**SEGURIDAD COMO PROFESIÓN**

**Cuestiones legales**

* Asuntos legales personales: nuestra manera de manejar la información
* Asuntos legales corporativos: leyes, políticas de privacidad y repercute con multas y hasta condenas
* Derecho internacional y ciberseguridad: países donde se implementan medidas legales para mejorar la seguridad

**Cuestiones éticas**

* Asuntos éticos personales: la mentalidad de nosotros como personas, no porque no exista una ley debo cometer actos ilegales
* Asuntos éticos corporativos: cuestiones legales

La ciberseguridad es una profesión crucial para la era digital actual donde las amenazas cibernéticas y los ataques informáticos son cada vez más sofisticados y frecuentes.

Los profesionales de la ciberseguridad son responsables de proteger los sistemas, redes, datos y recursos digitales de individuos, empresas y organizaciones contra posibles amenazas y ataques cibernéticos.

Dentro del área de ciberseguridad, así como en la informática, existen áreas de desempeño en lo que se puede especializar como:

* ANALISTA DE SEGURIDAD
* INGENIERO (A) DE SEGURIDAD
* PENETRATION TESTER
* ANALISTA DE INCIDENTES DE SEGURIDAD: investigar sobre alguna violación de seguridad
* ARQUITECTO DE SEGURIDAD: diseña una infraestructura de seguridad de acuerdo a la triada
* ESPECIALISTA FORENSE: recupera evidencia relacionado a seguridad
* GESTOR(A) DE SEGURIDAD:
* CONSULTOR(A) DE SEGURIDAD

Para convertirse en un profesional de ciberseguridad, se requiere un solido conocimiento de sistemas informáticos, redes, programación, criptografía, amenazas cibernéticas, configuración de servidores, entro otros. Muchos profesionales en este campo obtienen certificaciones relevantes.

Algunas certificaciones que son relevantes dentro del campo de la ciberseguridad son:

* CISSP
* CISM
* CEH
* CompTIA Security+
* CCSP

Consecuencias:

* Reputación dañada
* Vandalismo
* Robo
* Pérdida de ingresos

Los atacantes son personas o grupos que intentan aprovechar vulnerabilidades para obtener una gran ganancia personal o financiera.

Amenazas internas y externas

Ciber atacantes: personas externas – atacantes organizados, hackers, aficionados.

Personas internas

La tendencia de ataques, aunque haya disminuido, siempre existe el riesgo en aumenta tanto para dispositivos móviles como en personas. Como sabemos los accesorios comienzan a conectarse a internet (IOT) como los smartwatchs, bocinas inteligentes, entre otros, y poco a poco estos dispositivos también forman parte de los objetivos que ciberdelincuentes intentan atacar.

Otros datos relevantes sobre la relevancia de ser un profesionista en ciberseguridad son:

Dos tercios (67%) de los profesionales TI creen que el mal uso de dispositivos en sus organizaciones creció de alguna u otra forma.

Los ataques “next gen” a la cadena de suministros aumentaron 420% durante todo el año 2020.

63% de las intrusiones maliciosas en redes son resultado de datos de autenticación (nombres de usuario y contraseña) que han sido comprometidos en otros ciberataques. (Microsfoft).

**Normatividad**

Las normas son documentos técnicos legales que son establecidas por una organización o por una autoridad reconocida con el fin de estandarizar y regular aspectos específicos de la actividad humana. Estas reglas buscan establecer un marco de referencia común que garantice la uniformidad, calidad, seguridad y la interoperabilidad en diversos campos, desde la tecnología y la industria, hasta salud, medio ambiente y más.

Cuentan con las siguientes características:

Contienen especificaciones técnicas de aplicación voluntaria

Son elaborados por consenso de las partes interesadas:

* Fabricantes
* Administraciones
* Usuarios y consumidores
* Centros de investigación y laboratorios
* Asociaciones y colegios profesionales

En la normativa en México relacionado a la ciberseguridad podemos encontrar:

NMX-I-27001NYCE: sistema de gestión de la ciberseguridad de la información (SGCI) parte 1 y 2.

NMX-I-1337-NYC: ciberseguridad – directrices para la gestión de ciberseguridad en el sector energético parte 1 y 2.

**Norma:**

Es una especificación reglamentaria para conseguir un grado optimo en la calidad. Estas se elaboran por instituciones que, a base de la experiencia y desarrollo tecnológico, son aprobadas por consenso.

