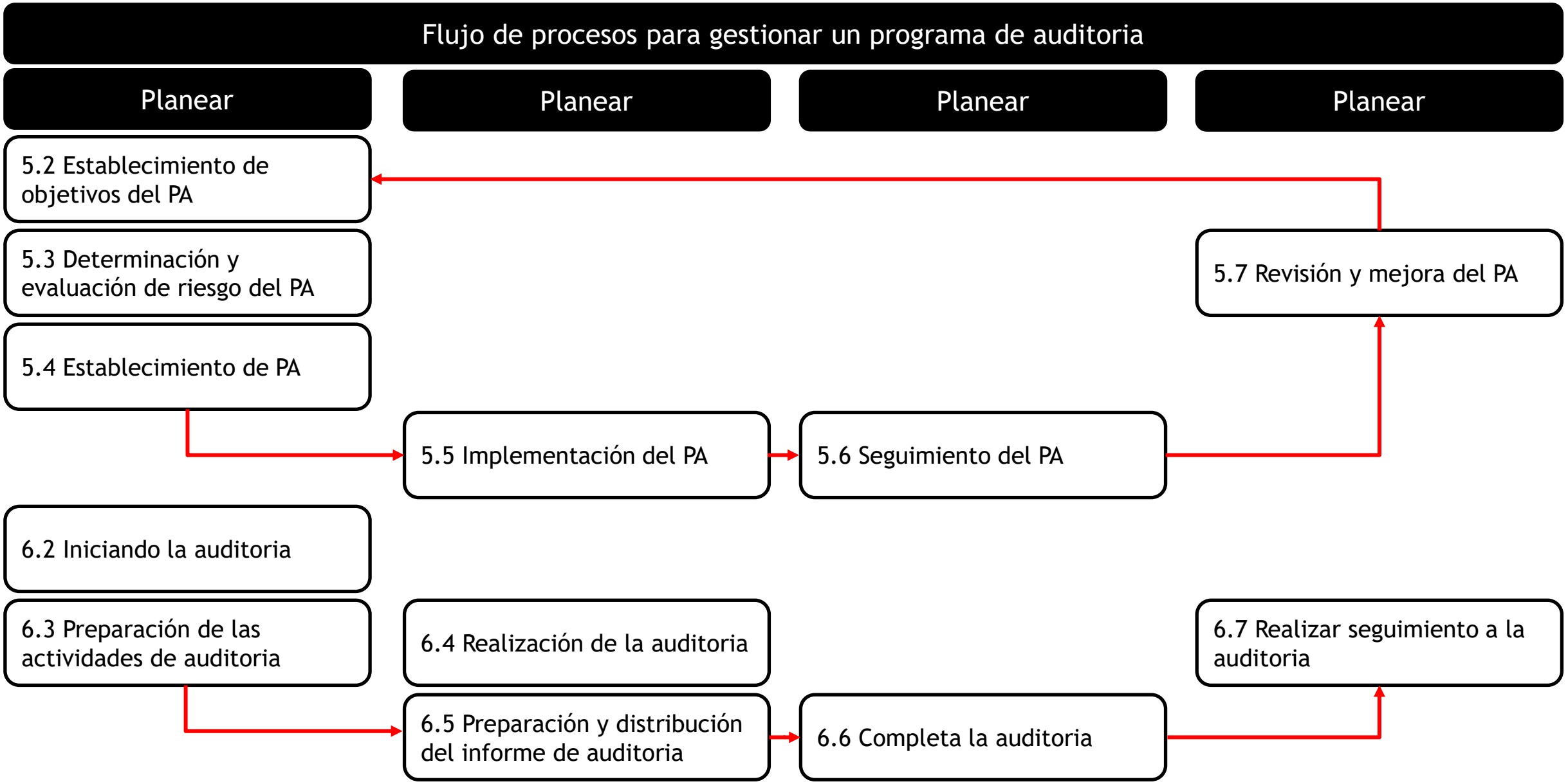
¿Qué es una Auditoria de Tercera Parte

Es la auditoría realizada por un organismo independiente de la organización, proveedores y sus clientes. Es una evaluación realizada por un Organismo Evaluador de la Conformidad de acuerdo a un sistema de gestión de seguridad de la información ISO/IEC 27001:2013

