

TC2027 Seguridad Informática

Prof. Jeann José Frias Garza

Módulo 1

Introducción y conceptos básicos

Temas y subtemas del curso

1. Introducción y conceptos básicos.

1.1 ¿Por qué necesitamos seguridad informática?.

1.2 Metas de la seguridad informática: integridad, disponibilidad y confidencialidad.

1.3 Responsabilidades éticas y legales.

1.4 Panorama organizacional de la seguridad informática.

1.5 Panorama tecnológico de la seguridad informática.

1.6 Aspectos legales de la seguridad informática.

1.7 Los orígenes de inseguridad: definición, implantación, operación.

1.8 Certificaciones a nivel individuo: CompTIA/Security+, ISC2/CISSP, SANS/GIAC, ISACA/CISA y otros.

1.9 Certificaciones a nivel sistema: Orange Book, ITSEC, Common Criteria y otros.

1.10 Certificaciones a nivel organización: ISO/IEC 27001, BS7799, NIST 800-12 y otros.

1.6 Aspectos legales de la seguridad informática.

1.6 Describir los derechos y deberes de los profesionales y organizaciones de tecnologías de información con la sociedad y el estado para garantizar la seguridad informática.

1.6 Aspectos legales de la seguridad informática.

- Licenciamiento - derecho de uso y no la propiedad (Ej. SW)
- Leyes de Propiedad Intelectual para la protección de artículos (items) tangibles e intangibles y la propiedad
 - Propiedad industrial (invenciones - patentes, marcas registradas, diseños industriales, etc).
 - Derechos de autor (Copyright) - Literatura, trabajo artístico, esculturas, pinturas, etc.
- Reglas de importación y exportación (información, tecnología y productos) - Ejemplo Restricciones fuera de USA
- Regulaciones para flujo de datos transfronterizos (Cross Border data transfer)
- Privacidad
 - Brechas de seguridad de datos (Notificar sobre la divulgación no autorizada de datos)
- BSA - Business Software Alliance
- Siempre busquen consejo legal de expertos, usted debe tener nociones básicas y generales.

Regulaciones

Nombre	Descripción	Nombre	Descripción
PCI-DSS Payment Card Industry - Data Security Standard	Industria de tarjetas de pago Requerimientos y procedimientos de evaluación de seguridad	Federal Information Security Management Act (FISMA)	USA - Información sensitiva y vital - Gobierno
Ley federal de protección de datos personales en posesión de los particulares	Privacidad	EU General Data Protection Regulation (GDPR)	Unión Europea - Regulación de protección de privacidad de datos
HIPAA (Health Insurance Portability and Accountability Act)	Legislación para la privacidad de datos y seguridad para proteger la información médica.	Gramm-Leach-Bliley Act (GLBA)	Manejo de Información crediticia o financiera

1.7 Los orígenes de inseguridad: definición, implantación, operación.

1.7 Identificar los tres niveles en los que se gestan las inseguridades en una infraestructura informática.

Orígenes de la inseguridad

Definición	Implantación	Operación
<ul style="list-style-type: none">● Estrategia● Arquitectura - Diseño	<ul style="list-style-type: none">● Proyectos● Construcción● Pruebas	<ul style="list-style-type: none">● Uso● Monitoreo
<ul style="list-style-type: none">● No considerar el factor humano, cultural y de comportamiento● Sin compromiso de la alta dirección● No contar con personal de seguridad dedicado	<ul style="list-style-type: none">● Incidentes por el proceso de transición (instalación y configuración)● No realizar pruebas de seguridad (hackeo ético o penetración)	<ul style="list-style-type: none">● Realizar monitoreo en tiempo real● Pérdida de datos● No instalar parches de seguridad (vulnerabilidades)● No hacer respaldos
Personas, Procesos y Tecnología		

1.8 Certificaciones a nivel individuo: CompTIA/Security+, ISC2/CISSP, SANS/GIAC, ISACA/CISA y otros.

1.8 Describir el propósito, las metas y los procesos de certificación en seguridad informática para profesionales de Tecnologías de Información, listando los más conocidos.

Certificaciones para personas

Propósito


- Ayuda a validar o acreditar el conocimiento y/o experiencia y/o competencias de las personas en un tema en particular.

Utilizadas por las personas y las organizaciones para **desarrollar** planes de carrera o para selección y reclutamiento.

Procesos típicos

- Aplicar un examen evaluando conocimientos o experiencia
 - Opción múltiple
 - Con escenarios o contexto
- Validando la experiencia de forma documental (descripciones y evidencia)
 - Enviar Título Profesional
 - Enviar otras certificaciones
 - Describir actividades y/o entregables

**Certificaciones de Seguridad de la Información o
Seguridad Informática - Personas**

Nivel	Especializadas - Técnicas	Administrativas - Gerenciales
Básico	CompTIA / Security+ 	
Intermedio	eCouncil / CEH  SANS / GIAC 	ISACA / CISA  CISA Certified Information Systems Auditor® <small>An ISACA® Certification</small>
Avanzado	ISC2 / CISSP  Certified Information Systems Security Professional	ISACA / CISM  CISM Certified Information Security Manager® <small>An ISACA® Certification</small>

1.9 Certificaciones a nivel sistema: Orange Book, ITSEC, Common Criteria y otros.

1.9 Describir el propósito, las metas y los procesos de certificación en seguridad informática para procesos y sistemas de Tecnologías de Información, listando los más conocidos.

Certificaciones de Seguridad de la Información o
Seguridad Informática - **Sistemas**

Certificación	Descripción	Referencia
Orange Book	Trusted Computer System Evaluation Criteria (TCSEC)	http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt http://searchsecurity.techtarget.com/answer/Is-the-Orange-Book-still-relevant-for-assessing-security-controls
ITSEC	Information Technology Security Evaluation Criteria (ITSEC) criterios para evaluar la seguridad en productos y sistemas.	https://en.wikipedia.org/wiki/ITSEC
Common Criteria	Provee requerimientos para seguridad en productos y medidas de aseguramiento para evaluaciones de seguridad.	https://www.commoncriteriaportal.org/ https://www.commoncriteriaportal.org/cc/

Certificaciones a nivel sistema

Actividad en equipo- Crear una tabla comparativa de los criterios y métodos para evaluación de seguridad en productos (Certificación a nivel sistema)

IT SEC - TCSEC - CC (Common Criteria)

Solicitar el formato al profesor para su llenado y crear una copia.

Common criteria

Ejercicio:

Buscar Red Hat Enterprise Linux Version 7.1 en:

Sistemas Operativos

<http://www.commoncriteriaportal.org/products/>

Ver el Reporte de Certificado

Diferencia entre Certificación y Acreditación

Certificación	Acreditación
<p>Evaluación técnica integral de las componentes de seguridad y su cumplimiento con el propósito de ser acreditado.</p> <ul style="list-style-type: none">• El proceso de certificación puede utilizar evaluación de protección (safeguard), análisis de riesgos, verificación, pruebas y técnicas de auditoría para evaluar qué tan apropiado es un sistema específico.• La meta del proceso de certificación es asegurar que el sistema, producto o red es correcto para los propósitos del cliente. <p>Es una revisión técnica que evalúa los mecanismos de seguridad y su efectividad</p>	<p>Es la aceptación formal de que tan adecuada es la seguridad y funcionalidad general de un sistema.</p> <p>Es la aceptación oficial de la gerencia de la información sobre los hallazgos encontrados durante el proceso de certificación.</p>

1.10 Certificaciones a nivel organización: ISO/IEC 27001, BS7799, NIST 800-12 y otros.

1.10 Describir el propósito, las metas y los procesos de certificación en seguridad informática para organizaciones, listando los más conocidos.

