RESUMEN SEGUNDO PARCIAL SEGURIDAD Y CALIDAD EN APLICACIONES WEB

Unidad N°3: Criptografía

Elementos teóricos de la criptografía

D(k, E(k, m)) = m

"m" representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto claro, o plaintext) que pueden ser enviados.

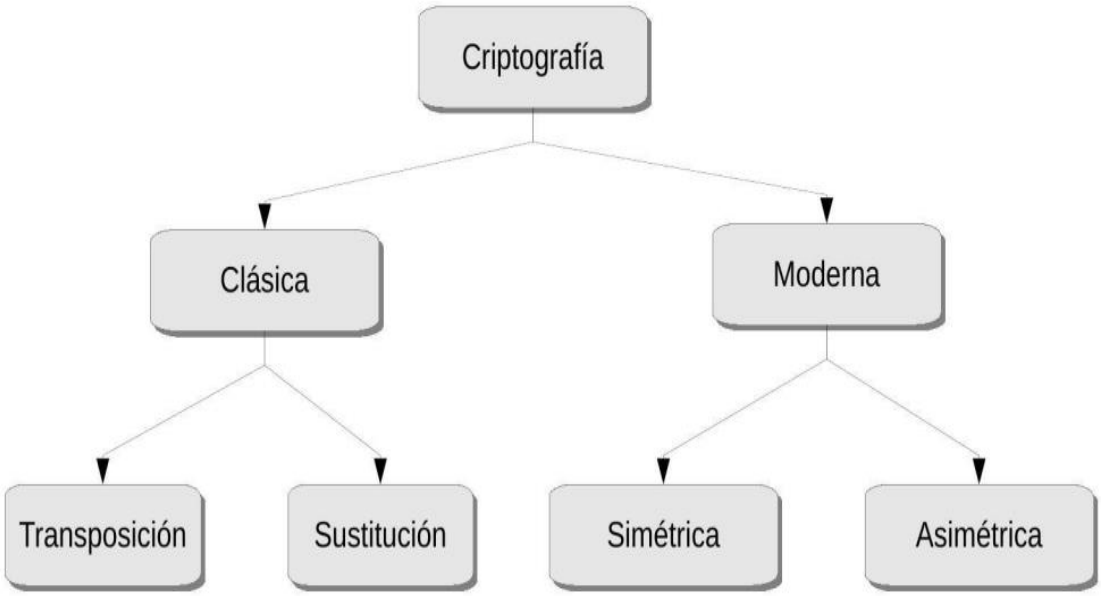
"C" representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.

"k" representa el conjunto de claves que se pueden emplear en el criptosistema.

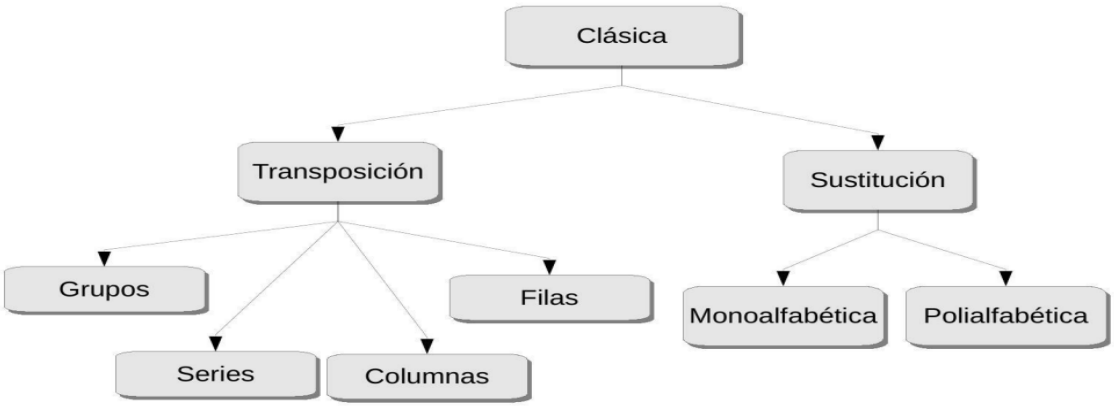
"E" es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de **M** para obtener un elemento de **C**. Existe una transformación diferente **E** para cada valor posible de la clave **k**.

"D" es el conjunto de transformaciones de descifrado, análogo a **E**.

Clasificación



Criptografía clásica



Transposición

Los cifradores por transposición utilizan la técnica de permutación de forma que los caracteres del texto se reordenan mediante un algoritmo específico.

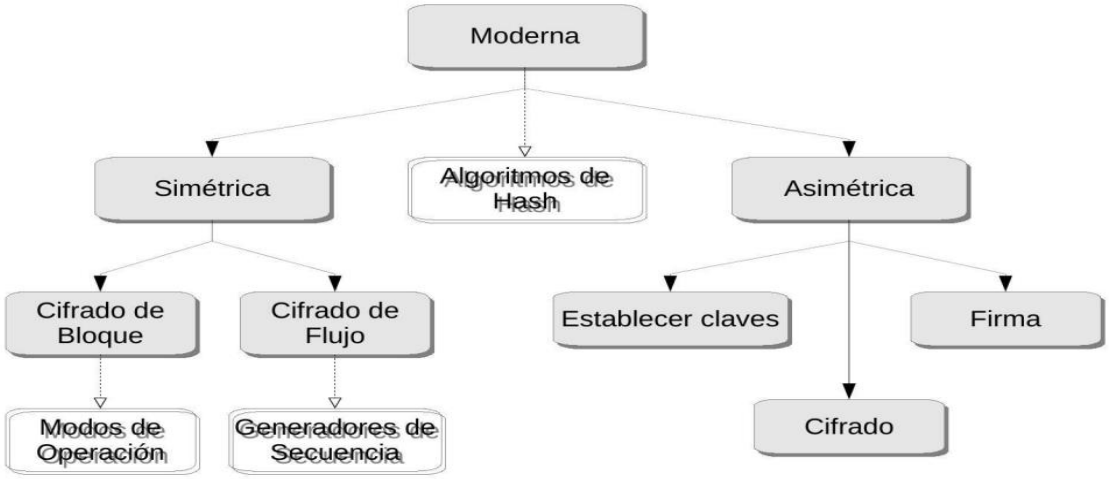
Sustitución

Los cifradores por sustitución utilizan la técnica de modificación de cada carácter del texto en claro por otro correspondiente al alfabeto de cifrado.