SEGURIDAD CERO

Gestión de un Programa de Auditoria

Gestión de un Programa de Auditoria




SEGURIDAD
CERO
Atributos Personales de los
Auditores

Atributos Personales de los Auditores

A. **Ético,** es decir, justo, veraz, sincero, honesto y discreto
B. **De mente abierta,** es decir, dispuesto a considerar ideas o puntos de vista alternativos
C. **Diplomático,** es decir, discreto al tratar con individuos
D. **Observador,** es decir, observando activamente el entorno físico y las actividades
E. **Perceptivo,** es decir, consciente de y capaz de comprender situaciones
F. **Versátil,** es decir, capaz de adaptarse fácilmente a diferentes situaciones.
G. **Tenaz,** es decir persistente y enfocado en alcanzar objetivos.

Atributos Personales de los Auditores

H. Decisivo, es decir, capaz de llegar a conclusiones oportunas basadas en el razonamiento lógico y el análisis;
I. Autosuficiente, es decir, capaz de actuar y funcionar independientemente mientras interactúa efectivamente con otros
J. Capaz de actuar con fortaleza, es decir, capaz de actuar de manera responsable y ética, aunque estas acciones no siempre sean populares y en ocasiones pueden dar lugar a desacuerdos o confrontaciones;
K. Abierto a la mejora, es decir, dispuesto a aprender de las situaciones
L. Culturalmente sensible, es decir, atento y respetuoso con la cultura del auditado
M. Colaborador, es decir, interacción efectiva con otros, incluidos los miembros del equipo de auditoría y el personal del auditado.

SEGURIDAD CERO

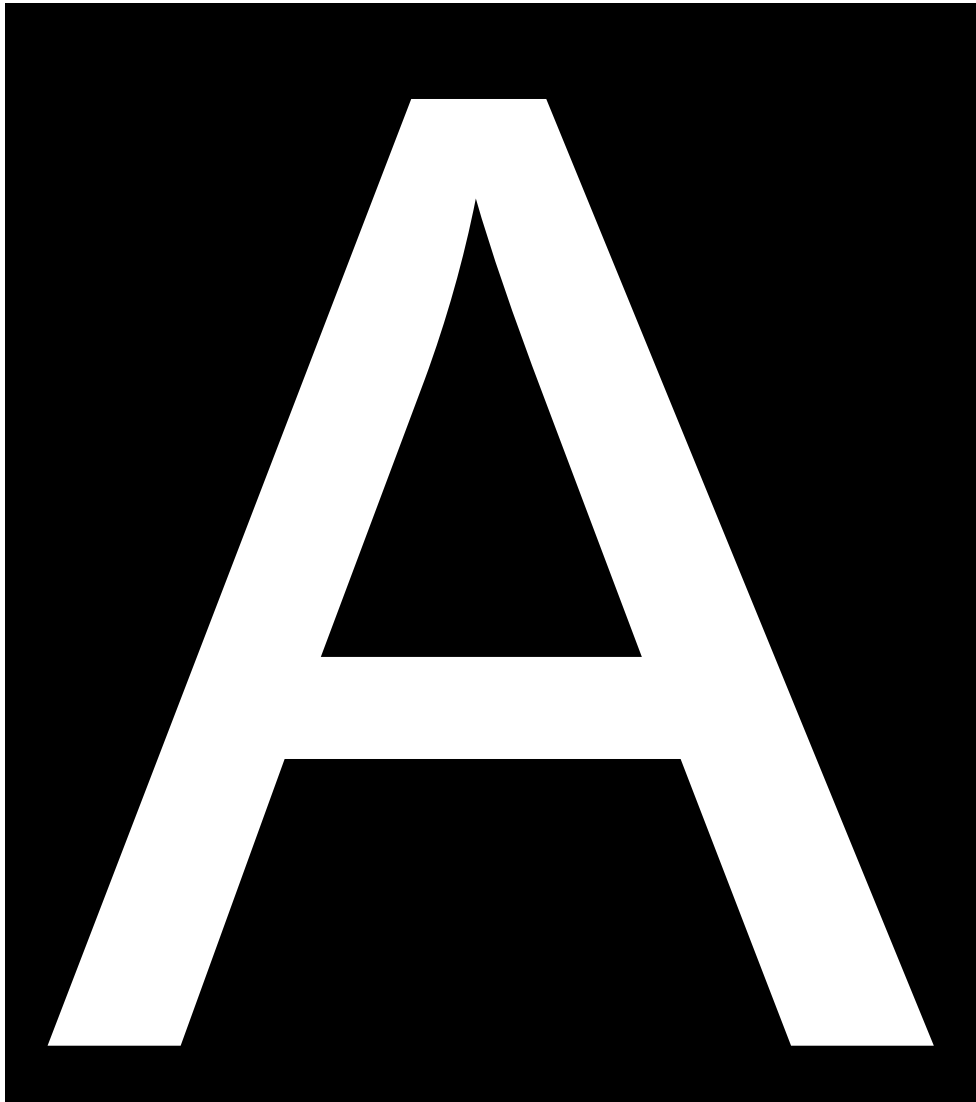
Conocimientos y Habilidades de un Auditor Líder

