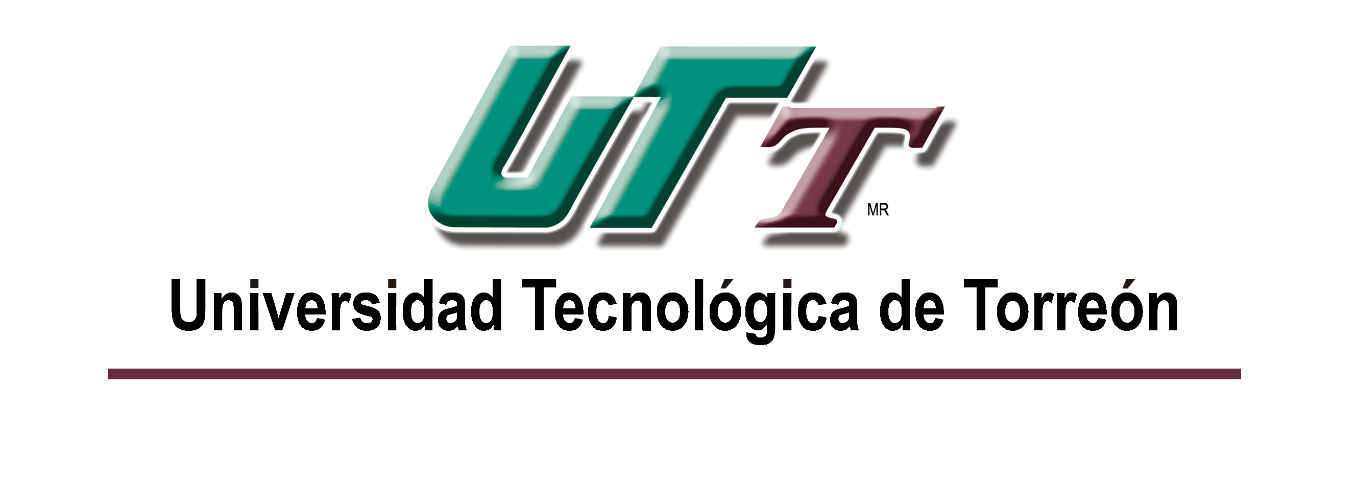
Imagen que contiene Icono

Descripción generada automáticamente

**Gráfico

Descripción generada automáticamente con confianza mediaSEGURIDAD INFORMÁTICA  
UNIDAD I**

Alumnos:

Jesús Arturo Hernández Cristán 22170138

Marco Antonio Chavez Baltierrez 22170149

Abraham Alonso Reynoso González 22170060

ING. Daniel Rosales Díaz Mirón

Carrera: Ingeniería en Desarrollo

y Gestión de Software

Cuatrimestre: 7 Sección: A

Fecha: 02/Septiembre/2024

INDICE

[INTRODUCCIÓN 3](#_Toc176607160)

[SEGURIDAD INFORMÁTICA 4](#_Toc176607161)

[Unidad I – Principios de seguridad informática 4](#_Toc176607162)

[1.1 - Aspectos técnicos y legales del manejo de la información 4](#_Toc176607163)

[1.2 – Estándares del manejo de la información 6](#_Toc176607164)

[1.3 – Conceptos de seguridad 9](#_Toc176607165)

[1.4 – Conceptos de criptografía 9](#_Toc176607166)

[Bibliografía 11](#_Toc176607167)

# INTRODUCCIÓN

En el presente documento, abordaremos el tema de la seguridad informática, un ámbito de crucial importancia en la era digital actual. Dada la creciente relevancia de la información en nuestro entorno tecnológico, es imperativo comprender los fundamentos de su protección.

Este archivo está estructurado para proporcionar una visión integral de los principios de seguridad informática. Comenzaremos analizando los aspectos técnicos y legales relacionados con el manejo de la información. Es fundamental entender que la seguridad informática no solo implica consideraciones tecnológicas, sino también un marco legal ds

Posteriormente, examinaremos los estándares establecidos para el manejo de la información. Estos estándares constituyen las directrices y mejores prácticas que rigen nuestra aproximación a la seguridad de los datos.

A continuación, profundizaremos en los conceptos fundamentales de seguridad. Esta sección nos permitirá identificar las amenazas potenciales y las estrategias de protección necesarias en el entorno digital.

Finalizaremos con una introducción a los conceptos de criptografía, una herramienta esencial en nuestro arsenal de seguridad informática, que nos permite salvaguardar la confidencialidad e integridad de la información.