- **Monoalfabético**
  Si el alfabeto de cifrado es el mismo que el del mensaje o bien el único, hablamos entonces de cifradores monoalfabéticos; es decir, existe un único alfabeto en la operación de transformación del mensaje en criptograma.

- **Polialfabético**
  Por el contrario, si en dicha operación intervienen más de un alfabeto, se dice que el cifrador es polialfabético. Los cifradores por sustitución polialfabética utilizan diferentes caracteres para el reemplazo de un mismo carácter de origen.

Criptografía moderna



Algoritmos simétricos

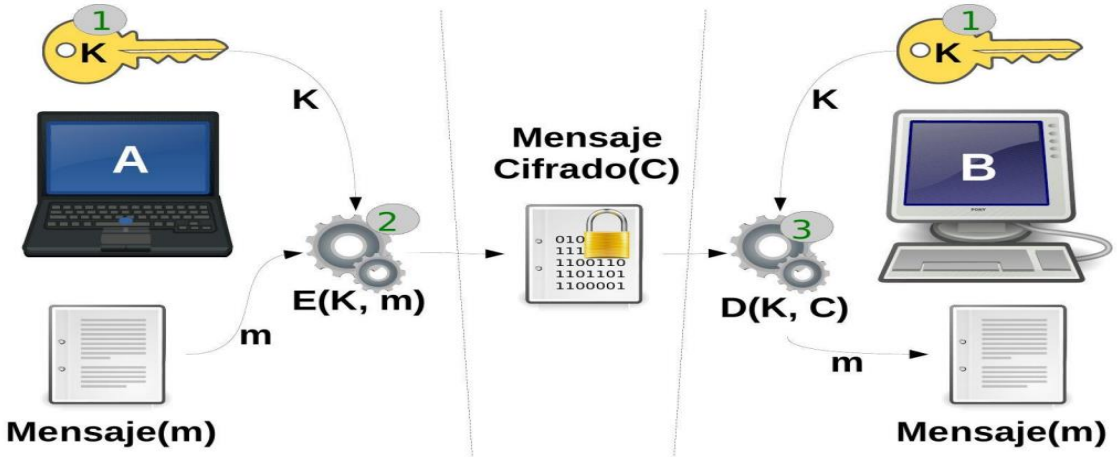
Un sistema de cifrado simétrico es un tipo de cifrado que usa una misma clave para cifrar y para descifrar. Las dos partes que se comunican mediante el cifrado simétrico deben estar de acuerdo en la clave a usar de antemano. Una vez de acuerdo, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra usando la misma clave.

Ventajas

- Sencillez de implementación
- Robustez
- Velocidad de cifrado
- Longitud del mensaje

Desventajas

- La clave debe ser compartida previamente con seguridad
- La comunicación entre múltiples actores requiere numerosas claves



Ejemplos

- DES-LUCIFER (1976, Data Encryption Standard)
- 3DES (1998, Triple Data Encryption Standard, NIST)
- AES-Rijndael (2001, Advanced Encryption Standard, NIST)
- Serpent (1998)
- Twofish
- RC6 (1998, Rivest Cipher 6)
- MARS (1998, IBM)
- GOST (1994, Magma URSS)
- CAMELLIA (2000, NTT y Mitsubishi Electric)
- IDEA (1991, lnternational Data Encription Algorithm)
- Blowfish (1993, diseñado por Bruce Schneier)
- RC5 (1994, Rivest Cipher 5)

Cifrado de bloque

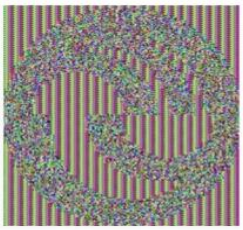
Es un método de cifrado que se utiliza para proteger la confidencialidad y seguridad de la información mediante la transformación de bloques de datos en texto cifrado. En lugar de cifrar los datos de forma individual, se dividen en bloques de tamaño fijo y cada bloque se cifra por separado utilizando un algoritmo criptográfico.

Es ampliamente utilizado en aplicaciones que requieren seguridad y realizan transmisión de información sensible a través de canales inseguros. Al aplicarlo, se dificulta la tarea de los atacantes de acceder a la información original sin poseer la clave adecuada, brindando una capa adicional de protección para los datos.

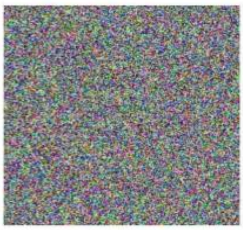
Referencia: Ataques por marca de agua

Los ataques por marca de agua pueden tener como objetivo eliminar la marca de agua o intentar descifrar la información oculta en ella.

Original



ECB



CBC

Modos de operación

- **ECB: Electronic codebook**

  Este método el mensaje se fracciona en partes y cada una es cifrada de manera independiente.

  Padding o Esquema de Relleno

  Los algoritmos simétricos de bloque requieren que el mensaje sea fragmentado en partes de una longitud fija; esto plantea el problema de que el mensaje en su totalidad o su ultimo bloque podría ser de longitud menor a la requerida, en este caso se recurre a los métodos de padding para resolver el problema. Es decir, es un método para completar el final de un bloque de datos

  Algunos de ellos son:

  - Bit padding (RFC1321, ISO/IEC 9797-1)
  - ISO/IEC 7816-4
  - PKCS#7 (RFC2315, Sec 10.3)
  - ISO 10126
  - ANSI X.923

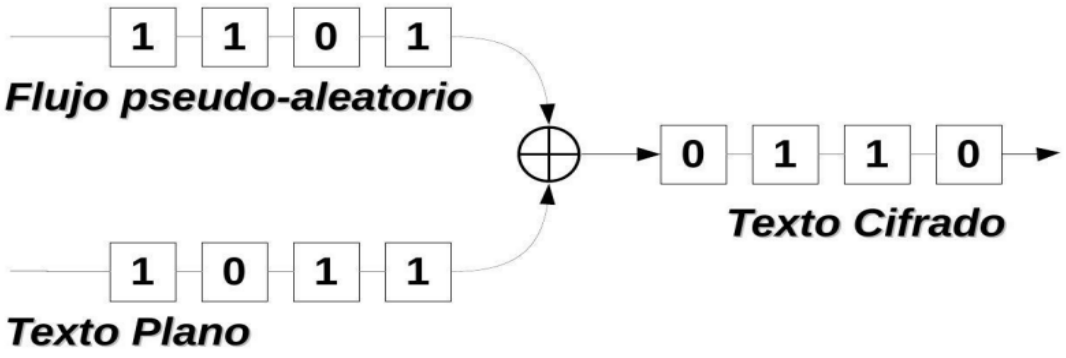
- **CBC: Cipher block chaining**
  Este método el mensaje se fracciona en partes y se realiza un XOR con el bloque previo antes de cifrar cada parte.

