UNIDAD 3: CRIPTOGRAFÍA

*Elementos teóricos de la criptografía -> **D(k, E(k, m)) = m***

- ***m** -> Representa el conjunto de todos mensajes sin cifrar (denominado texto plano 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** -> 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 --- CRIPTOGRAFÍA MODERNA:

SUB-CLASIFICACIÓN:

CRIPTOGRAFÍA CLÁSICA:

- *TRASPOSICIÓN:* Estos cifradores utilizan la técnica de permutación de forma que los caracteres del texto se reordenan mediante un algoritmo específico.
- *SUSTITUCIÓN:* Utilizan la técnica de modificación de cada carácter del texto en claro por otro correspondiente al alfabeto de cifrado. Si se usa un solo alfabeto es monoalfabético (cifrado de César) si se usan más de uno es polialfabético.
- *SUSTITUCIÓN POLIALFABÉTICA:* Usan diferentes caracteres (de más de un alfabeto) para el reemplazo de un mismo carácter. Ej Cifrado de Vignere (matriz de alfabetos).

ESQUEMAS DE CODIFICACIÓN:

- *BINARIO* -> Representa la información a nivel de bits con 0 y 1.
- *HEXADECIMAL* -> Representa la información con 16 caracteres con representación gráfica (0123456789ABCDEF) asignando 4 bits a cada carácter.
- *BASE64* -> Representa la información con 64 caracteres representables (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/)

CRITOGRAFÍA MODERNA -> Tiene dos tipos principales de algoritmos en sub-clasificaciones:

ALGORITMOS SIMÉTRICOS -> Tipo de cifrado que utiliza la misma clave tanto para cifrar como para descifrar. Ambas partes deben (emisor y receptor) estar de acuerdo con dicha 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.

/*VER GRÁFICO PARA ENTENDER MEJOR VISUALMENTE*/

ALGORITMOS SIMÉTRICOS DE BLOQUE:

- 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, International Data Encryption Algorithm)
- Blowfish (1993, Bruce Scheiner)
- RC5 (1994, Rivest Cipher 5)

REFERENCIA MATEMÁTICA-XOR

Es conmutativa A xor B = B xor A

Asociativa (A xor B) xor C = A xor (B xor C)

Autoinversa (A xor B) xor B = A

Modos de cifrado de bloques.

ECB *-> Electronic Codebook, el mensaje se fracciona en partes y se cifran independientemente.*

Padding o Esquema de relleno. *-> Método que completa el final de un bloque de datos. Resuelve el problema en algoritmos simétricos de bloque donde el mensaje en su totalidad o en su último bloque tiene una longitud menor a la requerida.*

Bit padding(RFC 1321, ISO/IEC 9797-1) *-> Opera a nivel de bits, agrega 1 y N cantidad de 0*

ISO/IEC 7816-4 *-> Igual que bit padding pero opera a nivel bytes, agrega 80 y N cantidad de 0*

PKCS#7(RFC 2315, Sec 10.3) *-> Opera a nivel bytes, N cantidad de bytes idénticos*

ISO 10126 *-> Opera a nivel bytes, agregar N cantidad de bytes aleatorios hasta el ante último*

ANSI X.923 *-> Opera a nivel bytes, agrega N cantidad de 00 hasta el ante último byte.*

CBC *-> (Cipher Block Chaining). El mensaje se fracciona en partes y se realiza un XOR antes de cifrar cada parte.*

CFB *-> (Cipher Feedback). 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.*

OFB *-> (Output Feedback). Igual al CFB solo que el bloque a ser utilizado como entrada del siguiente proceso es tomado antes de hacerle el XOR*

CTR *-> (Modo de Counter o Contador). Usa un "nonce" que es alterado por un contador incrementado en cada bloque de datos, para luego obtener un valor y aplicarle XOR.*

OTROS MODOS DE CIFRADO DE BLOQUE.

- PCBC
- CCM
- CWC
- EAX
- GCM (Galois Counter Mode)
- PCFB
- XCBC

CIFRADO DE FLUJO -> Se usa 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).

Función generadora de bits pseudo-aleatoria -> Permite obtener secuencias de bits criptográficamente aleatorias.

