Tecnológico de Monterrey

TC2027 Seguridad Informática

Prof. Jeann José Frias Garza

Tecnológico de Monterrey

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.

1.1 ¿Por qué necesitamos seguridad informática?

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.

Valor de la información

Tecnológico de Monterrey

¿Cuál es el valor del activo?	Valor	Bien	Se puede copiar	Precio (Afectado por)	Protección
Oro	?	Tangible	No (No se puede clonar)	Variable (Mercado)	Banco
Billete de 500 pesos	?	Tangible	No (Falsificación)	Fijo (Inflación)	Banco
Marca	?	Intangible	Si (Piratería)	Variable (Reputación)	Leyes y regulaciones
SW	?	Intangible	Si (Piratería)	Variable (Mercado)	Leyes y regulaciones + ?
De la información	?	Intangible	Si	Variable (Mercado)	**?**

Valor de la información

¿Cuál será la información más valiosa?

- Datos personales (Nombre, dirección, Localización, etc)
- Datos de tarjetas de crédito (Nombre, Número Tarjeta, Vigencia, CVV)
- Datos financieros (Saldos y transacciones)
- Datos de preferencias (mercadotecnia)

¿Seguridad informática?

Tecnológico de Monterrey

Responsabilidades

- Proteger los activos de Información en medios electrónicos (se puede extender a medios no electrónicos)
- Tecnología, procesos y recursos humanos
- Leyes y regulaciones (Datos personales o seguridad de la información)

Incidentes

- Pérdida de información
- Modificación de información
- No disponibilidad de la información

Ejemplos

- Admite Movimiento Ciudadano haber entregado a Amazon el padrón electoral
  - http://www.jornada.unam.mx/2016/04/28/politica/007n1pol
  - https://www.databreaches.net/personal-info-of-93-4-million-mexicans-exposed-on-amazon/

Ejercicio

- Investigar 1 noticias por equipo sobre brechas de seguridad en México en los últimos 3 años
- Comentar con el grupo, no se puede repetir

Actividad - Estado de la seguridad informática

Reporte

State of Cyber Security 2017 - ISACA (⇓)

Descargar y almacenar los documentos

https://cybersecurity.isaca.org/state-of-cybersecurity#3-part-1-february

https://cybersecurity.isaca.org/state-of-cybersecurity#0-part-2-june

Utilizando la información de los documentos responda lo siguiente en un documento de **Gdrive** (Crear y compartir una carpeta con los compañeros y el profesor):

Parte 1.

- ¿Cómo podemos explicar la dificultad para cubrir vacantes de seguridad de la información?

Parte2.

- ¿Cuáles son los principales tipos de ataques?. Explique brevemente cada uno
- Explique las amenazas al cómputo móvil y al Internet de las cosas.

Incluir las referencias

Blockchain y seguridad

Tecnológico de Monterrey

¿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

Actividad - Seguridad y Blockchain

Tecnológico de Monterrey

En un documento de Gdrive

- ¿Cuáles son los retos de seguridad y privacidad para el Blockchain?

- Buscar 2 noticias de brechas de seguridad para Blockchain / Bitcoins y redactar lo siguiente:
  - Resumen del caso (3 a 5 párrafos)
  - Monto de la pérdida (en Dlls)
  - Fecha de la brecha
  - Fecha de la noticia
  - Referencia

Seguridad informática

Metas	Alcance	Limitaciones
● Proteger la información (Confidencialidad, Integridad y Disponibilidad)	● Información en medios electrónicos ● En uso, almacenamiento y transportación ● Considerar aspectos de personas, procesos y tecnología Nota: La seguridad de la información incluye la que no está en medios electrónicos (física, ondas sonoras)	● Falta de concientización de las personas sobre la importancia (Personas son el eslabón más débil) ● Falta de compromiso de la alta dirección ● Debilidades inherentes a la información y medios para almacenar y transportar

Metodología (procesos), conjunto de recursos (humanos, materiales - tecnológicos, financieros) y patrón de comportamiento para garantizar la persistencia de la información y la perdurabilidad de las organizaciones.