  Vector de inicialización
  Es un valor aleatorio o pseudoaleatorio utilizado en combinación con una clave para inicializar un algoritmo de cifrado simétrico en modo de operación de cifrado por bloques. El propósito del IV es introducir aleatoriedad en el proceso de cifrado y evitar la generación de patrones repetitivos.

- **CFB: Cipher Feedback**
  Este método el mensaje se fracciona en partes, se cifra un vector de inicialización y al resultado se le realiza un XOR con el bloque del mensaje. Los bloques posteriores utilizan como entrada el texto cifrado para reemplazar al vector de inicialización.
- **OFB: Output Feedback**
  Este método opera de manera similar a CFB con la diferencia que el bloque a ser utilizado como entrada del siguiente proceso es tomado de la salida del algoritmo justo antes de realizar el XOR.
- **CTR: Modo de Counter o contador**
  Este modo de operación (al igual que en OFB) se utiliza un "nance" equivalente al IV anterior, que es alterado por un contador incrementado en cada bloque de datos, para obtener un valor que luego será operado con el bloque de datos usando XOR .

Cifrado de flujo

Consistía en emplear una secuencia aleatoria de igual longitud que el mensaje, que se usaría una única vez (One Time Pad), combinándola mediante alguna función simple y reversible como el or exclusivo(XOR) con el texto en claro carácter a carácter. Este método presenta el grave inconveniente de que la clave es tan larga como el propio mensaje. Se utiliza una función generadora de bits pseudo-aleatorios a fin de obtener un flujo de bits que pueda ser procesado con los bits del mensaje mediante una operación básica (XOR).



Funciones de HASH

Se define como una función o método no reversible para generar un valor que represente de manera casi unívoca a un dato.

Principales usos

- Soporte para criptografía asimétrica
- Tablas de Hash
- Verificación de integridad
- Soporte para procesos de autenticación

MAC (Message Authentication Code)

Adiciona criptografía al proceso de hash para aumentar la seguridad del mismo.

Funciones HASH

- **MD4 (Message Digest, Mensajes Digitales)**
  Se realiza una manipulación de bits para obtener el valor hash, obteniéndolo de forma rápida, provocando que sea más riesgoso en un ataque. Se considera un estándar de Internet (RFC-1320) [STA98].
- **MD5 Extensión a MD4**
  La obtención del valor hash es lento pero considerado más seguro. Está especificado como un estándar de internet (RFC-1321).
- **SHA-1 (Secure Hash Algorithm, Algoritmo Hash Seguro)**
- **SHA-2 (Secure Hash Algorithm, Algoritmo Hash Seguro)**
- **SHA-3 (Secure Hash Algorithm, Algoritmo Hash Seguro)**
- **RIPEMD-160**

Funciones de Derivación de Claves

Conocidas como KDF (Key Derivation Function) son funciones no reversibles que tienen el objetivo de generar una o más claves en base a un valor maestro o clave inicial secretos, más un conjunto de parámetros que configuran el comportamiento de la función afectando el resultado.

Normalmente se basan en funciones pseudo-aleatorias, funciones de hash con múltiples iteraciones y procesos de inclusión de 'Salt'. Se han originado para evitar a ataques de diccionario y tablas de arcoiris.

- PBKDF2 - (2000) Password-Based Key Derivation Function 2 - RFC2898 y (PKCS#5, NIST SP 800-132)
- bcrypt - (1999) Basado en el algoritmo de Blowfish
- scrypt - (2012) Basado en PBKDF2_HMAC_SHA256
- HKDF - (2010) HMAC-based Extract-and-Expand Key Derivation Function RFC5869
- Argon2 - (2015) Por la Universidad de Luxemburgo - RFC9106

Algoritmos asimétricos

El sistema de cifrado de clave pública usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla para que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

Ventajas

- No requiere confidencialidad en la distribución de clave
- La misma clave puede ser utilizada por múltiples actores en la comunicación
- Permite autentificar mensajes

Desventajas

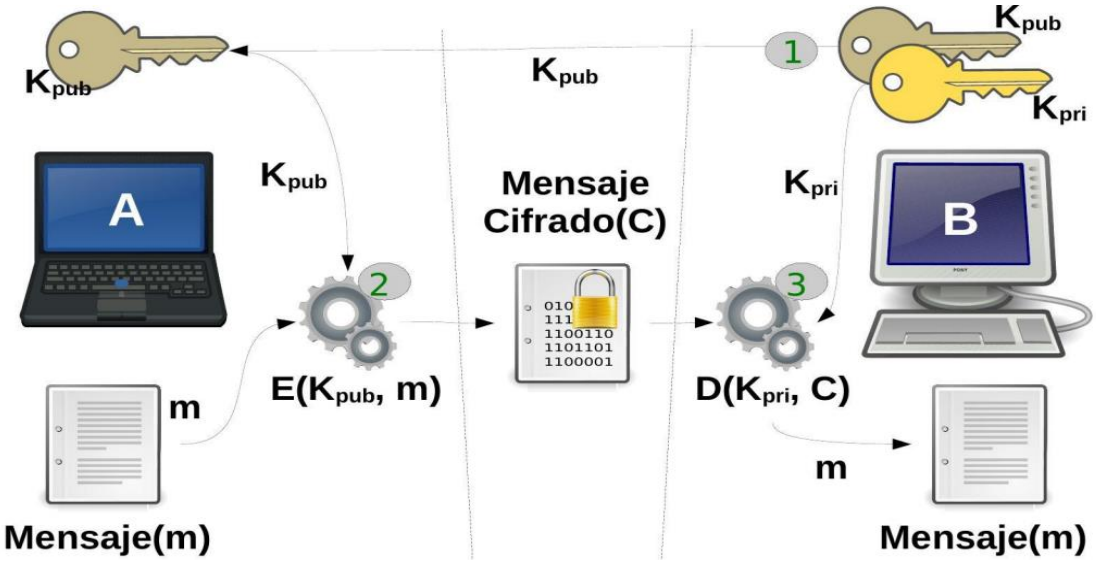
- Velocidad de cifrado/descifrado
- Longitud de mensaje limitado
- Tamaño del mensaje cifrado es mayor
- Se requieren claves de gran extensión

Este tipo de algoritmos suelen disponer de las siguientes operaciones:

1. Generación de claves
2. Cifrado
3. Descifrado
4. Firma
5. Verificación de firma

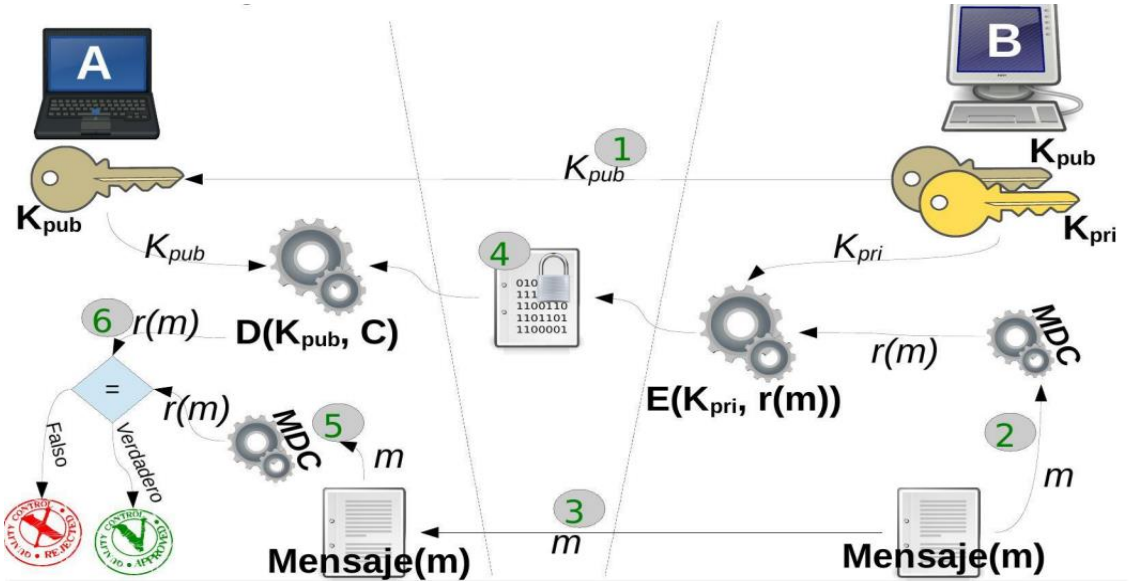
Ejemplos

- **Define-Hellman**
  Este algoritmo nos permite compartir un mensaje cifrado entre dos actores que no han tenido contacto previo; por esta razón suele utilizarse para acordar una clave de cifrado a través de un canal inseguro y sin autenticación.
- **RSA**
  Se basa en la dificultad para factorizar grandes numeras.
- **EIGamal**
  Se basa en el problema de los logaritmos discretos El hecho de aplicar aritmética modular hace el problema de hallar e irresoluble en un tiempo razonable
- **DSA**
  El algoritmo DSA (Digital Signature Algorithm) es una parte el estándar de firma digital DSS (Digital Signature Standard), definido en el FIPS-186. Este algoritmo, propuesto por el NIST, data de 1991, es una variante del método asimétrico de EIGamal.
- **ECC**, Criptografía de curva elíptica (ECDH, ECDSA...)



Autentificación de mensaje (Firma)

Algunos algoritmos asimétricos permiten que se pueda autenticar un mensaje para garantizar su integridad. En este caso la clave que se emplea para cifrar es la clave privada, justo al revés que para la simple codificación de mensajes.



Algoritmos públicos y privados

Los algoritmos públicos son aquellos cuya definición y funcionamiento se ponen a disposición pública, permitiendo que cualquier persona o entidad acceda al mismo para su evaluación o investigación.

En contraparte los privados son aquellos cuyo funcionamiento interno es desconocido; en el ámbito de la criptografía estos últimos son considerados menos confiables.

Http vs Https

http: Hyper Text Transfer Protocol, protocolo para transmisión de información en plano, sin cifrado. Su puerto por defecto es el número 80.

https: Hyper Text Transfer Protocol Secure protocolo para transmisión información cifrada mediante SSL o TLS. Su puerto por defecto es el número 443.

SSL (Secure Sockets Layer)

Es un protocolo que proporciona privacidad e integridad entre dos aplicaciones. El sistema SSL es independiente del protocolo utilizado; esto significa que puede asegurar transacciones realizadas en la Web a través del protocolo HTTP y también conexiones a través de los protocolos FTP, POP e IMAP. SSL actúa como una capa adicional que permite garantizarla seguridad de los datos y que se ubica entre la capa de la aplicación y la capa de transporte (por ejemplo, el protocolo TCP)

Los datos que circulan en un sentido y otro entre el cliente y el servidor se cifran mediante un algoritmo simétrico como DES o RC4. Un algoritmo de clave pública – generalmente RSA - se utiliza para el intercambio de las claves de cifrado y para las firmas digitales. El algoritmo utiliza la clave pública en el certificado digital del servidor. Con el certificado digital del servidor, el cliente también puede verificar la identidad del servidor.

Fases

1. Establecimiento de la conexión y negociación de los algoritmos criptográficos que van a usarse en la comunicación.
2. Intercambio de claves.
3. Cifrado simétrico de tráfico.

TLS (Transport Layer Security)

TLS {Transport Layer Security) es una evolución del protocolo SSL (Secure Sockets Layer), es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor.

- RFC 2246 (1999) - The TLS Protocol Version 1.0
- RFC 4346 (2006) - The TLS Protocol Version 1.1
- RFC 5246 (2008) / RFC 6176 (2011) - The TLS Protocol Version 1.2
- RFC 8446 (2018) - The TLS Protocol Version 1.3

Firma Electrónica

Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

Firma Digital

Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Se utiliza para garantiza la autenticidad de datos.

Propiedades

- Va ligada indisolublemente al mensaje. Una firma digital válida para un documento no puede ser válida para otro distinto.
- Solo puede ser generada por su legítimo titular. Al igual que cada persona tiene una forma diferente de escribir, y que la escritura de dos personas diferentes puede ser distinguida mediante análisis caligráficos, una firma digital sólo puede ser construida por la persona o personas a quienes legalmente corresponde.
- Es públicamente verificable. Cualquiera puede comprobar su autenticidad en cualquier momento, de forma sencilla.

Modelos de Infraestructura de Seguridad

PKI - Infraestructura de Clave Publica

Es una combinación de hardware, software, políticas y procedimientos de seguridad que define un entorno de confianza centralizado y provee garantías para operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Componentes:

- Autoridad de Certificación (CA, Certificate Authority): Emite y revoca certificados, vinculando las claves públicas con la identidad del propietario.
- Autoridad de Registro (RA, Registration Authority): Verifica la relación de los certificados y la identidad de sus titulares.
- Autoridad de Validación (VA, Validation Authority): Es la encargada de comprobar la validez de los certificados digitales.
- Autoridad de Sellado de Tiempo (TSA, TimeStamp Authority): Es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.
- Los repositorios: Almacenan información relativa a la PKI, como certificados y listas de revocación (CRL, Certificate Revocation List).
- Los usuarios y entidades finales que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública.

Certificados Digitales

Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular

Es esencialmente una clave pública, un identificador e información accesoria; firmados digitalmente por una autoridad de certificación, y su utilidad es demostrar que una clave pública pertenece a un usuario concreto.

El estándar X.509 solo define la sintaxis de los certificados, por lo que no está atado a ningún algoritmo en particular, y contempla los siguientes campos:

- Versión.
- Número de serie.
- Identificador del algoritmo empleado para la firma digital.
- Nombre del certificador.
- Periodo de validez.
- Nombre del sujeto.
- Clave pública del sujeto.
- Identificador único del certificador.
- Identificador único del sujeto.
- Extensiones.
- Firma digital de todo lo anterior generada por el certificador.

Certificados Digitales de revocación

Cuando una clave pública pierde su validez por destrucción o robo de la clave privada correspondiente, por ejemplo, es necesario anularla. Para ello se emplean los denominados certificados de revocación que no son más que un mensaje que identifica a la clave pública que se desea anular, firmada por la clave privada correspondiente.

Online Certificate Status Protocol

OCSP: es un método para determinar el estado de vigencia de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados).

Anillo o Circulo de confianza

Es un modelo de confianza distribuido que provee garantías para operaciones criptográficas como el cifrado, la firma o el no repudio de transacciones electrónicas basado en la cantidad de firmas de actores de confianza que posea una clave pública.

Ley de Firma Digital - República Argentina Ley 25.506

El proyecto de Firma Digital tiene por objetivo lograr la implementación de esta herramienta tecnológica en los sistemas administrativos y de gestión de los distintos organismos que conforman la Administración Pública, con el fin de que el accionar de éstos resulte más eficiente. La Secretaría de Gabinete y Coordinación Administrativa actúa como Ente Licenciante otorgando, denegando o revocando las licencias de los certificadores licenciados y

supervisando su accionar. En este sentido, los certificadores licenciados son entidades públicas o privadas que se encuentran habilitados por el Ente Licenciante para emitir certificados digitales, en el marco de la Ley 25.506 de Firma Digital.

Unidad N°4: Aplicaciones de seguridad

Logging

Su finalidad se vincula a las siguientes puntos:

- Identificar incidentes de seguridad
- Monitorear violaciones a las políticas
- Asistir en controles de no-repudio
- Proveer información sobre problemas o situaciones atípicas
- Contribuir con información específica para la investigación de incidentes que no pueda obtenerse de otras fuentes
- Contribuir con la defensa ante vulnerabilidades y exploits mediante de la detecci6n de ataques

¿Dónde registrar?

Sistemas de archivos, almacenamiento en la nube, bases de datos SQL y NoSQL

¿Qué registrar ?

Fallas de validación, autenticación, autorización, anomalías, fallas de aplicación, eventos legales...

¿Que NO registrar ?

Código fuente, identificadores de sesion, credenciales y tokens de acceso, claves de cifrado, SPI...

Enmascaramiento de datos

Es el proceso mediante el cual se reemplazan las datos sensibles de un sistema con el objetivo de proteger esta información confidencial ante situaciones que escapen al control sobre la misma.

Validación de entrada

La debilidad de seguridad más común en aplicaciones web es la falta de validación apropiada de las entradas del cliente o del entorno. Esta debilidad lleva a casi todas las principales vulnerabilidades en las aplicaciones web, tales como inyección a interprete, ataques locale/ Unicode, ataques al sistema de archivos y desbordamientos de memoria.

Nunca se debe confiar en las datos introducidos por el cliente, ya que tiene todas las posibilidades de manipular las datos. La validación debe cubrir los aspectos semánticos como sintácticos de la información ingresada.

Autenticación en la Web

Su objetivo es proveer servicios de autenticación segura a las aplicaciones Web, mediante:

- Vinculando una unidad del sistema a un usuario individual mediante el uso de una credencial
- Proveyendo controles de autenticación razonables de acuerdo al riesgo de la aplicación.
- Denegando el acceso a atacantes que usan varios métodos para atacar el sistema de autenticación.

Consideraciones generales

- La autenticación es solo tan fuerte coma sus procesos de administraci6n de usuarios
- Use la forma más apropiada de autenticaci6n adecuada para su clasificaci6n de bienes
- Re-autenticar al usuario para transacciones de alto valor y acceso a áreas protegidas
- Autenticar la transacción, no el usuario
- Las contraseñas son trivialmente rotas y no son adecuadas para sistemas de alto valor

Buenas practicas

1) User IDs
2) Fortaleza de contraseñas
3) Implementar métodos seguros de recuperación
4) Almacenar contraseñas de forma segura
5) Transmitir contraseñas solo sobre TLS
6) Solicitar re-autenticación
7) Utilizar sistemas de autenticación de factor múltiple
8) Manejo de mensajes de error
9) Prevenir ataques por fuerza bruta

Métodos de protección ante ataques de automatización

- MFA o autenticación de factor múltiple
- Bloqueo de cuenta
- CAPTCHA
- Preguntas de seguridad o palabras a memorables

Objetivos

- Asegurar que únicamente usuarios autorizados puedan realizar acciones permitidas con su correspondiente nivel de privilegio.
- Controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.

- Prevenir ataques de escalada de privilegios, como por ejemplo utilizar funciones de administrativas siendo un usuario anónimo o incluso un usuario autenticado.

Contraseñas de un solo uso

OTP "One Time Password" o "contraseña de un solo uso", corresponde a un valor confidencial que no puede ser reutilizado.

HOTP Algoritmo de generación de "contraseñas de un solo uso basadas en HMAC". RFC-4226

TOTP "Time-based One Time Password" o "contraseña de un solo uso basada en tiempo", es un valor confidencial que no puede ser reutilizado y que además cuenta con un tiempo de vida acotado. RFC-6238

Técnicas de autenticación de Usuarios

1) Autenticación básica y segura (HTTP-Basic, HTTP-Digest)
2) Autenticación basada en formularios (Usuario-contraseña)
3) Autenticación integrada (JSS, ASP.NET, Active Directory)
4) Autenticación basada en certificado (x509)
5) Autenticación fuerte o de factor múltiple (Algo que sabes, algo que tienes, algo que eres, tu ubicación)

JWT - Json Web Token

Es un estándar abierto (rfc7519) utilizado para transmitir de forma segura informaci6n en formato JSON. Está compuesto por tres partes: el encabezado que especifica el tipo de token y el algoritmo de firma, la carga útil que contiene los datos relevantes y la firma que verifica la integridad del token. Los tokens JWT se utilizan en aplicaciones web y servicios API para la autenticación y autorización, ya que son seguros, compactos y autocontenidos. Son portables y se pueden utilizar en diferentes sistemas siempre y cuando se comparta la clave necesaria para verificar la firma del token. Esto permite la interoperabilidad entre servicios y aplicaciones.

Métodos de control de acceso

1. **Role Based Access Control (RBAC)**
   Las decisiones de acceso se basan en las funciones y responsabilidades de un individuo dentro de la organización o de la base de usuarios. El proceso de definición de las funciones se basa por lo general en el análisis de los objetivos y la estructura de una organización que por lo general está relacionada con la política de seguridad.
2. **Discretionary Access Control (DAC)**
   Es un medio para restringir el acceso a la información sobre la base de la identidad de las usuarios y/o la pertenencia a ciertos grupos. Decisiones de acceso se basan normalmente en las autorizaciones concedidas a un usuario

basándose en las credenciales que presento en el momento de la autenticación (nombre de usuario, contraseña, hardware / identificador de software, etc.)

3. **Mandatory Access Control (MAC)**
   Garantiza que la ejecución de la política de seguridad de la organización no se basa en el cumplimiento del usuario en la aplicación web. MAC asegura la información mediante la asignación de etiquetas de sensibilidad en la información y comparando esto con el nivel de sensibilidad de un usuario está operando a. Mecanismos MAC asignan un nivel de seguridad a toda la información, asignar un control de seguridad de cada usuario, y garantizar que todos las usuarios solo tengan acceso a los datos pertinentes.
4. **Attribute Based Access Control (ABAC)**
   Es un sistema de control basado en atributos asignados a cualquier componente del sistema (usuarios, recursos, etc.). El mismo establece políticas que utilizan la información de dichos atributos para establecer si un acceso está permitido, de esta forma se establece un sistema de control basado en relaciones.

Buenas prácticas de implementación

- Codificar el control en la actividad objetivo
- Disponer de un Controlador Centralizado (ACL)
- Utilizarun Control Central de Acceso, en las diferentes capas
- Verificar la política del lado del servidor (Server-side)

Ataques de control de acceso

1. **Vertical Access Control Attacks** - Un usuario convencional obtiene accesos superiores o de administrador.
2. **Horizontal Access Control attacks** - Con el mismo rol o nivel el usuario puede acceder a información de otros usuarios.
3. **Business Logic Access Control Attacks** - Abusar de una o más actividades para realizar una operación con un resultado no autorizado para ese usuario.

Administración de Usuarios y privilegios

Objetivos

- Las funciones de nivel de administrador están segregadas apropiadamente de la actividad del usuario.
- Los usuarios no pueden acceder o utilizar funcionalidades administrativas
- Proveer la necesaria auditoria y trazabilidad de funcionalidad administrativa

Mejores practicas

- Cuando se está diseñando aplicaciones, trazar la funcionalidad administrativa fuera y asegurarse que los controles apropiados de acceso y auditoría están en su lugar.

- Considerar procesos – en algunas ocasiones todo lo que se requiere es entender como los usuarios pueden ser prevenidos de utilizar una característica con la simple falta de acceso.
- Acceso de servicio de asistencia es siempre un término medio – ellos necesitan acceso para ayudar a las clientes, pero no son administradores.
- Diseñar cuidadosamente la funcionalidad de servicio de asistencia / moderador / soporte al cliente alrededor de una capacidad administrativa limitada y aplicación segregada o acceso.
- Todos los sistemas deberían tener aplicaciones separadas del acceso de los usuarios para los administradores.
- Sistemas de alto valor deberían separar estos sistemas en un servidor separado, que tal vez no sea accesible desde el amplio Internet sin acceso para la administración de redes, como a través del uso de una VPN fuertemente autenticada o desde la red de un centro de operaciones de confianza.

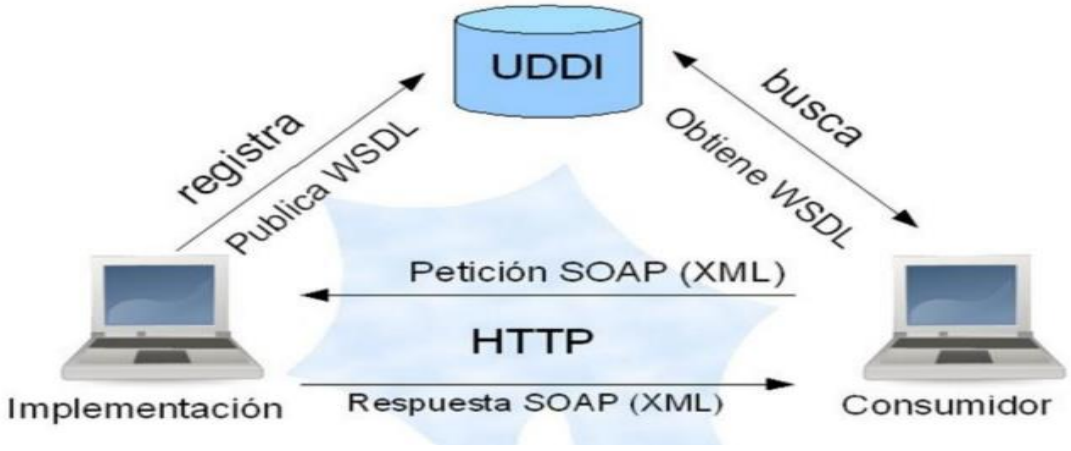
DevSecOps

Es un conjunto de prácticas que combinan el desarrollo de software (Dev), la seguridad (Sec), y las operaciones de tecnología de la información (Ops) para asegurar y acortar el ciclo de vida del desarrollo de software.