Conocimientos y Habilidades de un Auditor Líder

A. Principios, procesos y métodos de auditoría:

El conocimiento y las habilidades en esta área le permiten al auditor asegurar que las auditorías se realicen de manera consistente y sistemática.

- ✓ Comprender los tipos de riesgos y oportunidades asociados con la auditoría y los principios de la auditoría basada en el riesgo
- ✓ Planificar y organizar el trabajo de manera efectiva
- ✓ Realizar la auditoría dentro del cronograma acordado
- ✓ Priorizar y enfocarse en asuntos importantes
- ✓ Comunicarse de manera efectiva, oralmente y por escrito
- ✓ Evaluar la confiabilidad de los hallazgos y conclusiones
- ✓ Documentar las actividades y hallazgos de auditoría e informes
- ✓ Mantener la confidencialidad y seguridad de la información.

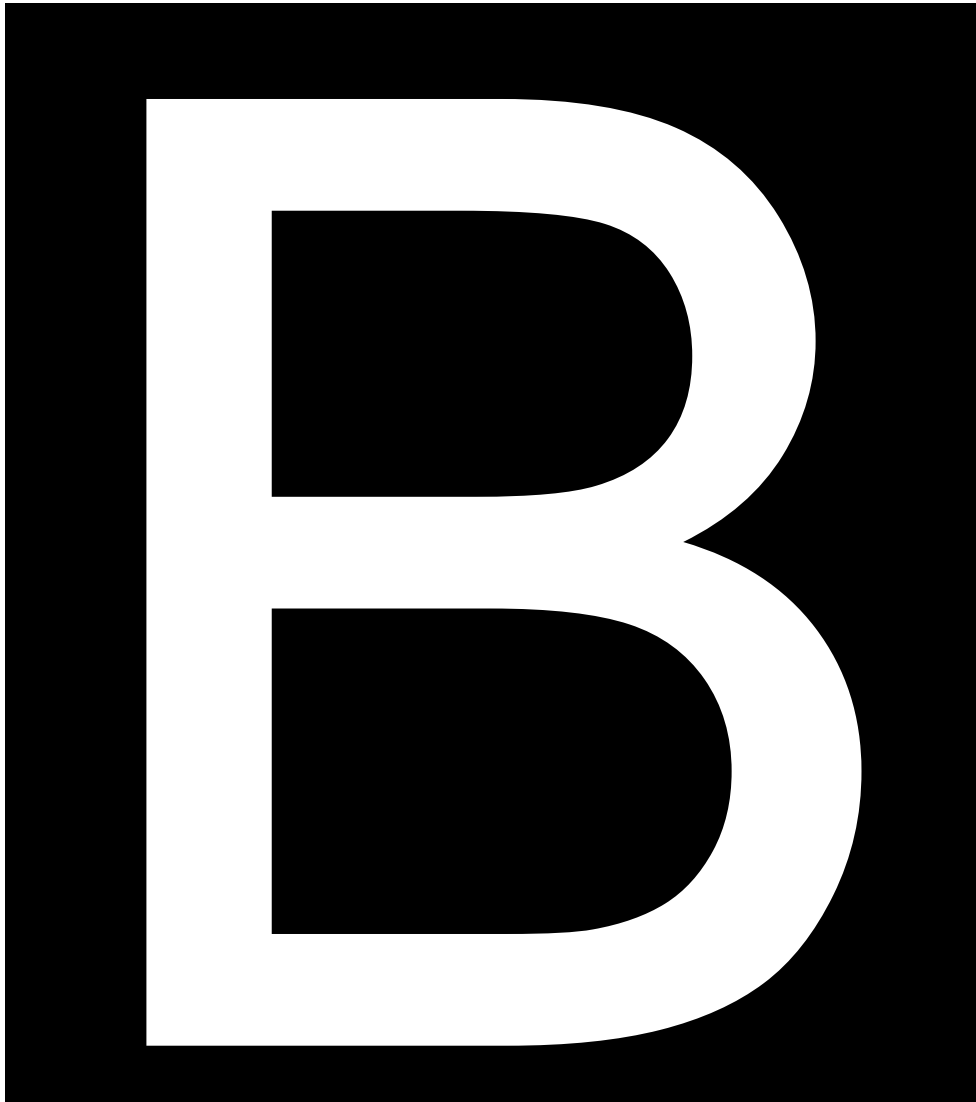


Conocimientos y Habilidades de un Auditor Líder

B. Normas del sistema de gestión y otras referencias:

El conocimiento y las habilidades en esta área le permiten al auditor comprender el alcance de la auditoría y aplicar criterios de auditoría, y deberían cubrir lo siguiente:

- ✓ Normas del sistema de gestión u otros documentos normativos u orientativos/de apoyo utilizados para establecer criterios o métodos de auditoría
- ✓ La aplicación de los estándares del sistema de gestión por el auditado y otras organizaciones
- ✓ Relaciones e interacciones entre los procesos del SGSI
- ✓ Comprender la importancia y la prioridad de múltiples estándares o referencias
- ✓ Aplicación de estándares o referencias a diferentes situaciones