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

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

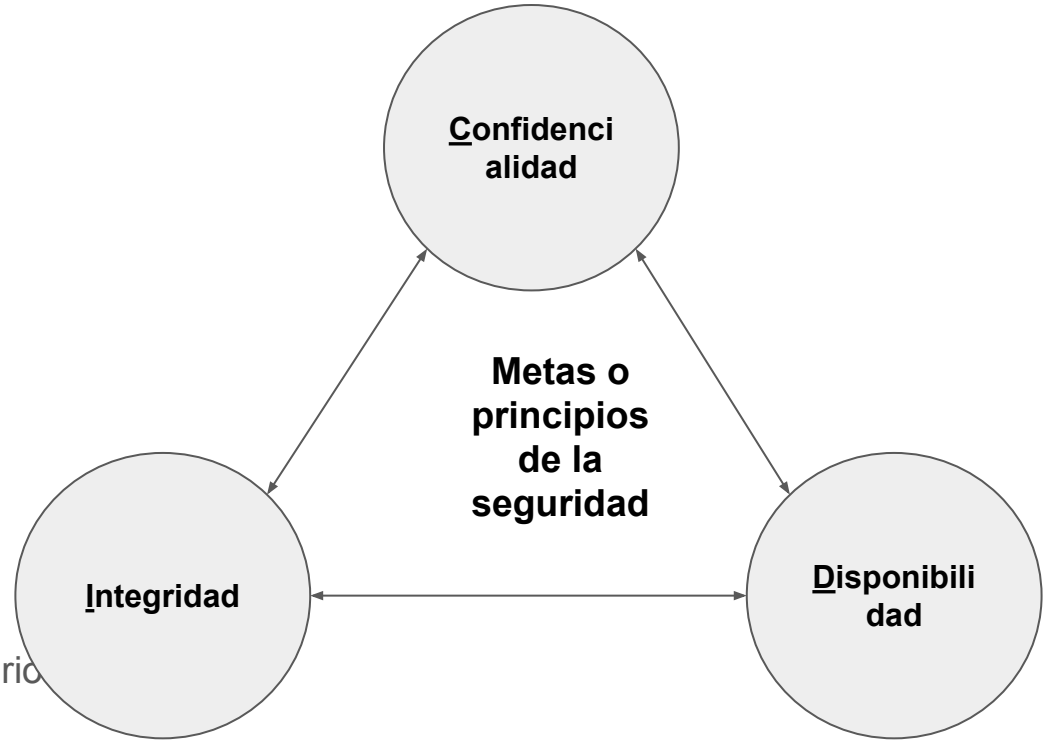
Principios

Objetivo: Garantizar un nivel óptimo de las 3 metas

Confidencialidad - "Propiedad de la información para que no esté disponible o sea divulgada a individuos, entidades o procesos no autorizados"

Integridad - “Mantener y asegurar la precisión y completitud de los datos en su ciclo de vida, es decir que los datos no pueden ser modificados de una forma no autorizada”

Disponibilidad - “La información esté disponible o accesible cuando sea necesario



Official (ISC)2 Guide to the CISSP CBK, Fourth Edition, Adam Gordon

Conceptos adicionales

Identificación. “Es una afirmación de quién es o qué es algo”

Autenticación. “Verificar la identidad”

- Lo que sabes: Password
- Lo que tienes: Token, tarjeta magnética
- Lo que eres: Biométricos