**Estándar:**

Son normas aprobadas redactadas establecidas para garantizar el acoplamiento de elementos que se construyen de forma independiente, con la finalidad de garantizar un repuesto en caso de ser necesario.

Principales organizaciones de normalización y estandarización:

**Código penal federal**

El código penal federal en México es el conjunto de leyes que establecen los delitos y las acciones penales que se aplican a nivel federal en el país. Establece las normas legales que rigen el sistema de justicia penal en casos de infracciones graves que afectan el orden y la seguridad del país.

Algunos artículos relacionados a la seguridad y resguardo de la información incluidos en el código penal federal son:

**Artículo 211 Bis**

**Artículo 284 Bis**

**Artículo 385 Bis**

**Artículo 387 Ter**

**Artículo 210 Ter**

Se refiere al delito de sabotaje informático estableciendo sanciones…

**Articulo 211 Quáter**

Contempla penas para quienes cometan el delito de ataque a la integridad de sistemas informáticos, realizando acciones que se pongan en riesgo la operación segura de sistemas de información.

**Leyes de transparencia y acceso a la información**

En México, la transparencia y el acceso a la información están regulados principalmente por la Ley General de Transparencia y Acceso a la Información Publica y por las leyes de transparencia a nivel estatal. Estas leyes tienen como objetivo garantizar el acceso de los ciudadanos a la información gubernamental y promover la rendición de cuentas por parte de las instituciones públicas.

**Objetivo:**

Promover lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos Constitucionales Autónomos o con autonomía legal y cualquier otra entidad federal.

Promover la transparencia de la gestión pública mediante la difusión de información que general los sujetos obligados; garantizar la protección de los datos personales en posesión de dichos sujetos; favorecer la rendición de cuentas a los ciudadanos, así como manejar la organización y manejo de los documentos.

Entre los aspectos clave de la Ley de Transparencia se encuentran:

* Protección de datos personales
* Principios de transparencia
* Información publica
* Portales de transparencia
* Solicitud de información
* Sujetos obligados

Las leyes de transparencia en México buscan fortalecer la participación ciudadana, el control social y la supervisión de las actividades gubernamentales. Estas leyes promueven la apertura y la responsabilidad de las instituciones públicas, fomentando la confianza y la rendición de cuentas en el gobierno.

**Articulo 63**

**Artículo 64**

**Ley de protección de datos personales en posesión de particulares**

La ley federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), es un cuerpo normativo en México, aprobado por el Congreso de la Unión el 27 de abril de 2010, mismo que tiene como objetivo regular el derecho a la autodeterminación informativa.

Esta ley fue publicada el 5 de julio de 2010 en el Diario Oficial de la Federación y entro en vigor el 6 de julio de 2010. Sus disposiciones son apreciables a todas las personas físicas o morales, del sector publico o privado, tanto a nivel federal como estatal.

**Objetivo:**

* Regular la forma en que deben usarse los datos personales de personas físicas y morales en el ámbito privado.
* Proteger a las personas con relación con el tratamiento de su información.
* Garantizar que los individuos puedan ejercer el derecho a decidir sobre el uso de sus datos.
* Establece el aviso de privacidad.

Tipos de datos

**DATO PERSONAL:**

* Cualquier información concerniente a una persona física identificada o identificable. Consentimiento: expresivo verbalmente, escrito, medio electrónico, óptico u otra tecnología.
* Consentimiento: táctico si el titular no manifiesta oposición.

**DATO PERSONAL SENSIBLE:**

* Datos personales que afectan a esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve a un riesgo grave.

Ejemplo:

* Origen racial o étnico
* Estado de salud presente y futuro
* Información genética
* Creencias religiosas, filosóficas y morales
* Afiliación sindical
* Opiniones políticas
* Preferencia sexual

Consentimiento: expresivo y por escrito, firma autógrafa, electrónica o cualquier mecanismo de autenticación.

**MODELOS DE SEGURIDAD**

Un modelo de seguridad informática es un esquema para especificar y forzar políticas de seguridad.

Existen mecanismos para prevenir el acceso ilegal o no deseado, la interferencia o no intencional con la operación adecuada y prevista, o el acceso inadecuado a la información confidencial en sistemas de automatización y control industrial. La seguridad electrónica incluye computadoras, redes, sistemas operativos, aplicaciones y otros componentes configurables programables del sistema.