# SEGURIDAD INFORMÁTICA

## Unidad I – Principios de seguridad informática

### 1.1 - Aspectos técnicos y legales del manejo de la información

#### Ley general de protección de datos personales de México

Aquí el desarrollador debe implementar medidas de seguridad para proteger los datos de los usuarios que ingresan al sistema, evitando que puedan verse comprometidos. Un ejemplo de esto sería la utilización de técnicas de encriptación, otro seria establecer controles de acceso que definan claramente quién puede realizar determinadas acciones dentro del sistema, entre otras formas de protección. Desde el comienzo se deben tomar estas precauciones para garantizar la seguridad de todos los usuarios, además es fundamental documentar cada medida de seguridad añadida para mantener un orden y control adecuados en todo momento.

#### Ley de propiedad industrial

Esta ley es como un escudo protector para nuestras ideas y creaciones innovadoras en el mundo del desarrollo de software. Ya que alguien que ha trabajado durísimo en una idea revolucionaria, esta ley te ayuda a que nadie pueda simplemente copiarla y llevarse el crédito, esto es súper útil tanto para desarrolladores independientes como para empresas de desarrollo de software, ya que supongamos que inventas un algoritmo increíble, puedes patentarlo y ser el único con derecho a distribuirlo. Otro concepto interesante es el de secreto comercial, digamos que tu empresa ha desarrollado un software ultra avanzado que te da ventaja sobre la competencia, puedes mantenerlo en secreto, así tus competidores no pueden copiarlo y tú mantienes esa ventaja que tanto te costó conseguir.

#### Ley federal de derechos de actor

Esta ley es muy importante para nosotros los desarrolladores de software, ya que básicamente nos protege haciendo que todo el software que creamos sea considerado una obra protegida automáticamente. Esto significa que nadie puede vender, distribuir o usar nuestro software sin que les demos permiso primero esto es como tener un escudo legal para nuestro trabajo, ya que si alguien intenta pasarse de listo y usa nuestro software sin autorización, están cometiendo una infracción y se pueden meter en problemas legales serios.

Lo bueno de esta ley es que nos da el control total sobre nuestras creaciones y podemos decidir quién usa nuestro software y cómo, lo que es crucial cuando has invertido tanto tiempo y esfuerzo en desarrollar algo, además nos ayuda a proteger nuestras ideas innovadoras y a mantener una ventaja competitiva en el mercado.

#### Ley federal de datos personales en posesión de particulares

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares es como un libro de buenas prácticas que constantemente necesitamos consultar. Esto se debe a que trabajamos con datos personales todos los días, ya sea de nuestros usuarios o incluso de la empresa para la que trabajamos, esta ley básicamente nos indica cómo debemos manejar sus datos para evitar problemas legales.

Lo primero que hay que recalcar es que no podemos simplemente tomar los datos de la gente y hacer lo que queramos con ellos, ya que antes de hacerlo necesitamos su consentimiento, esto es como pedir prestado algo, pero para esto necesitamos subir un aviso de privacidad en el que se indique claramente nuestra intención y no podemos hacer uso de letra pequeña y una vez con los datos, no podemos tratarlos como si fueran nuestros.

#### Código penal federal

El Código Penal Federal es como el libro de reglas para el mundo digital cuando nos referimos a software, este código se encarga de definir qué está prohibido y cuáles son las consecuencias si alguien hace cosas del lado equivocado. Un ejemplo seria si alguien se dedica a piratear software o a crear copias falsas, se está metiendo en un gran problema, pasa lo mismo con los hackers que intentan entrar en sistemas ajenos sin permiso y las consecuencias pueden acabar con una multa por grandes cantidades de dinero o en casos más graves pasar un tiempo en prisión, es por esto es que no se debe de jugar con esto porque te podría afectar mucho.

#### Ley general de transparencia y acceso a la información

No hay duda de que esta ley es de interés para los desarrolladores de software, es por eso es especialmente relevante si trabajas en el sector público o si tu software lo utiliza, ya que aunque la ley está diseñada para proporcionar a la gente acceso a la información del gobierno, también introduce regulaciones sobre cómo se puede desarrollar software al respecto.

Ya que si trabajas en el desarrollo de software que se utiliza para o en entidades gubernamentales, primero necesitas estar al tanto de que el software al que contribuyes debe realizarse según los estándares de transparencia que establece esta ley, esto significa que la información que maneja o produce el software del público debe hacerse pública conforme a las disposiciones de la ley, por así decirlo el software no solo tiene que funcionar bien sino también facilitar la información al público.