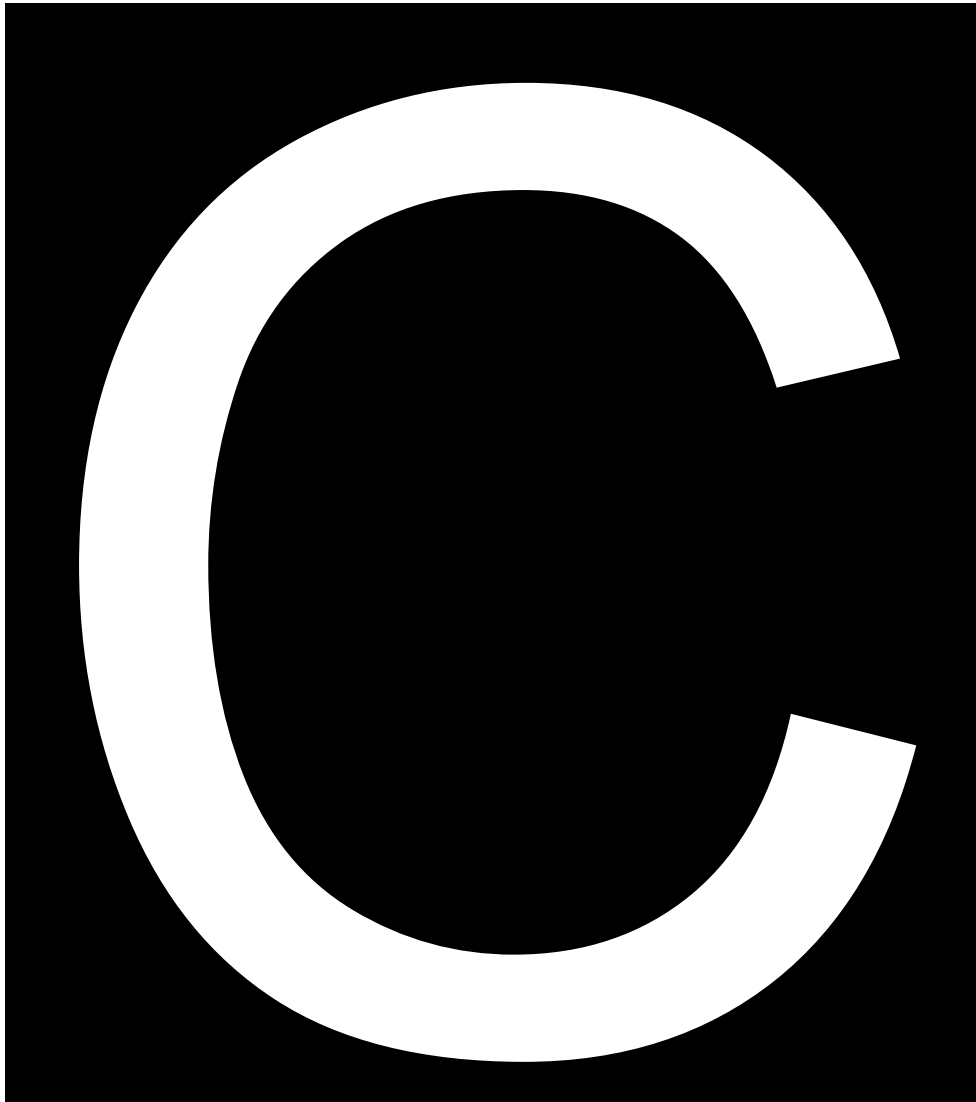


Conocimientos y Habilidades de un Auditor Líder

C. La organización y su contexto:

El conocimiento y las habilidades en esta área le permiten al auditor comprender la estructura, el propósito y las prácticas de gestión del auditado y debería cubrir lo siguiente:

- ✓ Necesidades y expectativas de las partes interesadas relevantes que impactan en el sistema de gestión;
- ✓ Tipo de organización, gobierno, tamaño, estructura, funciones y relaciones;
- ✓ Conceptos generales de negocios y gestión, procesos y terminología relacionada, incluida la planificación, presupuestación y gestión de personas;
- ✓ Aspectos culturales y sociales del auditado.

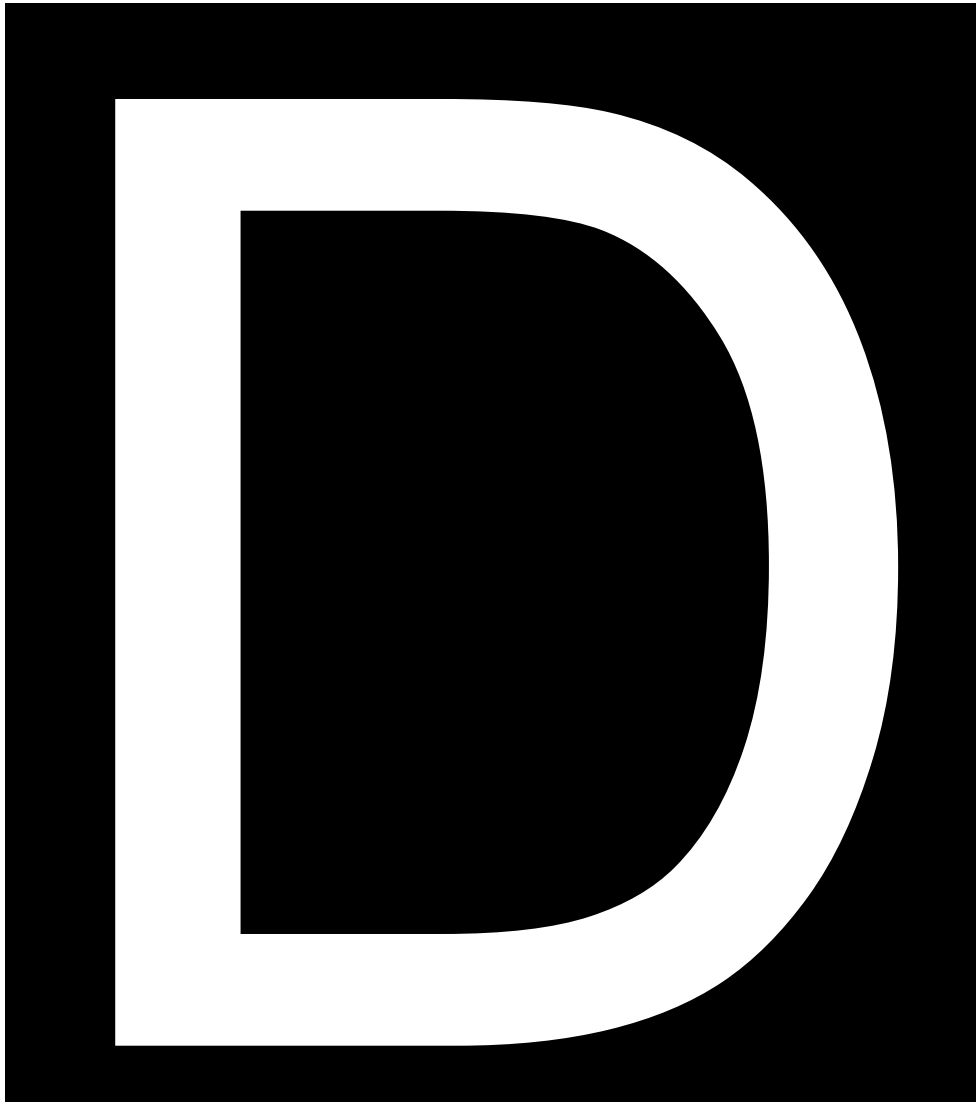


Conocimientos y Habilidades de un Auditor Líder

D. Requisitos reglamentarios y legales y otros:

El conocimiento y las habilidades en esta área le permiten al auditor conocer y trabajar dentro de los requisitos de la organización. Los conocimientos y habilidades específicos de la jurisdicción o de las actividades, procesos, productos y servicios del auditado deberían cubrir lo siguiente:

- ✓ Requisitos legales y reglamentarios, así como sus agencias de gobierno
- ✓ Terminología jurídica básica
- ✓ Contratación y responsabilidad