Modelo “Seguridad en Profundidad”, el cual es “Promovido por Microsoft como un conjunto necesario de prácticas para mantener seguro un sistema o una red de sistemas”.

* Datos
* Aplicación
* Host
* Red interna
* Perímetro
* Seguridad física
* Políticas, procedimientos, concientización

**COBIT**

Un marco de referencia que puede ser utilizado en las empresas como guía para integración de las operaciones relacionadas con el área de Tecnologías de Información es COBIT (Control Objectives for Information and related Technology).

Cuenta con 34 procesos que cubren 2010 objetivos de control:

* Planificación y Organización
* Adquisición e Implantación
* Entrega y Soporte
* Supervisión y evaluación

En sus diferentes versiones, la más reciente (COBIT 5 for information security), considera algunos procesos que brindan una guía básica para definir, operar y monitorear un sistema para gestión de la seguridad, como son:

* APO13
* DSS04
* DSS05

**NIST**

Es una agencia de la administración de tecnología del departamento de comercio de los Estados Unidos.

Propósito: promover la innovación y la competencia industrial en metrología, normas y tecnología para estabilidad económica y la calidad de vida.

Objetivos:

1. priorización y definición de alcance
2. Organización
3. Crear una perta actual
4. Ejecutar un análisis de riesgos
5. Crear una perta objetivo
6. Determinar analizar y priorizar las brechas detectadas
7. Implementar el plan de acción

**ISACA**

Asociación de Auditoria y Control de Sistemas de Información (ISACA es el acrónimo de Information Systems Audit and Control Association).

ISACA surgió en 1967 de un reducido grupo de personas con trabajos similares de auditoria de controles en sistemas informáticos que se estaban haciendo más críticos para las operaciones de sus organizaciones.

Objetivos:

* Promover la educación y la mejora de conocimientos y habilidades de sus miembros en las disciplinas de la auditoria, el aseguramiento, el control y la seguridad de los sistemas de información.
* Incentivar el intercambio fluido de información, así como de estándares, investigaciones y enfoques aplicables a estas disciplinas.
* Realizar presentaciones periódicas sobre estos tópicos.
* Establecerse como un líder de opinión en la comunidad profesional y académica sobre el gobierno de TI como una disciplina profesional que ayuda al logro de los objetivos de las empresas.

La importancia de implementar modelos de seguridad es que recapitula la aplicación y uso de las normas y estándares, principalmente la familia 27000.

Aplicar modelos de seguridad permite:

**Estandarización y buenas prácticas:** los modelos de seguridad, como NIST y COBIT, establecen estándares y mejores prácticas reconocidas en la industria. Siguiendo estos buenos modelos, las organizaciones pueden adoptar un enfoque coherente y eficaz para gestionar la seguridad y la tecnología.

**Gestión de incidentes:** estos modelos incluyen pautas para la respuesta a incidentes y la recuperación en caso de problemas de seguridad. Ayudan a las organizaciones a estar preparadas para enfrentar incidentes y minimizar su impacto.

**Mejora de la eficacia:** los modelos de seguridad promueven la eficacia en las operaciones al establecer procesos y controles claros. Esto puede resultar en una mejor gestión de recursos, tiempo y costos.

Gestión de recursos tecnológicos: COBIT se enfoca en la gestión de tecnología y la alineación de las TI con los objetivos del negocio. Ayuda a asegurar que los recursos tecnológicos sean utilizados de manera efectiva para lograr metas organizacionales.

**Mejora continua:** estos modelos fomentan la mejora continua al proporcionar un ciclo de retroalimentación para evaluar, ajustar y optimizar los controles y procesos de seguridad.

**Comunicación y colaboración:**

**OSSTMM**

Metodología abierta de comprobación de la seguridad, es un de los estándares profesionales mas completos y comúnmente utilizados en Auditorias de seguridad para revisar la seguridad de los sistemas desde internet.

Los campos que abarca esta metodología de código abierto son:

**Enfoque Holistico:** la OSSTMM se enfoca en una evaluación de seguridad completa, abarcando aspectos como la infraestructura, procesos, el personal y la tecnología.

**Pruebas basadas en escenarios reales:** la metodología se basa en la simulación de ataques reales y utiliza múltiples escenarios para evaluar la seguridad desde diferentes perspectivas.

**Tres componentes fundamentales:** la OSSTMM se divide en tres componentes principales: requerimientos de seguridad, medidas de seguridad y pruebas de seguridad.

1. **Requerimientos de seguridad:** define las expectativas de seguridad que una organización debe cumplir. Incluye elementos como políticas, estándares y regulaciones.
2. **Medidas de seguridad:** describe los controles de seguridad que una organización tiene en su lugar, como firewalls, sistemas de detección de intrusiones, políticas de acceso, etc.
3. **Pruebas de seguridad:** esta es la parte principal de la metodología y se enfoca en la realización de pruebas de seguridad específicas para evaluar la efectividad de los controles y las medidas de seguridad.

**Flexibilidad y personalización:** la OSSTMM permite adaptarse a diferentes entornos y necesidades organizacionales, lo que facilita su aplicación en una variedad de escenarios.

**Aprendizaje continuo:** la metodología promueve el aprendizaje continuo y la mejora a través de la retroalimentación constante y la revisión de procesos.

**Enfoque en resultados medibles:** la OSSTMM se centra en la obtención de resultados medibles y cuantificables, lo que proporciona a las organizaciones una comprensión clara de su nivel de seguridad.

**OWASP**

Proyecto de código abierto para determinar y combatir causas que hacen un software inseguro.

Una comunidad libre y abierta enfocada a la seguridad de las aplicaciones.

1. Trabajan en crear:
2. Artículos
3. Metodologías
4. Documentación
5. Herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera

|  |
| --- |
| Inyección |
| Autenticación rota |
| Exposición de datos sensibles |
| Entidades externas XML |
| Control de acceso roto |
| Configuraciones incorrectas de seguridad |
| Secuencias de comandos entre sitios (XSS) |
| Deserialización insegura |
| Usar componentes con vulnerabilidades conocidas |
| Registro y monitoreo insuficientes |

Las 10 principales vulnerabilidades de OWASP en 2021 son:

Algunos de los proyectos de OWASP que más popularidad de uso cuentan son:

|  |
| --- |
| OWASP Top Ten |
| Cheat sheet series |
| Web security testing guide |
| Secure coding practices |
| Application security verification standard |
| OWASP development guide |
| API security project |
| Cloud-Native aplication security |
| OWASP amass user guide |
| Security knowledge framework |

Algunos otros proyectos de OWASP importantes son:

* **WebScarab:**

**TIPOS DE SEGURIDAD**

**Seguridad física**

Amenazas de seguridad física: robo, fraude y sabotaje.

Acceso físico: para evitar el acceso físico es necesario implantar mecanismos de prevención y detección.

* **Prevención:** analizador de retina, tarjetas inteligentes, videocámaras, vigilantes jurados.
* **Detección:** cámaras de vigilancia de circuito cerrado, alarmas, sensores.

**Subsistema de la seguridad física**

* Protección exterior (barreras)
* Monitoreo o alarma (dispositivos mecánicos, eléctricos, electrónicos)
* Iluminación de protección
* Seguridad de cierre (cajas fuertes y bóvedas)
* Sistemas de cerradura y llave
* Identificación y control (tarjetas de identificación, control de estaciones de trabajo).
* Sistema de vigilancia (guardias, cámaras, punto único de acceso).
* Programa de sensibilización (encuestas de seguridad).

**Desastres naturales:**

Los desastres naturales pueden causar muy graves consecuencias, algunos desastres a tener en cuenta son:

* Terremotos y vibraciones
* Tormentas eléctricas
* Inundaciones y humedad
* Incendios y humos
* Sobrecalentamientos

**Para exposición ambiental:**

* Paneles de alarmas
* Detectores de agua
* Detectores de humo
* Sistemas de supresión de incendios
* Protectores de voltajes
* SAI-UPS

**Alteraciones del entorno:**

* Electricidad
* La corriente estática
* Ruido eléctrico
* Temperaturas extremas

**Control físico:** protección de la infraestructura, control de intrusos, monitoreo, guardias de seguridad, control ambiental.

**Control técnico:** control de acceso lógico a los activos, dispositivos de seguridad.

**control administrativo:** políticas, estándares, procedimientos y auditorias.

**Seguridad lógica**

**Seguridad legal**