### 1.2 – Estándares del manejo de la información

#### ISO 27001

Esta norma es un estándar internacional que dicta cómo implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la información, o SGI. El objetico principal es asegurarse de que la información esté bien protegida en tres aspectos clave: confidencialidad, integridad y disponibilidad. Esto significa que solo las personas autorizadas pueden acceder a la información, que los datos no se alteren sin permiso y que siempre estén accesibles cuando se necesiten.

La idea es que las empresas puedan hacer uso de esta norma como una guía para identificar y gestionar los riesgos relacionados con la seguridad de su información de una manera más eficiente.

#### ISO 17799

La ISO 17799, que también se conoce como "Tecnología de la información – Código de buenas prácticas para la gestión de la seguridad de la información", establece un marco bastante completo para manejar la seguridad de la información en una organización. Lo que hace es enfocarse en identificar, evaluar y gestionar los riesgos asociados a la seguridad de los datos.

Esta norma ofrece una serie de directrices muy claras para que las organizaciones puedan detectar esos riesgos y gestionarlos de manera eficiente. De esta forma, no solo se refuerzan las medidas de protección, sino que también se reduce significativamente la probabilidad de que ocurran incidentes relacionados con la seguridad de la información.

#### COBIT

COBIT es un marco diseñado para ayudar a las empresas a gestionar y gobernar su tecnología de la información (TI). Originalmente creado en 1996 por ISACA y ahora en su versión COBIT 2019, COBIT empezó como una guía para auditores de TI, pero hoy en día abarca a muchos más actores, como la Junta Directiva, la dirección ejecutiva y auditoría.

La idea detrás de COBIT es hacer una distinción clara entre lo que es "gobierno" y "gestión" en TI. El gobierno se encarga de asegurarse de que las decisiones y prioridades de TI estén alineadas con los objetivos de la empresa y se monitoreen adecuadamente. Normalmente, esto está en manos del Consejo de Dirección. Por otro lado, la gestión se enfoca en ejecutar esas decisiones, planificando, construyendo y operando las actividades necesarias para cumplir con los objetivos, y esto suele ser responsabilidad de la dirección ejecutiva.

COBIT también incluye los componentes clave para un buen sistema de gobierno, como procesos, estructuras organizativas, políticas, y la cultura dentro de la empresa. Todo esto ayuda a crear un sistema de TI más eficiente y bien dirigido.

#### NIST

#### El Instituto Nacional de Estándares y Tecnología (NIST) es una agencia que se enfoca en impulsar la innovación a través de la ciencia, los estándares y la tecnología de medición. Su Marco de Ciberseguridad (CSF) es un conjunto de estándares, guías y mejores prácticas que ayudan a las organizaciones a gestionar mejor los riesgos relacionados con la ciberseguridad.

#### Una de las grandes ventajas del CSF del NIST es su flexibilidad, lo que permite que se adapte fácilmente a los procesos de seguridad que ya existan en una organización, sin importar la industria. Además, es una excelente base para que las empresas privadas en Estados Unidos comiencen a implementar tanto seguridad de la información como una gestión efectiva de los riesgos de ciberseguridad.

#### ITIL

ITIL, que significa **Information Technology Infrastructure** **Library**, es un conjunto de buenas prácticas que ayuda a las organizaciones a mejorar la prestación de servicios, especialmente en el ámbito de TI. Básicamente, ofrece una guía para gestionar servicios de TI de forma más eficiente, alineando la gestión con los objetivos y estrategias de la empresa.

Este marco se basa en cinco etapas que forman el ciclo de vida de un servicio: Estrategia de servicio, que establece metas y prioridades; Diseño del servicio, que se enfoca en la infraestructura y los procesos; Transición del servicio, que asegura cambios sin interrupciones; Operación del servicio, que garantiza la estabilidad diaria; y Mejora continua de los servicios, que busca perfeccionar los procesos progresivamente.

Lo bueno de ITIL es su flexibilidad, ya que las empresas pueden adoptar solo las partes que les resulten más útiles y adaptarlas según sus necesidades. Esto permite a las organizaciones ser más eficientes en su gestión de TI y lograr mejores resultados.