CIFRADOS DE FLUJO:

- RC4
- Salsa20*
- ChaCha20
- Trivium*
- A5/1, A5/2
- Chameleon
- FISH
- Helix
- Grain
- ISAAC

- MUGI
- Panama
- Phelix
- Pike
- SEAL
- SOBER/SOBER-128
- WAKE
- Rabbit

FUNCIONES DE HASH -> Son funciones o métodos no reversibles que generan 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.

MDC -> Funciones que dan como resultado bloques de longitud fija **a** a partir de bloques desi longitud fija **b** con **a < b**

MAC -> (Message Autentication Code) agrega criptografía al proceso de hash para aumentar la seguridad del mismo.

Tipos de implementaciones:

- *BASADOS EN CIFRADOS POR BLOQUES:* Cifra el mensaje empleando un algoritmo por bloques en modo de operación CBC.
- *HMAC:* Se basa en el uso de cualquier función MDC aplicada sobre una versión del mensaje que tiene un conjunto de bits añadidos.
- *BASADOS EN GENERADORES DE SECUENCIA:* Se emplea un generador de secuencia pseudoaleatorio que parte el mensaje en 2 subcadenas, alimentando cada parte un Registro de Desplazamiento Retroalimentado. El valor MAC se obtiene del estado final de estos registros.

FUNCIONES DE HASH:

- **MD4(Ron Rivest - RSA, Security Inc):** Produce un valor hash de 128 bits. Se considera un estándar de internet (RCF-1320).
- **MD5:** Extensión de MD4, es más lento, pero más seguro. Estándar (RFC-1321).
- **SHA-1(NIST):** Produce un valor de hash de 160 bits. Estándar (FIPS PUB 180-1).
- **SHA-2(NSA Y NIST):** Es un conjunto de algoritmos comprendidos por (SHA-224, SHA-256, SHA384 Y SHA-512).
- **SHA-3(Keccak):** Operación en 224, 256, 384 o 512 bits.
- **RIPEMD-160(Hans Dobbertin, Antoon Bosselaers, Bart Preneel - RIPE):** Genera una salida de 160 bits.

FUNCIONES DE DERIVACIÓN DE CLAVES (KDF – Key Derivation Function): Son funciones no reversibles que tiene 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. Se basan en funciones pseudoaleatoria, funciones hash con múltiples iteraciones y procesos de inclusión de 'Salt'. Evitan ataques de diccionario y tablas de arcoíris.

- **PBKDF2 (2000)-> Password-Based Key Derivation Function 2 RFC-2898 Y (PKCS#5, NIST SP 800-132).**
- **bcrypt (1999) -> Basado en 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 ASIMETRICOS -> Es un sistema de cifrado de clave pública que usa un par de claves para el envío de mensajes (ambas pertenecen a la misma persona a la que se ha enviado el mensaje). Una de las claves es **pública** y puede entregarse a cualquier persona, y la otra es **privada** y se debe guardar bien pues se usa para descifrar el mensaje. Los remitentes usan la clave publica para cifrar el mensaje a el destinatario y este lo descifra con la clave privada.

ALGORITMO ASIMETRICO – DIFFIE HELLMAN -> Algoritmo que permite compartir un mensaje cifrado entre dos actores sin contacto previo. Suele usarse para acordar una clave de cifrado por un canal inseguro y sin autenticación.

Caso de uso: Diffie-Hellman permite que dos partes acuerden una clave compartida sin compartir sus claves privadas directamente. Ambas partes generan valores públicos y privados, intercambian los públicos y calculan una clave compartida. Aunque los valores públicos son compartidos abiertamente, la clave resultante solo puede ser calculada por las partes que conocen sus valores privados.

EJEMPLOS DE ALGORITMOS ASIMETRICOS:

- **Diffie-Hellman**
- **RSA**
- **ElGamal**
- **DSA**
- **ECC, Criptografía de curva elíptica (ECDH, ECDSA...)**

CIFRADO ->

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 la firma*/

AUTENTICACIÓN ->

Autenticación de mensaje (Firma) -> Algunos algoritmos asimetricos 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, al reves de la simple codificación de mensajes.