MFA - Multi Factor Authentication

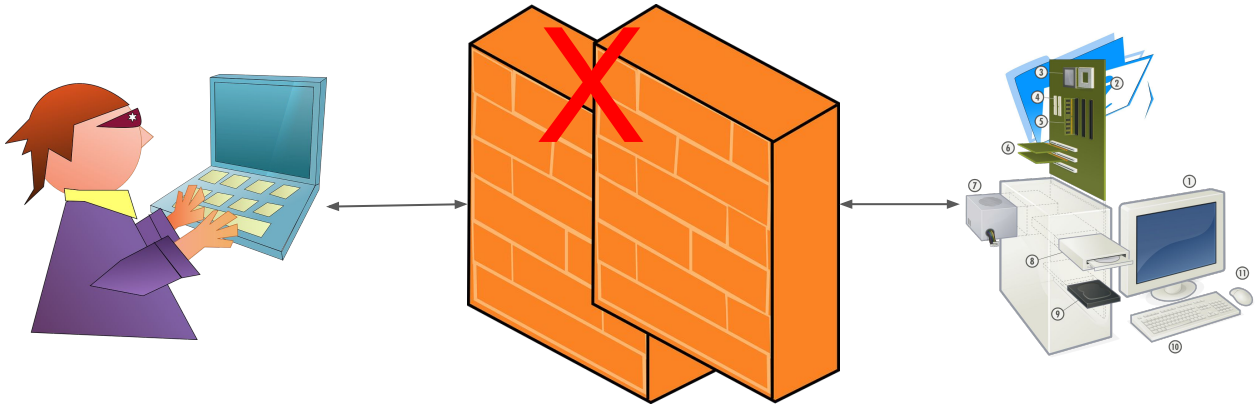
Autorización. Una vez identificado y autenticado, se debe determinar que recursos de información tienes permiso de acceder y qué acciones puedes ejecutar

No - repudiación. “Implica que un parte de una transacción no puede negar haber recibido la transacción ni la otra parte negar el envío de la transacción”

Official (ISC)2 Guide to the CISSP CBK, Fourth Edition, Adam Gordon

Conceptos adicionales

- Activo - Valor
- Amenaza
- Vulnerabilidad
  - Personas
  - Procesos
  - Tecnología



Conceptos adicionales

Clasificación de la información

Ejemplo:

- **P**ública
- **I**nterna
- **C**onfidencial

Ejercicio de clasificación para información personal:

1. Estados de cuenta bancarios ( )
2. Número de teléfono celular ( )
3. Fotos ( )
4. C.V. ( )
5. Domicilio ( )

1.3 Responsabilidades éticas y legales.

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

http://www.acm.org/about-acm/code-of-ethics

http://ethics.acm.org/code-of-ethics

https://www.isc2.org/ethics/default.aspx

http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx

http://www.issa.org/?page=CodeofEthics

Código ética

(ISC)² Code Of Ethics

Code

All information security professionals who are certified by (ISC)² recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all (ISC)² members are required to commit to fully support this Code of Ethics (the "Code"). (ISC)² members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification. (ISC)² members are obligated to follow the ethics complaint procedure upon observing any action by an (ISC)² member that breach the Code. Failure to do so may be considered a breach of the Code pursuant to Canon IV.

There are only four mandatory canons in the Code. By necessity, such high-level guidance is not intended to be a substitute for the ethical judgment of the professional.

Code of Ethics Preamble:

- The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

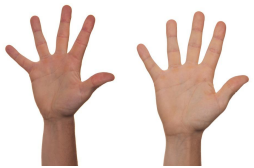
- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principles.
- Advance and protect the profession.

https://www.isc2.org/ethics/default.aspx

1.3 Responsabilidades éticas y legales.

Ejercicio

¿Porqué tener un código de ética que rija el desempeño de profesionales en seguridad informática?



¿Cómo nos aplica como profesionales?

¿Cómo lo aplicamos para el reto?

1.4 Panorama organizacional de la seguridad informática.

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

1.4 Panorama organizacional de la seguridad informática.

- **Gobierno y Gestión**
  - **Estructuras - Organigrama (Puestos y roles)**
  - **Personas y competencias**
  - **Buenas prácticas**
  - **Procesos, procedimientos y políticas**

https://www.sfia-online.org/en/sfia-6/skills/strategy-architecture/information-strategy/information-security

1.4 Panorama organizacional de la seguridad informática.

Estructuras

- Definir puestos y roles:
  - CISO, CSO - Oficial de Seguridad de la Información
  - Oficial de privacidad
  - Administradores de Seguridad

Personas y competencias

- Definir competencias (SFIA)
- Programas de comunicación y concientización

Buenas prácticas

- Seleccionar, implementar y mantener buenas prácticas, estándares y marcos de referencia de gestión de riesgos, seguridad informática y seguridad de la información

Procesos

- Implementar procesos, políticas y procedimientos para el Sistema de gestión de Seguridad de la Información

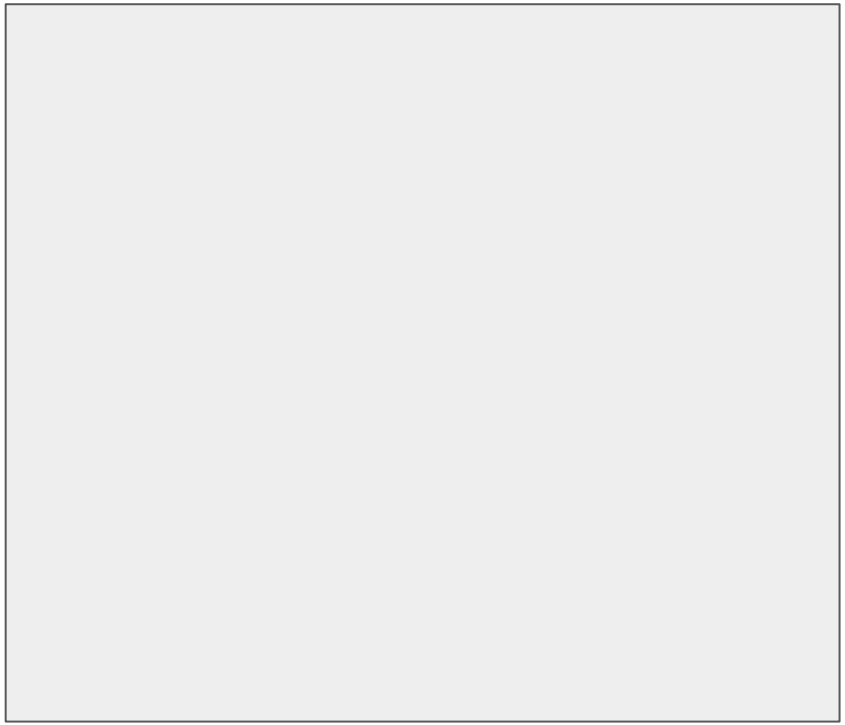
https://www.sfia-online.org/en/sfia-6/skills/strategy-architecture/information-strategy/information-security

1.4 Panorama organizacional de la seguridad informática.

Estructuras - Organigrama (Puestos y roles)

Ejercicio:

- Crear un organigrama para las siguientes posiciones dentro del área de seguridad de la información y/o informática
  - CISO, CSO - Oficial de Seguridad de la Información
  - Oficial de privacidad
  - Administradores de Seguridad
- ¿Qué otras posiciones existirán?
  - En el área de TI: Infraestructura o soporte técnico, desarrollo de sistemas, etc.
  - En las áreas de Negocio, riesgos o legales.