### 1.3 – Conceptos de seguridad

#### Accesibilidad

La accesibilidad asegura que sistemas, aplicaciones y datos estén disponibles y operativos para los usuarios autorizados cuando los necesiten, sin interrupciones. Es crucial para mantener la continuidad del negocio y evitar pérdidas económicas. Las amenazas a la accesibilidad incluyen ataques de denegación de servicio, fallos técnicos y errores humanos. Para garantizarla, se deben implementar redundancia, copias de seguridad, mantenimiento continuo y planes de recuperación ante desastres, asegurando que la información y los sistemas permanezcan disponibles y funcionales para todos los usuarios.

#### Confidencialidad

La confidencialidad protege la información contra accesos no autorizados, asegurando que solo personas y sistemas autorizados puedan acceder a datos sensibles. Es crucial para resguardar la privacidad de datos personales, financieros y de negocios. Amenazas comunes incluyen phishing, malware y robo de credenciales. Para proteger la confidencialidad se usan técnicas como encriptación, controles de acceso, autenticación multifactor y políticas de contraseñas seguras. Esto previene la pérdida de datos y mantiene la confianza de los usuarios, garantizando que la información no sea divulgada sin autorización.

#### Disponibilidad

La disponibilidad en seguridad informática asegura que los sistemas, servicios y datos estén accesibles y operativos para los usuarios autorizados cuando los necesiten. Es crucial para evitar interrupciones que puedan afectar la operatividad de una organización. Las principales amenazas incluyen ataques de denegación de servicio (DoS), fallos técnicos y errores humanos. Para garantizar la disponibilidad, se implementan medidas como redundancia de sistemas, copias de seguridad y planes de recuperación ante desastres. Mantener la disponibilidad es esencial para asegurar la continuidad del servicio y minimizar los riesgos de inactividad.

#### Autenticación

La autenticación es el proceso de verificar la identidad de un usuario, dispositivo o sistema antes de permitirle el acceso a recursos protegidos. Es fundamental para garantizar que solo los usuarios autorizados puedan acceder a la información. Los métodos de autenticación más comunes incluyen contraseñas, autenticación de dos factores (2FA), biometría (huellas digitales, reconocimiento facial) y tokens de seguridad. Una autenticación robusta protege contra accesos no autorizados, ayuda a prevenir fraudes y es un pilar básico en la seguridad de cualquier sistema.

#### Integridad

La integridad en seguridad informática asegura que la información y los datos se mantengan exactos, completos y sin alteraciones no autorizadas, tanto durante su almacenamiento como en su transmisión. Esto es clave para garantizar que los datos no sean manipulados, corrompidos o modificados de manera malintencionada. Las amenazas a la integridad incluyen malware, errores humanos y ataques de manipulación de datos. Para protegerla, se utilizan técnicas como controles de acceso, firmas digitales, algoritmos de hash y auditorías regulares. Mantener la integridad es esencial para asegurar la confiabilidad y precisión de la información.

#### Control de acceso

El control de acceso es un mecanismo de seguridad que regula quién o qué puede ver o utilizar recursos en un entorno informático. Su objetivo es garantizar que solo los usuarios y dispositivos autorizados puedan acceder a sistemas, datos o aplicaciones específicos. Los métodos más comunes incluyen listas de control de acceso (ACL), permisos basados en roles (RBAC) y autenticación multifactor (MFA). Un buen control de acceso protege contra accesos indebidos, minimiza riesgos de filtración de datos y ayuda a mantener la seguridad y privacidad de la información crítica.

### 1.4 – Conceptos de criptografía

#### Criptografía simétrica

La criptografía simétrica es la que usa la misma clave para cifrar y descifrar información. Esto significa que todas las personas que necesiten acceder a la información cifrada deben tener la clave compartida.

Esta clave conocida como clave secreta es esencial para el cifrado y descifrado. No se trata solo de mantener la clave confidencial sino de protegerla adecuadamente para que no sea divulgada. También la simétrica es eficiente para proteger grandes volúmenes de datos y se usa comúnmente en áreas como el cifrado de datos almacenados, la validación de mensajes y la generación de números aleatorios, etc.

#### Criptografía asimétrica

La criptografía asimétrica, también conocida como criptografía de clave pública, utiliza dos claves diferentes pero matemáticamente relacionadas para asegurar la comunicación y proteger la información. Estas dos claves son:

* **Clave Pública:** Puede ser compartida con cualquier persona. Se utiliza para cifrar datos.
* **Clave Privada:** Se mantiene en secreto y se utiliza para descifrar datos cifrados con la clave pública correspondiente.

**Ventajas:**

* **Seguridad:** Ofrece una alta seguridad al eliminar la necesidad de compartir una clave secreta entre las partes.
* **Autenticación:** Permite verificar la identidad del remitente a través de firmas digitales.

**Desventajas:**

* **Desempeño:** El cifrado y descifrado asimétrico suele ser más lento que el cifrado simétrico debido a la complejidad matemática involucrada.

**Aplicaciones Comunes:**

* **Intercambio Seguro de Claves:** Usado para intercambiar claves simétricas de manera segura.
* **Certificados Digitales:** Utilizados en protocolos como HTTPS para asegurar comunicaciones en la web.

#### Cifrado por bloques y por flujo

Los cifrados en bloque y los de flujo son dos formas diferentes de cifrar datos, cada uno con su estilo.

**Cifrados de bloque**

En los cifrados de bloque, lo que haces es dividir la información en pedazos de un tamaño fijo, digamos de 64 o 128 bits, y a cada uno de esos bloques les aplicas el mismo proceso de cifrado con una sola clave. Por ejemplo, con AES o DES. Es como si cortaras un pastel en trozos iguales y luego les pusieras la misma cobertura.

**Cifrados de flujo**

En cambio, los cifrados de flujo son más dinámicos, van bit por bit o byte porbyte. Generan un flujo de claves aleatorio, y esa clave se mezcla con los datos originales usando XOR. Estos son más prácticos cuando estás manejando datos en tiempo real, como en transmisiones de video o audio en vivo. Es como si en lugar de cubrir todo el pastel de una vez, lo fueras decorando parte por parte mientras lo sirves.

Entonces, los de bloque trabajan por partes grandes y fijas, mientras que los de flujo son más flexibles y cifran conforme los datos van llegando.

# Bibliografía

Consejo de la Judicatura Federal. Sistema de gestión de seguridad de datos personales. <https://www.cjf.gob.mx/transparencia/resources/datos/sistemaGestionSeguridadDatosPersonales.pdf>

Thales Group. Protecting software intellectual property. <https://cpl.thalesgroup.com/es/software-monetization/protecting-software-intellectual-property>

Delete Technology. Legislación y normativa de software en México. <https://www.deletetechnology.com/blog/legislacion-y-normativa-de-software-en-mexico#:~:text=C%C3%B3digo%20Penal%20Federal.-,Ley%20Federal%20del%20Derecho%20de%20Autor,una%20infracci%C3%B3n%20de%20estos%20derechos>.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Marco de competencias. <https://micrositios.inai.org.mx/marcocompetencias/?page_id=370>

Amazon Web Services. What is cryptography? <https://aws.amazon.com/es/what-is/cryptography/>

Conceptos basicos de seguridad informatica

<http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf>

Utimaco. ¿Qué es la criptografía simétrica? <https://utimaco.com/es/servicio/base-de-conocimientos/gestion-de-claves-y-secretos/que-es-la-criptografia-simetrica>

GlobalSuite Solutions. ¿Qué es la norma ISO 27001 y para qué sirve? <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>

NORMAS ISO ORG. Norma ISO 17799 <https://normasiso.org/norma-iso-17799/>

GlobalSuite Solutions. ¿Qué es COBIT y para qué sirve? <https://www.globalsuitesolutions.com/es/que-es-cobit/#COBIT_Control_Objetives_for_Information_and_Related_Technology>

IBM ¿Qué es el marco de ciberseguridad NIST? <https://www.ibm.com/mx-es/topics/nist>

Freshservice. ¿Qué es ITIL y para qué sirve? <https://www.freshworks.com/es/freshservice/itil/que-es-itil/>

Instituto EITCI. ¿Qué son los cifrados de bloque y en qué se diferencian de los cifrados de flujo en términos de cifrado de datos? <https://es.eitca.org/la-seguridad-cibern%C3%A9tica/eitc-es-ccf-fundamentos-de-la-criptograf%C3%ADa-cl%C3%A1sica/aplicaciones-de-cifrados-en-bloque/modos-de-operaci%C3%B3n-para-cifrados-en-bloque/examination-review-modes-of-operation-for-block-ciphers/what-are-block-ciphers-and-how-do-they-differ-from-stream-ciphers-in-terms-of-data-encryption/>

¿Que es la criptografia asimetrica?

<https://protecciondatos-lopd.com/empresas/criptografia-asimetrica/>