RSA (Ronald Rivest, Adi Sharmir, Leonard Adleman - 1977) -> Se basa en la dificultad de factorizar grandes números.

Generación de claves:

Se eligen dos números primos grandes, **p** y **q**.

Se calcula el producto **n = p x q**, y se obtiene la función totiente de Euler ϕ (**n**) = **(p - 1) x (q - 1)**

Se elige un número **e** (usualmente un número primo relativo a ϕ (**n**)) como clave de cifrado pública.

Se calcula **d** de manera que **d x e** ≡1(mod ϕ (**n**))d×e≡1(modϕ(n)); **d** se mantiene como clave de descifrado privada.

Cifrado:

El remitente utiliza la clave de cifrado pública **(e,n)** para cifrar el mensaje **M** como **C≡M¨e(mod n)**

Descifrado:

El destinatario utiliza la clave de descifrado privada **(d,n)** para descifrar el mensaje cifrado **C** como **M≡C4(mod n)**

ElGamal -> Se basa en la dificultad de factorizar grandes números (el problema de los logaritmos discretos) **(y = log disc a(X))**

Generación de claves:

Elija un número primo p y un generador g.

Cada parte elige una clave privada x y calcula la clave pública y ≡ g^x (mod p)**.**

Cifrado:

El remitente elige k y calcula c1 ≡ g^k (mod p) y c2 ≡ M * y^k (mod p), donde M es el mensaje.

Descifrado:

El destinatario usa sus claves privada y pública para calcular s ≡ c1^x (mod p).

Obtiene el inverso multiplicativo de s y lo usa para descifrar M ≡ c2 * s (mod p).

ElGamal es un algoritmo de clave pública utilizado para el intercambio seguro de claves y la firma digital.

DSA (DIgital Signature Algorithm – DSS – FIPS-186, propuesto por NIST en 1991) -> Es una variante del método asimetrico ElGamal.

Generación de claves:

Elija un número primo grande p.

Seleccione un número g que genere un subgrupo de orden primo.

Cada entidad elige una clave privada x y calcula la clave pública y ≡ g^x (mod p).

Firma:

Elija un número efímero k y calcule r ≡ (g^k mod p) mod q, donde q es un divisor primo de p-1.

Calcule s ≡ k^(-1)(H(M) + x * r) mod q, donde H(M) es el hash del mensaje M.

Verificación:

Verifique que 0 < r < q y 0 < s < q.

Calcule w ≡ s^(-1) mod q.

Calcule u1 ≡ H(M) * w mod q y u2 ≡ r * w mod q.

Calcule v ≡ (g^(u1) * y^(u2) mod p) mod q.

La firma es válida si v = r.

ALGORITMOS PÚBLICOS Y PRIVADOS:

- **PÚBLICOS ->** Su definición y funcionamiento están a la disposición pública, permitiendo que cualquiera pueda acceder al mismo para su evaluación y/o investigación.

- **PRIVADOS ->** Su funcionamiento interno es desconocido. En el ámbito de la criptografía, estos son considerados menos confiables.

HTTP VS HTTPS

HTTP -> Hyper Text Transfer Protocol, protocolo para transmición de información en plano, sin cifrado. Su puerto por defecto es el 80.

HTTPS -> Hyper Text Transfer Protocol Secure, protocolo para transmición de información cifrada mediante SSL o TLS. Su puerto por defecto es 443.

SSL (Secure Socket Layer) (Netscape - 1996) -> Protocolo que proporciona privacidad e integridad entre dos aplicaciones, es independiente del protocolo utilizado. Garantiza la seguridad de los datos y se ubica entre la capa de la aplicación y la capa de transporte (como por ej, TCP).

Los datos que circulan en ambos sentidos entre cliente-servidor se cifran mediante un algoritmo simetrico como DES o RC4 y un algoritmo de clave pública como RSA se usa para el intercambio de claves de cifrado y firmas digitales.

Las versiones 1 y 2 del SSL solo proporcionan autenticación del servidor, la version 3 proporciona la autenticación del cliente usando los certificados digitales del cliente y del servidor.

FASES.