Web Services

En el nivel más simple, los servicios web pueden ser vistos como aplicaciones web especializadas que difieren principalmente en la capa de presentación. Mientras que las aplicaciones web son típicamente basadas en HTML, los servicios web son basados en XML/SOAP.

Los servicios Web típicamente representan una interfaz publica funcional, que se llama de forma programática



Web Services - WS-Security – WSS

El estándar WSS lidia con varias áreas medulares de seguridad dejando muchos detalles a los llamados documentos perfil. Las áreas principales, ampliamente definidas por el estándar son:

- Maneras de agregar encabezados de seguridad (encabezados WSSE) a las sabres de SOAP
- Adjuntar testigos de seguridad y credenciales al mensaje
- lnsertando un estampado de tiempo
- Firmar el mensaje
- Cifrado del mensaje
- Extensibilidad

WS-Policy: Describe capacidades y limitaciones de la seguridad, políticas e intermediarios (reglas de seguridad, algoritmos soportados, etc.)

WS-Trust: Describe un framework para para facilitar la interoperaci6n de WS en forma segura.

WS-Privacy: Describe el modelo sobre como las Web Services manejan las peticiones y preferencias de seguridad

WS-SecureConversation: Describe cómo manejar y autenticar el intercambio de mensajes, el contexto de seguridad y claves de sesión.

WS-Federation: Describe como administrar y manejar la relaciones de confianza entre sistemas federados.

WS-Authorization: Describe como administrar la autorización de datos y políticas.

REST

Es una técnica de arquitectura para sistemas distribuidos, su nombre es un acrónimo que deriva de *"Representational State Transfer".*

Su objetivo fue evitar el uso de métodos complejos como CORBA, RPC y SOAP para interconexión de sistemas; con este fin las aplicaciones ReSTFul usan llamados HTTP para las operaciones **CRUD {Create/Read/Update/Delete)** orientando su diseño a elementos en lugar de operaciones.

Unidad N°5: Calidad

Definiciones

- Propiedad o conjunto de propiedades inherentes a un objeto que permiten apreciarlo coma mejor, igual o peor que otros objetos de su especie.
- Conjunto de propiedades y de características de un producto o servicio que le confieren capacidad para satisfacer necesidades expresadas o implícitas.
- Grado en el que un conjunto de características inherentes cumple con las requisitos.

Calidad Total

la Calidad Total es un concepto de gestión de empresa orientada hacia la mejora continuada de los procesos y actividades a través de la participación de todos/as con el objetivo de mejorar el nivel de sensibilización de los/as clientes tanto internos como externos.

- **PLANIFICAR** lo que se pretende alcanzar, incluyendo con ello la incorporación de las observaciones a lo que se viene realizando.
- **HACER** o llevar adelante lo planeado.
- **VERIFICAR** que se haya actuado de acuerdo a lo planeado así como los efectos del plan.
- **ACTUAR** a partir de los resultados a fin de incorporar lo aprendido, lo cual es expresado en observaciones y recomendaciones.

Calidad de Software

Es el conjunto de cualidades que lo caracterizan y determinan su utilidad y existencia. La calidad está asociada a la de eficiencia, flexibilidad, corrección, confiabilidad, mantenibilidad, portabilidad, usabilidad, seguridad e integridad del software.

Calidad de Interna (ISO 9126)

La calidad interna esta especificada por un modelo de calidad, y puede ser medida y evaluada por media de atributos estáticos de documentos tales coma la especificación de requerimientos, arquitectura o diseño; piezas de código fuente, etc. En etapas tempranas del ciclo de vida del software es posible medir, evaluar y controlar la calidad interna de estos productos, pero asegurar la calidad interna no es generalmente suficiente para asegurar la calidad externa.

Calidad de Externa (ISO 9126)

La calidad externa esta especificada también por un modelo de calidad, y puede ser medida y evaluada por medio de propiedades dinámicas del código ejecutable en un sistema de computación, esto es, cuando un módulo o aplicación completa es ejecutado en una computadora o en una red simulando lo más cercanamente posible un ambiente real. En fases tardías del ciclo de desarrollo del software, es posible medir, evaluar y controlar la calidad externa de estos productos ejecutables

Características para la Interna/Externa

- **Funcionalidad**: Adecuación, Exactitud, Interoperabilidad, Seguridad, Conformidad de la funcionalidad.
- **Confiabilidad:** Madurez, Tolerancia a errores, Recuperabilidad, Conformidad de la fiabilidad.
- **Usabilidad:** Entendimiento, Aprendizaje, Operabilidad, Atracción, Conformidad de uso.

- **Eficiencia:** Comportamiento de tiempos, Utilización de recursos, Conformidad de eficiencia.
- **Capacidad de Mantenimiento:** Capacidad de ser analizado, Cambiabilidad, Estabilidad, Facilidad de prueba, Conformidad de facilidad de mantenimiento.
- **Portabilidad:** Adaptabilidad, Facilidad de instalación, Coexistencia, Intercambiabilidad, Conformidad de portabilidad.

Calidad en Uso (IS0 9126)

Es la capacidad de un producto de software de facilitar a usuarios específicos alcanzar metas específicas con eficacia, productividad, seguridad y satisfacción en un contexto especifico de uso. La calidad en uso es la visión de calidad de los usuarios de un ambiente conteniendo software, y es medida sobre los resultados de usar el software en el ambiente, entes que sobre las propiedades del software en sí mismo.

ISO/IEC 25000 SQuaRE

El estándar ISO/IEC 25000 SQuaRE (Software Product Quality Requeriments and Evaluation) provee información para organizar, enriquecer y unificar las series que cubren dos procesos principales: **especificación de requerimientos de calidad del software** y **evaluación de la calidad del software,** soportada par el proceso de medición de calidad del software.

Unidad N°6: Normas

CMM - Capability Maturity Model

El Modelo de Madurez de Capacidades, es un modelo de evaluación de los procesos de una organización, predecesor de CMMI. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute).

