Guía de preparación

Edición 201804

Índice

1. Visión general

EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.SP)

Alcance

EXIN Information Security Foundation based on ISO/IEC 27001 es una certificación que valida los conocimientos de un profesional acerca de lo siguiente:

- Información y seguridad: conceptos, valor de la información e importancia de la fiabilidad.
- Amenazas y riesgos: relación entre amenazas y fiabilidad.
- Enfoque y organización: política de seguridad y disposiciones para la seguridad de la información.
- Medidas: físicas, técnicas y organizativas.
  Y
- Legislación y normas: importancia y operación.

Resumen

La seguridad de la información constituye la protección de la información de una amplia gama de amenazas para, de este modo, asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el rendimiento del capital invertido, así como de las oportunidades de negocio.

La Seguridad de la Información es cada vez más importante. La globalización de la economía conduce a un creciente intercambio de información entre organizaciones (sus empleados, clientes y suministradores) y a un uso de redes cada vez mayor, como la red interna de la empresa, la conexión con redes de otras empresas e Internet.

La normativa internacional para la gestión de la seguridad de la información ISO/IEC 27001, es ampliamente respetada y citada. Además, proporciona un marco para la organización y gestión de un programa de seguridad de la información. Implantar un programa basado en esta norma servirá debidamente a una organización en su objetivo de satisfacer un gran número de los requisitos a los que se enfrenta en el complejo entorno operativo actual. Una buena comprensión de esta norma es importante para el desarrollo personal de todo profesional de la seguridad de la información.

En los módulos de Seguridad de la Información de EXIN se utiliza la siguiente definición: La Seguridad de la Información se ocupa de la definición, implantación, mantenimiento, conformidad y evaluación de un conjunto de controles (medidas) coherentes que protegen la disponibilidad, integridad y confidencialidad del suministro de información (manual o automático).

En el módulo Information Security Foundation based on ISO/IEC 27001, se evalúan los conceptos básicos de seguridad de la información y su coherencia. El conocimiento básico de este módulo contribuye a la comprensión de que la información es algo vulnerable y de que se requieren medidas para protegerla.

Contexto

El Certificado de EXIN Fundamentos de Seguridad de la Información basado en ISO/IEC 27001 es parte del programa de cualificación de Seguridad de la Información. A este módulo le siguen los Certificados de Information Security Management Professional based on ISO/IEC 27001 e Information Security Management Expert based on ISO/IEC 27001.

Grupo objetivo

El examen de Fundamentos de Seguridad de la Información basado en ISO/IEC 27001 está indicado para cualquier persona en la organización que procese información. El módulo también es apropiado para pequeños negocios independientes, para los que es necesario tener un conocimiento básico sobre la Seguridad de la Información.
Este módulo puede ser un buen comienzo para nuevos profesionales de la seguridad de la información.

Requisitos para la certificación

- Completar satisfactoriamente el examen EXIN Information Security Foundation based on ISO/IEC 27001.

Detalles del examen

Tipo de examen:	Preguntas de opción múltiple
Número de preguntas:	40
Calificación mínima para el aprobado:	65%
Consulta de libro o apuntes:	No
Equipos electrónicos permitidos:	No
Duración del examen	60 minutos

En este examen se aplican las normas de examen de EXIN.

Nivel de Bloom

La certificación EXIN Information Security Foundation based on ISO/IEC 27001 evalúa a los candidatos que se encuentran en el nivel 1 y 2 de Bloom de acuerdo con la taxonomía revisada de Bloom:

- Nivel 1 de Bloom: Conocer - se basa en recordar la información. Los candidatos tendrán que absorber, memorizar, reconocer y recordar. Este es un elemento esencial del aprendizaje antes de poder pasar a niveles superiores.
- Nivel 2 de Bloom: Comprender - un paso más allá de conocer. A este nivel, los candidatos demuestran que comprenden lo que es presentado y pueden evaluar cómo podrían aplicar el aprendizaje en su propio entorno.

Formación

Horas de contacto

El número mínimo de horas de contacto para este curso de formación es de 14 horas. Estas horas de contacto incluyen las prácticas de grupos, la preparación de exámenes y pausas breves. El número de horas no incluye el tiempo dedicado a los deberes, la logística relacionada con la sesión de examen, la sesión de examen o las pausas para almorzar.