1-Establecimiento de la conexión y negociacion de los algoritmos criptograficos que van a usarse en la comunicación.

2-Intercambio de clabes, empleando algun mecanismo de clave publica y autentificación a partir de sus certificados digitales.

3-Cifrado simetrico de trafico

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

CARACTERISTICAS ADICIONALES.

- Incompatible con SSL v3.0.
- Uso de funciones MAC en lugar de solo MDC.
- Numeración secuencial de todos los campos que componen la comunicación.
- Protección frente a ataques que intentan forzar el empleo de versiones antiguas (inseguras).
- El mensaje final de la conexión incorpora una signatura hash de todos los datos intercambios por los interlocutores.

ALGORITMOS UTILIZADOS.

- Cifrado Asimétrico -> RSA, Diffie Hellman (DHE), Curva Eliptica (ECDHE), DSA.
- Cifrado Simétrico -> RC2, RC4, IDEA, DES, TRIPLE DES o AES.
- Funciones de Hash -> MD5 o de la familia SHA.

VERSIONES.

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

FIRMA ELECTRÓNICA -> Es un conjunto de datos electronicos integrados, ligados o asociados de manera logica a otros datos electronicos, utilizado por el signatario como su medio de identificación carente de requisitos legales para ser considerada firma digital.

FIRMA DIGITAL -> Es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante. La firma digital debe ser susceptible de verificación por terceras partes, tal que se permita identificar al firmante y detectar cambios en el documento posterior a su firma.

PROPIEDADES.

- **Va ligada indisolublemente al mensaje.**
- **Solo puede ser generada por su legítimo titular.**
- **Es publicamente verificable.**

MODELOS DE INFRAESTRUCTURA DE SEGURIDAD

PKI – INFRAESTRUCTURA DE CLAVE PÚBLICA: Es una combinación de hardware, software, politicas y procedimientos de seguridad que define un entorno de confianza centralizado y provee garantias para operaciones criptograficas como el cifrado, la firma digital o el no repudio de transacciones electronicas.

CERTIFICADOS DIGITALES -> 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 o información accesoria 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 publica 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 -> Se usan cuando una clave pública pierde validez y es necesario anularla. No son más que un mensaje que identifica a la clave pública que se desea anular, firmada por la clave privada correspondiente.

PKI – COMPONENTES:

- *Autoridad de Certificación.*
- *Autoridad de Registro.*
- *Autoridad de Validación.*
- *Autoridad de Sellado de Tiempo.*
- *Los repositorios.*
- *Los usuarios y entidades finales.*

OCSP (Online Certificate Status Protocol): 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: Modelo de confianza distribuido que provee garantías para operaciones criptográficas basado en la cantidad de firmas de actores.

LEY DE FIRMA DIGITAL – REPUBLICA ARGENTINA -> Ley 25.506.

CERTIFICADORES LICENCIADOS.

- **AFIP**
- **ANSES**
- **ONTI**
- **ENCODE S.A**

UNIDAD 4: APLICACIONES DE SEGURIDAD

LOGGING -> Su finalidad se vincula a:

- Identificar incidentes de seguridad.
- Monitorear violaciones de politicas.
- Asistir en controles de no-repudio
- Provee información sobre problemas o situaciones atipicas

- 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 la detección de ataques.

¿Dónde registrar? -> Sistemas de archivos, almacenamiento en la nube, bases de datos SQL y NoSQL.

¿Qué registrar? -> Fallos de validación, autenticación, autorización, anomalías, fallas de aplicación, eventos legales.

¿Qué NO registrar? -> Código fuente, identificadores de sesion, credenciales y tokens de acceso, claves de cifrado, SPI...

ENMASCARAMIENTO DE DATOS -> Proceso por el cual se reemplazan los datos sensibles de un sistema con el objetivo de proteger la información confidencial ante situaciones que se salgan de control. ”Seudonimización" es el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado.

DEBILIDADES ASOCIADAS AL LOGGING:

- CWE - 117 Improper Output Neutralization for Logs
- CWE - 223 Omission of Security-relevant Information.
- CWE - 532 Insertion of Sensitive into Log File.
- CWE - 778 Insufficient Logging.

VALIDACIÓN DE ENTRADA -> Debe cubrir los aspectos semánticos como sintácticos de la información ingresada. (Se sugiere implementar validación “**White List**” para validar el ingreso de datos, describiendo el tipo de dato como listas de valores o expresiones regulares).

EXPRESIONES REGULARES DE VALIDACIÓN DE ENTRADA POR TIPOS:

URL -> (esto va al final de la expresión como en todas) -> [[:blank:]])?$.

IP -> [0-9]?)$.

EMAIL -> [a-zA-Z]{2,7}$.

NUMEROS -> ocho|nueve)$.

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 mediante el uso de una credencial.

- Proveyendo controles de autenticación razonables de acuerdo al riesgo de la app.
- Denegando el servicio a atacantes que usan varios métodos para atacar el sistema de autenticación.

CONSIDERACIONES GENERALES.

- La autenticación es solo tan fuerte como sus procesos de administración de usuarios.
- Use la forma más adecuada de autenticación apropiada para su clasificación de bienes.
- Re-autenticar al usuario para transacciones de alto valor y acceso a areas protegidas.
- Autenticar transaccion, no al usuario.
- Contraseñas trivialmente rotas, no son adecuadas en sistemas de alto valor.

BUENAS PRACTICAS.

- **User IDs -> Verificar que no sean CASE SENSITIVE.**
- **Fortaleza de Contraseñas -> Long min de 10 caracteres y max de 20.**
- **Implementar metodos seguros de recuperación.**
- **Almacenar contraseñas de forma segura > soporte criptografico.**
- **Transmitir contraseñas solo sobre TLS.**
- **Solicitar re-autenticación -> Antes de operaciones sensibles.**
- **Utilizar sistemas de autenticación de factor múltiples.**
- **Manejo de mensajes de error -> mensajes genericos.**
- **Prevenir ataques por fuerza bruta -> Captchas o controles de comportamiento.**

METODOS DE PROTECCIÓN ANTE ATAQUES DE AUTOMATIZACIÓN.

- *MFA o Autenticación de Factor Multiple.*
- *Bloqueo de cuenta*
- *CAPTCHA*
- *Preguntas de seguridad o palabras memorables.*

CONTRASEÑAS DE UN SOLO USO.

- **OTP:** One Time Password, 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:** Timed-based One Time Password, valor confidencial que no puede ser reutilizado y cuenta con tiempo de vida acotado. RFC-6238.

TECNICAS DE AUTENTICACIÓN DE USUARIOS.

- *A.Básica y segura (HTTP-Basic, HTTP-Digest)*

- *A.Basada en formularios (Usuario-contraseña)*
- *A.Integrada (ISS, ASP.NET, Active Directory)*
- *A.Basada en certificado (x509)*
- *A.Fuerte o de factor multiple.(algo que eres, que sabes que tienes, ubicación)*

JWT – JSON WEB TOKEN -> Es un estándar abierto (RFC-7519) utilizado para transmitir de forma segura información en formato JSON, está compuesto por: El encabezado que especifica tipo de token y algoritmo de firma, la carga util que contiene los datos relevantes y la firma que verifica la integridad del token. Se utilizan para la autenticación y autorización.

OBJETIVOS - AUTORIZACIÓN EN LA WEB:

- Asegurar que los usuarios realicen acciones permitidas de acuerdo a sus privilegios.
- Controlar el acceso a recursos protegidos mediante decisiones basadas en rol o privilegios de usuarios.
- Prevenir ataques de escalada de privilegios.

METODOS DE CONTROL DE ACCESO

ROLE BASES ACCESS CONTROL (RBAC) -> Las decisiones de acceso se basan en las funciones y responsabilidades de un individuo dentro de la organización o base de usuarios. Generalmente la definición de funciones está basada en objetivos y estructura de la organización. Ej una organización médica, roles de médico, enfermo, asistente, etc.

DISCRETIONARY ACCESS CONTROL (DAC) -> Medio para restringir el acceso a la información sobre la base de la identidad de los usuarios y/o la pertenencia a ciertos grupos. Las decisiones están basadas en las autorizaciones concebidas por el usuario con sus credenciales al momento de la autenticación. Ej El sistema de archivos de un sistema Unix (rwx)

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 lo compara con el nivel de sensibilidad de los usuarios. Ej. Aplicaciones militares (extremadamente seguro).

ATTRIBUTE BASED ACCESS CONTROL (ABAC) -> Sistema de control basado en atributos asignados a cualquier componente del sistema (recurso, usuarios, etc). Se utiliza un lenguaje de soporte como XACML para definir las reglas de acceso.

BUENAS PRACTICAS DE IMPLEMENTACIÓN:

- **Codificar el control en la actividad objetivo.**
- **Disponer de un Controlador Centralizado (ACL)**
- **Utilizar un Control Central de Acceso, en las diferentes capas.**

- **Verificar la política del lado del servidor (Server-Side)**

ATAQUES DE CONTROL DE ACCESO.

- **VERTICAL ACCESS CONTROL ATTACKS:** Un usuario convencional obtiene accesos superiores o de administrador.
- **HORIZONTAL ACCESS CONTROL ATTACKS:** Con el mismo rol o nivel, el usuario puede acceder a información de otros usuarios.
- **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 administrativo estan segregadas apropiadamente de la actividad del usuario**
- **Los usuarios no pueden acceder o utilizar funcionalidades administrativas**
- **Proveer la necesaria auditoría y trazabilidad de funcionalidad administrativa.**

DevSecOps -> Conjunto de prácticas que combinan el desarrollo de software (Dev), la seguridad (Sec) y las operaciones de la tecnología de la información (Ops) para asegurar y acortar el ciclo de vida del desarrollo de software.

WEB SERVICES -> Aplicaciones web especializadas que difieren en la capa de presentación, basados en XML/SOAP.

COMITÉS DE ESTÁNDARES.

- **W3C, Estandares de esquema XML (XML Schema), SOAP (Simple Object Access Protocol), XML-dsig, XML-enc, WSDL.**
- **OASIS, estándares de WS-Security.**
- **OASIS, UDDI (Universal Description Discovery and Integration).**
- **OASIS, SAML (Security Assertion MarkUp Language).**
- **Grupo de interoperabilidad de servicios Web.**

Los servicios web típicamente representan una interfaz pública funcional, que se llama de forma pragmática.

WS-Security-WSS -> El estándar WSS lidia con varias medulares de seguridad, las principales son.

- Encabezados WSSE a los sobres SOAP.
- Adjuntar testigos de seguridad y credenciales al mensaje.
- Insertando un estampado de tiempo.

- Firmar el mensaje
- Cifrado del mensaje
- Extensibilidad

- **WS-POLICY**
- **WS-TRUST**
- **WS-PRIVACY**
- **WS-SECURECONVERSATION**
- **WS-FEDERATION**
- **WS-AUTHORIZATION**

REST (Representational State Transfer)-> Técnica de arquitectura para sistemas distribuidos. Su origen data del año 2000 por Roy Fielding.

Su objetivo fue evitar el uso de metodos complejos como CORBA, RPC y SOAP para la interconexión de sistemas, por ello usan llamados HTTP para operaciones CRUD.

REQUEST -> http://server.net/hola/Mundo

PLAIN RESPONSE -> Hola Mundo!

XML RESPONSE -> <datos> Hola Mundo! </datos>

UNIDAD 5: CALIDAD

DEFINICIONES:

- **Propiedad o conjunto de propiedades inherentes a un objeto que permiten apreciarlo como mejor, igual o peor que otros objetos de su especie (DRAE).**
- **Conjunto de propiedades ycaracteristicas de un producto o servicio que le confieren capacidad para satisfacer necesidades expresadas o implícitas (ISO8042:1994)**
- **Grado en el que un conjunto de características inherentes cumple con los requisitos (ISO9000:2000)**

CALIDAD TOTAL POR DEMING:

- **PLANIFICAR ->** Lo que se pretende alcanzar, incluyendo la incoporación de las observaciones a lo que se viene realizando.
- **HACER ->** Llevar adelante lo planeado.