1.4 Panorama organizacional de la seguridad informática.

Personas y competencias

- Definir competencias (SFIA)
  - Gerencial
  - Tecnológico

- Programas de comunicación y concientización
  - Ingeniería social
  - Clean o clear desk
  - Security day

Ejercicio

Comentar sobre las competencias del SFIA

https://www.sfia-online.org/en/sfia-6/skills/strategy-architecture/information-strategy/information-security

https://www.sfia-online.org/en/sfia-6/skills/service-management/service-operation/security-administration

1.4 Panorama organizacional de la seguridad informática.

Buenas prácticas

- ISO 27000
- (ISC)² Common Body of Knowledge (CBK)
- NIST CYBERSECURITY FRAMEWORK

Procesos

- Política
  - De seguridad
  - Uso de contraseñas
  - Escritorio limpio (Clean or clear desk)
  - etc.

https://www.sfia-online.org/en/sfia-6/skills/strategy-architecture/information-strategy/information-security

https://www.sfia-online.org/en/sfia-6/skills/service-management/service-operation/security-administration

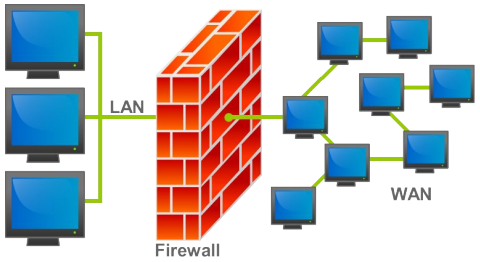
1.5 Panorama tecnológico de la seguridad informática.

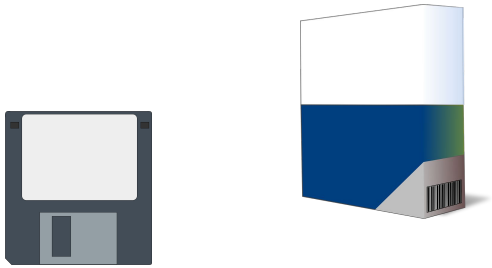
1.5 Definir los elementos a nivel tecnológico para garantizar la seguridad informática.

1.5 Panorama tecnológico de la seguridad informática.

Ejemplos de componentes tecnológicos

- Seguridad en redes: VPN, Firewalls, IDS, IPS
- Encripción (Librerías, HW)
- Hackeo ético, pruebas de penetración o vulnerabilidades
- Respaldos y manejo de medios
- WAF y DLP
- Control de acceso (Servidores, SO, móvil
- Administración de identidades (LDAP)
- SW Control de acceso y bitácoras
- SW Hardening de servidores





1.5 Panorama tecnológico de la seguridad informática.

Proveedores de soluciones

https://www-03.ibm.com/security/mx/es/products/?lnk=mpr_buse_mxes&lnk2=learn

https://www.checkpoint.com/

https://www.forcepoint.com/es

https://www.symantec.com/es/mx

https://aws.amazon.com/es/products/?nc2=h_ql_ny_livestream_blu

Ejercicio:

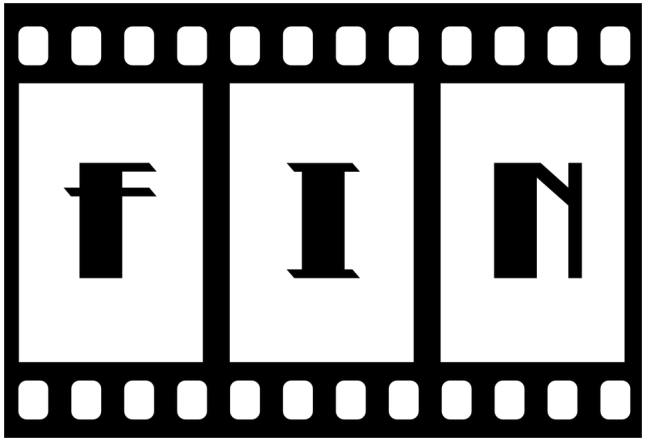
Buscar 1 proveedor de soluciones de seguridad para cada uno de los siguientes:

- CASB
- IDS/IPS
- SW (librerías para encripción)

Nota: No repetir los mostrados

Fin de módulo

Tecnológico de Monterrey



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

Tecnológico de Monterrey

¿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 encripción y funciones hash
- Seguridad de los nodos de blockchain en la red
- Ataques de negación de servicio (DoS o DDoS)