Niveles

- Capability Level 1 - Performed Informally
- Capability Level 2 - Planned and Tracked
- Capability Level 3 - Well Defined
- Capability Level 4 - Quantitatively Controlled
- Capability Level 5 - Continuously Improving

Security Base Practices

En total son 22 PAs, es todo lo que importa

CMMI - Capability Maturity Model® Integration

Los modelos CMMI® son colecciones de buenas prácticas que ayudan a las organizaciones a mejorar sus procesos. Estos modelos son desarrollados por equipos de producto con miembros procedentes de la industria, del gobierno y del Software Engineering Institute (SEI).

SSE-CMM - System Security Engineering - CMM

El Modelo de Madurez de Capacidades en la ingeniería de Seguridad de Sistemas es un modelo derivado del CMM y que describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de sistemas.

SAMM - Software Assurance Maturity Model

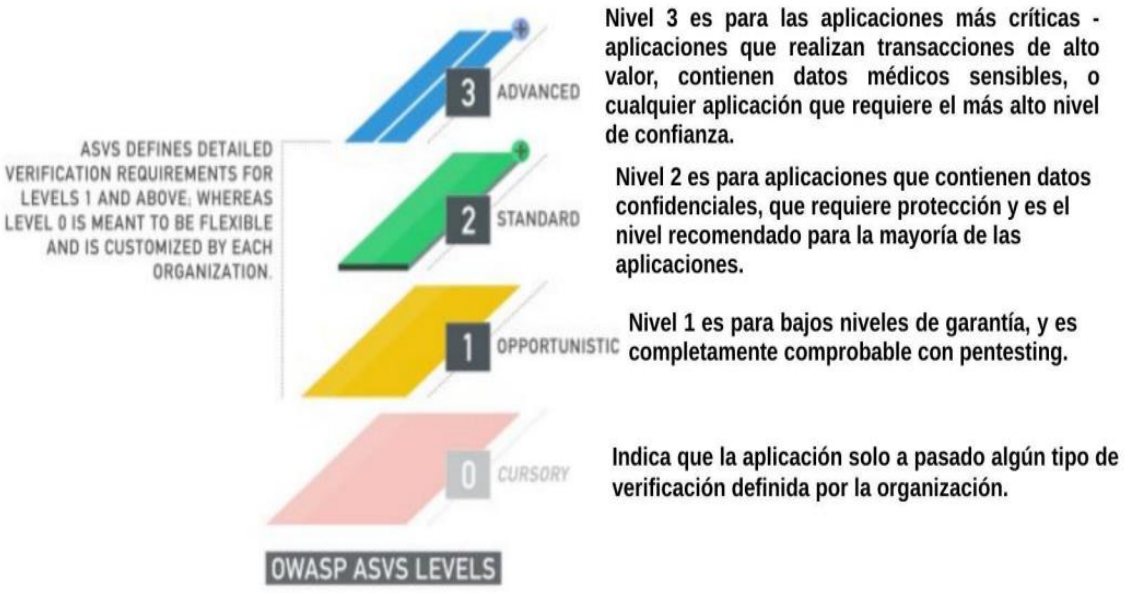
El modelo de madurez para el aseguramiento de software es un marco de trabajo abierto para ayudar a las organizaciones a formular e implementar una estrategia de seguridad para Software que sea adecuada a las necesidades específicas que está enfrentado la organización.

Niveles de madurez

- Nivel 0: Punto de inicio implícito, las actividades en la práctica no se han realizado
- Nivel 1: Entendimiento inicial y provisión ad hoc de la práctica de seguridad
- Nivel 2: Incremento en la eficiencia y/o efectividad de la práctica de seguridad
- Nivel 3: Dominio amplio de la práctica de seguridad

ASVS - Application Security Verification Standard

El objetivo principal del **Application Security Verification Standard (ASVS)** del OWASP es normalizar el rango de cobertura y el nivel de rigurosidad disponible en el mercado cuando se realiza la verificación de seguridad de aplicaciones web. Este estándar podrá ser utilizado tanto por los consumidores como por los proveedores del servicio o la herramienta.



Áreas de Requerimientos de Seguridad

- V1 - Arquitectura, Diseño y Modelado de Amenazas
- V2 - Autenticación
- V3 - Gestión de sesiones
- V4 - Control de Acceso
- V5 - Validación, Desinfección y Codificación
- V6 - Criptografía almacenada
- V7 - Manejo y Registro de Errores
- V8 - Protección de Datos
- V9 - Comunicación
- V10 - Código Malicioso
- V11 - Lógica de Negocio
- V12 - Archivos y Recursos
- V13 - API y Servicios Web
- V14 - Configuración

Normas

- **GDPR,** o "Reglamento General de protección de Datos" define la protección del tratamiento y circulación de los datos de personas físicas pertenecientes a la Unión Europea.
- **CCPA,** "California Consumner Privacy Act" define el control que los consumidores de California tienen sobre la información personal recolectada comercialmente.
- **HIPAA,** o "Health Insurance Portability and Accountability Act", es la ley federal de las Estados Unidos que define las estándares para la protección de la información sensible relativa a la salud de un paciente.
- **A4609** Comunicación del BCRA que define los requisitos mínimos de gestión, implementación, y control de las riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.
- **ISO 9001** en el alcance sobre el software y sobre las procesos productivos de la organización. No siempre sobre el desarrollo, puede ser en la identificación de requisitos, en el propio desarrollo y por ejemplo en la entrega y mantenimiento.
- **ISO/IEC 9003** ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software (NO es CERTIFICABLE. Es una norma de buenas prácticas para definir con más detalle los conceptos de software sobre los procesos de la organización).
- **ISO/IEC 12207**
- **IS0/IEC 15504**
- **IS0/IEC 9126.**
- **ISO/IEC 14598.**
- **ISO 25000.** La familia de normas 25000 establecen un modelo de calidad para el **producto software** además de definir la evaluación de la calidad del producto. Tiene 5

partes publicadas. Pretenden sustituir a ISO 9126 e ISO 14598 ya que desde 2001 no se publicaron nuevas versiones.

- **SCRUM.** No es una **norma,** es un método sencillo y práctico para empezar a practicar calidad. Fabricar y gestionar el desarrollo en tres fases fundamentales: una breve fase de planificación, en la cual se realizan las labores básicas de una planificación breve: visión general del proyecto (estimación muy general, viabilidad del sistema) y construcción del Backlog. por un lado y por otro el desarrollo de la arquitectura al detalle; otra de desarrollo, en la cual tienen lugar las famosos Sprints, y otra final de entrega y balance de los éxitos y fracasos logrados
- **1S0/IEC 27000:** es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC {International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.