**Certificaciones de Seguridad de la Información o
Seguridad Informática - Organización**

Estándar	Descripción	Referencia
ISO/IEC 27001	Estándar que provee requerimientos para un sistema de gestión de seguridad de la información - (<u>SGSI</u>)	https://www.iso.org/isoiec-27001-information-security.html
BS7799 / ISO 17799 / ISO 27002	Técnicas de seguridad - código de práctica para controles de seguridad de la información	https://www.iso.org/standard/54533.html
NIST 800-12	Introducción a la seguridad de la información. Panorama de alto nivel a los principios de la seguridad de la información, conceptos relacionados y familias de controles de seguridad.	http://csrc.nist.gov/publications/PubsSPs.html#SP-800-12-Rev-1

Serie ISO 27000

27001	<u>Sistema de gestión</u> de la seguridad de la información
27002	<u>Código de prácticas para controles de seguridad de la información</u>
27005	Gestión de <u>riesgos</u> de seguridad de la información
27017	Código de prácticas para controles de seguridad de la información para servicios en la nube (<u>Cloud</u>)

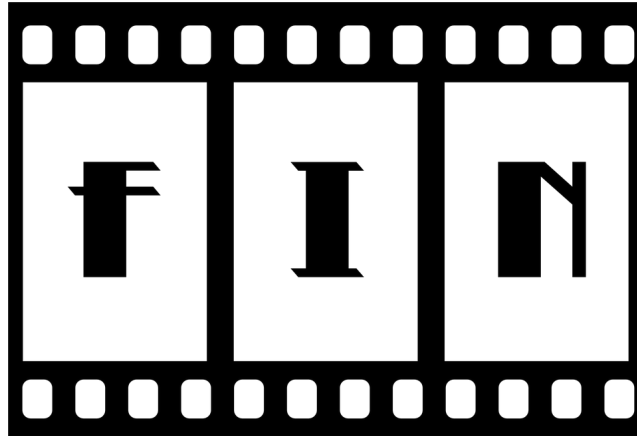
ISO 27002 - Código prácticas - Controles



ISO 27002:2013

- Políticas de seguridad de la información
- Organización de seguridad de la información
- Seguridad en recurso humano
- Administración de activos
- Criptografía
- Seguridad física y ambiental
- Seguridad en las operaciones
- Seguridad en comunicaciones
- Mantenimiento, desarrollo y adquisiciones de sistemas
- Relaciones con proveedores
- Administración de incidentes de seguridad de la información
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio
- Cumpimiento

Fin de módulo



Objetivos específicos de aprendizaje por tema: 1. Introducción y conceptos básicos.

1.1 Plantear las metas, alcances y limitaciones de la seguridad informática como una metodología, conjunto de recursos y patrón de comportamiento para garantizar la persistencia de la información y la perdurabilidad de las organizaciones.

1.2 Definir qué son las tres aristas del triángulo de seguridad y establecer el nivel óptimo para los diferentes tipos de organizaciones.

1.3 Explicar el porqué de un código de ética que rija el desempeño de profesionales en seguridad informática.

1.4 Definir los elementos a nivel organizacional para garantizar la seguridad informática.

1.5 Definir los elementos a nivel tecnológico para garantizar la seguridad informática.

Objetivos específicos de aprendizaje por tema: 1. Introducción y conceptos básicos.

1.6 Describir los derechos y deberes de los profesionales y organizaciones de tecnologías de información con la sociedad y el estado para garantizar la seguridad informática.

1.7 Identificar los tres niveles en los que se gestan las inseguridades en una infraestructura informática.

1.8 Describir el propósito, las metas y los procesos de certificación en seguridad informática para profesionales de Tecnologías de Información, listando los más conocidos.

1.9 Describir el propósito, las metas y los procesos de certificación en seguridad informática para procesos y sistemas de Tecnologías de Información, listando los más conocidos.

1.10 Describir el propósito, las metas y los procesos de certificación en seguridad informática para organizaciones, listando los más conocidos.

Blockchain y seguridad

¿Qué es blockchain?

Descargar (↓) y almacenar en Gdrive ISACA Tech Brief:
Blockchain Basics (free)
<http://www.isaca.org/COBIT/Pages/DownloadProduct.aspx?pc=WBCBB>

Casos de uso

- Transacciones
- Documentos de identidad (acta de nacimiento)
- Títulos de propiedad (Terrenos, casas)
- Crypto monedas (dinero)
- Votos

¿Cuál es la relación de blockchain con la seguridad y por tanto la materia?

Existen riesgos de seguridad en múltiples niveles y áreas específicas como:

- Control de acceso y seguridad a los activos de información
- Fortaleza de los algoritmos de encriptación y funciones hash
- Seguridad de los nodos de blockchain en la red
- Ataques de negación de servicio (DoS o DDoS)