Indicación de la carga de estudio

60 horas, dependiendo del conocimiento existente.

Proveedor de la formación

Puede consultar una lista de nuestros proveedores de formación acreditados en www.exin.com.

2. Requisitos del examen

Los requisitos del examen se detallan en las especificaciones del mismo. La tabla que se muestra a continuación, enumera los temas incluidos en el módulo (requisitos del examen) y los puntos que integran los mismos (especificaciones del examen).

Requisito del examen	Especificación del examen	Peso
1 Información y seguridad		**10%**
	1.1 El concepto de información	2.5%
	1.2 Valor de la información	2.5%
	1.3 Aspectos de fiabilidad	5%
2 Amenazas y riesgos		**30%**
	2.1 Amenaza y riesgos	15%
	2.2 Relaciones entre amenazas, riesgos y la fiabilidad de la información.	15%
3 Enfoque y Organización		**10%**
	3.1 Política de seguridad y organización de la protección	2.5%
	3.2 Componentes	2.5%
	3.3 Gestión de incidentes	5%
4 Medidas		**40%**
	4.1 Importancia de las medidas de seguridad	10%
	4.2 Medidas físicas de seguridad	10%
	4.3 Medidas técnicas	10%
	4.4 Medidas organizativas	10%
5 Legislación y normas		**10%**
	5.1 Legislación y normas	10%
	Total	100%

Especificaciones del examen

1 Información y seguridad

1.1 El concepto de información

El candidato puede…

1.1.1 explicar la diferencia entre datos e información.

1.1.2 describir el medio de almacenamiento que forma parte de la infraestructura básica.

1.2 Valor de la información

El candidato puede…

1.2.1 describir el valor de los datos/información para las organizaciones.

1.2.2 describir cómo el valor de los datos/información puede influir en las organizaciones.

1.2.3 explicar cómo los conceptos aplicados de la seguridad de la información protegen el valor de los datos/información.

1.3 Cuestiones de fiabilidad

El candidato puede…

1.3.1 identificar las cuestiones de fiabilidad de la información.

1.3.2 describir las cuestiones de fiabilidad de la información.

2 Amenazas y riesgos

2.1 Amenaza y riesgo

El candidato puede…

2.1.1 explicar los conceptos de amenaza, riesgo y análisis de riesgo.

2.1.2 explicar la relación entre una amenaza y un riesgo.

2.1.3 describir varios tipos de amenazas.

2.1.4 describir varios tipos de daño.

2.1.5 describir varias estrategias en materia de riesgos.

2.2 Relaciones entre amenazas, riesgos y la fiabilidad de la información

El candidato puede…

2.2.1 reconocer ejemplos de varios tipos de amenazas.

2.2.2 describir los efectos que tienen los distintos tipos de amenazas en la información y en el tratamiento de la información.

3 Enfoque y organización

3.1 Política de seguridad y organización de la protección

El candidato puede…

3.1.1 resumir los objetivos y el contenido de la política de seguridad.

3.1.2 resumir los objetivos y el contenido de la organización de la seguridad.

3.2 Componentes

El candidato puede…

3.2.1 explicar la importancia de un código de conducta.

3.2.2 explicar la importancia de la propiedad.

3.2.3 identificar los roles más importantes en la organización de la seguridad de la información.

3.3 Gestión de incidentes

El candidato puede…

3.3.1 resumir cómo se notifican los incidentes de seguridad y qué información se requiere.
3.3.2 dar ejemplos de incidentes de seguridad.
3.3.3 explicar las consecuencias de no notificar los incidentes de seguridad.
3.3.4 explicar qué implica el escalado de incidentes (funcional y jerárquicamente).
3.3.5 describir los efectos del escalado de incidentes en la organización.
3.3.6 explicar el ciclo de los incidentes.

4 Medidas

4.1 Importancia de las medidas de

El candidato puede…

4.1.1 describir varias formas en las que las medidas de seguridad pueden estructurarse u organizarse.
4.1.2 dar ejemplos de cada tipo de medida de seguridad.
4.1.3 explicar la relación entre riesgos y medidas de seguridad.
4.1.4 explicar el objetivo de la clasificación de la información.
4.1.5 describir el efecto de la clasificación.