SEGURIDAD CERO

CLASE #4

ISO 27001 Auditor Líder

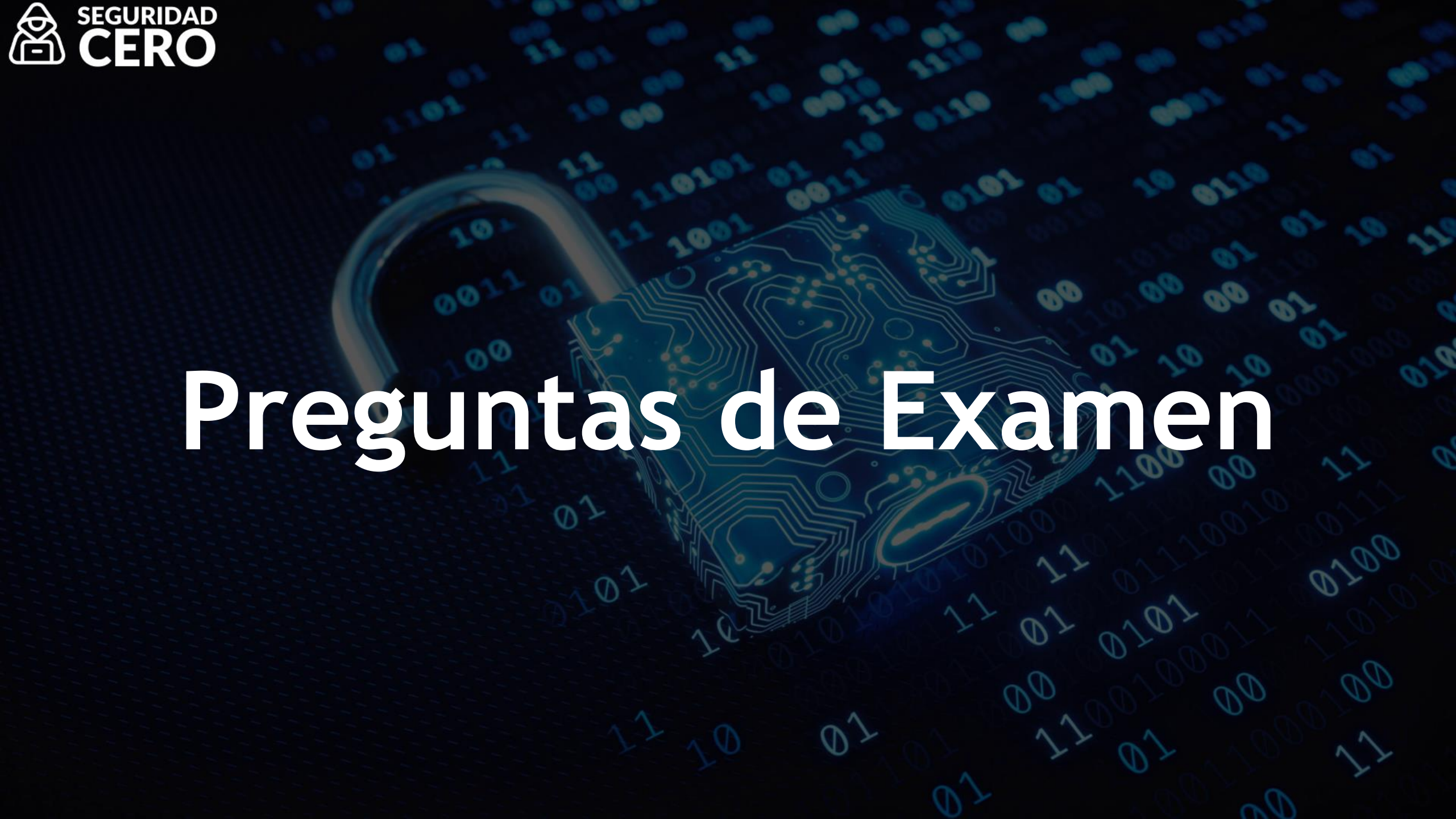
LUNES 02 NOVIEMBRE

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



Preguntas de Examen

Pregunta #1

¿Cómo abordar a un auditado que no entrega las evidencias solicitadas o extiende las fechas de entrega, poniendo en riesgo los tiempos de la auditoria?

Pregunta #1

¿Cómo abordar a un auditado que no entrega las evidencias solicitadas o extiende las fechas de entrega, poniendo en riesgo los tiempos de la auditoria?

Solicitando apoyo del sponsor del proyecto de auditoria

Establecimiento plazos máximos de entrega en base a los acuerdos iniciales

Evaluar ampliaciones en base a criterios razonables

Analizar con el cronograma de actividades cual es el tiempo máximo de espera

Contener las desviaciones reasignando los recursos del equipo de auditoria

Corroborar la integridad de las evidencias entregadas en periodos extendidos