- **VERIFICAR ->** Que se haya actuado de acuerdo a lo planeado asi 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 -> Conjunto de cualidades que lo caracterizan y determinan su utilidad y existencia. Está asociada a la eficiencia, flexibilidad, corrección, confiablidad, mantenibilidad, portabilidad, usabilidad, seguridad e integridad del software. La calidad del software es medible. Ej. Un software elaborado para el control de naves debe tener calidad "cero fallas".

CALIDAD DE INTERNA (ISO 9126) -> Está especificada por un modelo de calidad, y puede ser medida y evaluada por medio de atributos estáticos de documentos tales como la especificación de requerimientos, arquitectura o diseño; piezas de codigo fuente, etc. (Se evalúa en fases tempranas del ciclo de vida del software)

CALIDAD DE EXTERNA (ISO 9126) -> Está 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 (Se puede manejar en fases tardías del ciclo de desarrollo de software).

CARACTERISTICAS PARA LA INTERNA/EXTERNA.

- **FUNCIONALIDAD**
- **CONFIABILIDAD**
- **USABILIDAD**
- **EFICIENCIA**
- **CAPACIDAD DE MANTENIMIENTO**
- **PORTABILIDAD**

CALIDAD EN USO (ISO 9126) -> Sus propiedades son (Eficacia, Productividad, Satisfacción, Seguridad)

SQuaRE CARACTERISTICAS CONTEMPLADAS-> (Funcionalidad, Mantenibilidad, Portabilidad, Eficiencia, Usabilidad, Fiabilidad).

UNIDAD 6: NORMAS

CMM (Capability Maturity Model) -> Es un modelo de evaluación de los procesos de una organización, predecesor de CMMI.

CMMI (Capability Maturity Model Integration) -> Son colecciones de buenas prácticas que ayudan a las organizaciones a mejorar sus procesos.

SSE-CMM (System Security Engineering Capability Maturity Model) -> Modelo derivado del CMM que describe las caracteristicas esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de sistemas. PD: Tiene definido 22 PAs

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*

SAMM (Software Assurance Maturity Model) -> Marco de trabajo abierto para ayudar a las organizaciones a formular e implementar una estrategia de seguridad para software que se adecue a sus necesidades.

FUNCIONES ->

- **Gobierno**
- **Diseño**
- **Implementación**
- **Verificación**
- **Operaciones**

Niveles de madurez SAMM-> {0,1,2,3}

ASVS – Application Security Verification Standard -> El objetivo principal es normalizar el rango de cobertura y el nivel de rigurosidad disponible en el mercado cuando se realiza la verificación de seguridad en aplicaciones web.

ASVS – OWASP LEVELS.

- **0 – CURSORY -> Indica que la app ha pasado por algun tipo de verificación (sin detalles)**
- **1 – OPPORTUNISTIC -> Para bajos niveles de garantía, comprobable con pestenting.**
- **2 – STANDARD -> Para apps que contienen datos confidenciales, requieren protección, es el mas recomendado para la mayoría de aplicaciones.**
- **3 – ADVANCED -> Para apps más críticas que realizan transacciones de alto valor, apps que requieran el más alto nivel de confianza.**

ASVS – AREAS 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: Define la protección del tratamiento y circulación de los datos de personas físicas pertenecientes a la Unión Europea.

CCPA: Define el control que los consumidores de California tienen sobre la información personal recolectada comercialmente.

HIPAA: Ley Federal de los EE. UU que define los estándares para la protección de la información sensible relativa a la salud de un paciente.

PCI DSS: Estándar de seguridad que establece revisiones de cumplimiento anuales o trimestrales con diferentes métodos en función del volumen de operaciones manejadas, como: SAQ, QSA, ISA.

- **A4609:**
- **ISO 9001:**
- **ISO/IEC 9003:**
- **ISO/IEC 12207:**
- **ISO/IEC 15504:**
- **ISO/IEC 9126:**
- **ISO/IEC 14598:**
- **ISO 25000:**
- **SCRUM:** NO es una normal, es un método sencillo y práctico para empezar a practicar calidad, consta de tres fases fundamentales. PLANIFICACIÓN - VISIÓN GENERAL - CONSTRUCCIÓN BACKLOG.