4.2 Medidas físicas de seguridad

El candidato puede…

4.2.1 dar ejemplos de medidas físicas de seguridad.
4.2.2 describir los riesgos que conllevan unas medidas físicas de seguridad insuficientes.

4.3 Medidas técnicas

El candidato puede…

4.3.1 dar ejemplos de medidas técnicas de seguridad.
4.3.2 describir los riesgos que conllevan unas medidas técnicas de seguridad insuficientes.
4.3.3 comprender los conceptos de criptografía, firma y certificado digital.
4.3.4 identificar los tres pasos de la banca en línea (PC, sitio Web, pago).
4.3.5 identificar varios tipos de software malicioso.
4.3.6 describir las medidas que pueden utilizarse contra el software malicioso.

4.4 Medidas organizativas

El candidato puede…

4.4.1 dar ejemplos de medidas organizativas de seguridad.
4.4.2 describir los peligros y riesgos que conllevan unas medidas organizativas de seguridad insuficientes.
4.4.3 describir medidas de seguridad de acceso como la separación de cometidos y el uso de contraseñas.
4.4.4 describir los principios de gestión de acceso.
4.4.5 describir los conceptos de identificación, autenticación y autorización.
4.4.6 explicar la importancia para una organización de una Gestión de la Continuidad de Negocio bien establecida.
4.4.7 explicar la importancia de realizar ejercicios de prueba.

5 Legislación y normas

5.1 Legislación y normas

El candidato puede…

- 5.1.1 explicar por qué la legislación y las normas son importantes para la fiabilidad de la información.
- 5.1.2 dar ejemplos de legislación relacionada con la seguridad de la información.
- 5.1.3 dar ejemplos de normas relacionadas con la seguridad de la información.
- 5.1.4 indicar posibles medidas que puedan tomarse a fin de satisfacer los requisitos de legislación y normas.

3. Lista de conceptos del examen

En este capítulo se incluyen los términos y abreviaturas con los que los candidatos deberán familiarizarse.

Es necesario tener en cuenta que sólo el conocimiento de estos términos no es suficiente para aprobar el examen. Los candidatos deberán comprender los conceptos y ser capaces de poner ejemplos.

Inglés	Español
Access control	Control de acceso
Asset	Activo
Audit	Auditoría
Authentication	Autenticación
Authenticity	Autenticidad
Authorization	Autorización
Availability	Disponibilidad
Backup	Copia de seguridad
Biometrics	Biométrica
Botnet	Botnet
Business Assets	Activos del negocio
Business Continuity Management (BCM)	Gestión de la continuidad del Negocio
Business Continuity Plan (BCP)	Plan de continuidad del Negocio
Category	Categoría
Certificate	Certificado
Change Management	Gestión de Cambios
Classification (grading)	Clasificación (gradación)
Clear desk policy	Política de puesto despejado
Code of conduct	Código de conducta
Code of practice for information security (ISO/IEC 27002)	Código de buenas prácticas para la seguridad de la información (ISO/IEC 27002)
Completeness	Completitud
Compliance	Conformidad
Computer criminality legislation	Legislación sobre delincuencia informática
Confidentiality	Confidencialidad
Continuity	Continuidad
Controls	Controles
Copyright legislation	Legislación sobre los derechos de autor
Corrective	Correctivas
Correctness	Fidelidad
Cryptography	Criptografía
Cyber crime	Cyber crime
Damage	Daño
Data	Datos
Detective	De detección
Digital signature	Firma digital
Direct damage	Daño directo

Disaster	Desastre
Disaster Recovery Plan (DRP)	Plan de Recuperación de Desastres
Encryption	Encriptación
Escalation • Functional escalation • Hierarchical escalation	Escalado/Escalación • Escalado/Escalación funcional • Escalado/Escalación jerárquica
Exclusivity	Exclusividad
Hacking	Hacking
Hoax	Hoax
Identification	Identificación
Impact	Impacto
Incident cycle	Ciclo del incidente
Indirect damage	Daño indirecto
Information	Información
Information analysis	Análisis de la información
Information architecture	Arquitectura de la información
Information management	Gestión de la información
Information security review	Sistema de información
Information system	Revisión de la seguridad de la información
Infrastructure	Infraestructura
Integrity	Integridad
Interference	Interferencia
ISO/IEC 27001	ISO/IEC 27001
ISO/IEC 27002	ISO/IEC 27002
Key	Clave
Logical access management	Gestión del acceso lógico
Maintenance door	Acceso para mantenimiento
Malware	Códigos fraudulentos (malware)
Managing business assets	Gestión de activos del negocio
Non-disclosure agreement	Acuerdo de confidencialidad
Non-repudiation	No repudio
Risk avoiding	Evitar riesgos
Risk bearing	Asumir riesgos
Risk neutral	Riesgo neutro
Patch	Parche
Personal data protection legislation	Legislación sobre la protección de datos personales
Personal firewall	Cortafuegos personal
Phishing	Phishing
Precision	Precisión
Preventive	Preventivas
Priority	Prioridad
Privacy	Privacidad
Production factor	Factor de producción
Public Key Infrastructure (PKI)	Infraestructura de claves públicas
Public records legislation	Legislación sobre registros públicos
Qualitative risk analysis	Análisis de riesgo cualitativo
Quantitative risk analysis	Análisis de riesgo cuantitativo
Reductive	Reduccionistas

Redundancy	Redundancia
Reliability of information	Fiabilidad de la información
Repressive	Represivas
Risk	Riesgo
Risk analysis	Análisis de riesgo
Risk assessment (Dependency & Vulnerability analysis)	Evaluación de riesgos (Análisis de dependencia y vulnerabilidad)
Risk management	Gestión de riesgos
Risk strategy	Estrategia en materia de riesgos
Robustness	Robustez
Rootkit	Rootkit (Kit de Hacking)
Secret authentication information	Información de autenticación autentificación secreta
Security event	Evento de seguridad
Security in development	Seguridad en desarrollo
Security incident	Incidente de seguridad
Security measure	Medida de seguridad
Security Organization	Organización de la seguridad
Security Policy	Política de seguridad
Security regulations for the government	Normas de seguridad para el gobierno
Segregation of duties	Segregación de funciones
Social engineering	Ingeniería social
Spam	Correo basura (spam)
Spyware	Programa espía (spyware)
Stand-by arrangement	Medidas en espera (stand by)
Storage medium	Medio de almacenamiento
System acceptance testing	Prueba de aceptación del sistema
Threat	Amenaza
Timeliness	Oportunidad
Trojan	Troyano
Uninterruptible Power Supply (UPS)	Sistema de Alimentación Ininterrumpida
Urgency	Urgencia
User access provisioning	Provisión de acceso a usuarios
Validation	Validación
Verification	Verificación
Virtual Private Network (VPN)	Red Privada Virtual
Virus	Virus
Vulnerability	Vulnerabilidad
Worm	Gusano informático

4. Bibliografía

Literatura para el examen

A. Hintzbergen, J., Hintzbergen, K., Smulders, A. y Baars, H.
Foundations of Information Security – Based on ISO 27001 and ISO 27002
Van Haren Publishing, 3ª edición, 2015
ISBN 978 94 018 0012 9
eBook 978 94 018 0541 4

Matriz bibliográfica

Requisito del examen	Especificación del examen	Literatura
1 Información y seguridad		
	1.1 El concepto de información	Capítulo 3
	1.2 Valor de la información	Capítulo 3 y 4
	1.3 Aspectos de fiabilidad	Capítulo 3 y 4
2 Amenazas y riesgos		
	2.1 Amenaza y riesgos	Capítulo 3
	2.2 Relaciones entre amenazas, riesgos y la fiabilidad de la información.	Capítulo 3 y 11
3 Enfoque y Organización		
	3.1 Política de seguridad y organización de la protección	Capítulo 3, 5 y 6
	3.2 Componentes	Capítulo 6, 7, 8 y 13
	3.3 Gestión de incidentes	Capítulo 3, 15 y 16
4 Medidas		
	4.1 Importancia de las medidas de seguridad	Capítulo 3, 8 y 16
	4.2 Medidas físicas de seguridad	Capítulo 3 y 11
	4.3 Medidas técnicas	Capítulo 6, 11 y 12
	4.4 Medidas organizativas	Capítulo 3, 6, 9, 17 y 18
5 Legislación y normas		
	5.1 Legislación y normas	Capítulo 18

Contacto EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER