Principios de ciberseguridad

Miguel Solinas

Departamento de Computación

Julio XX22

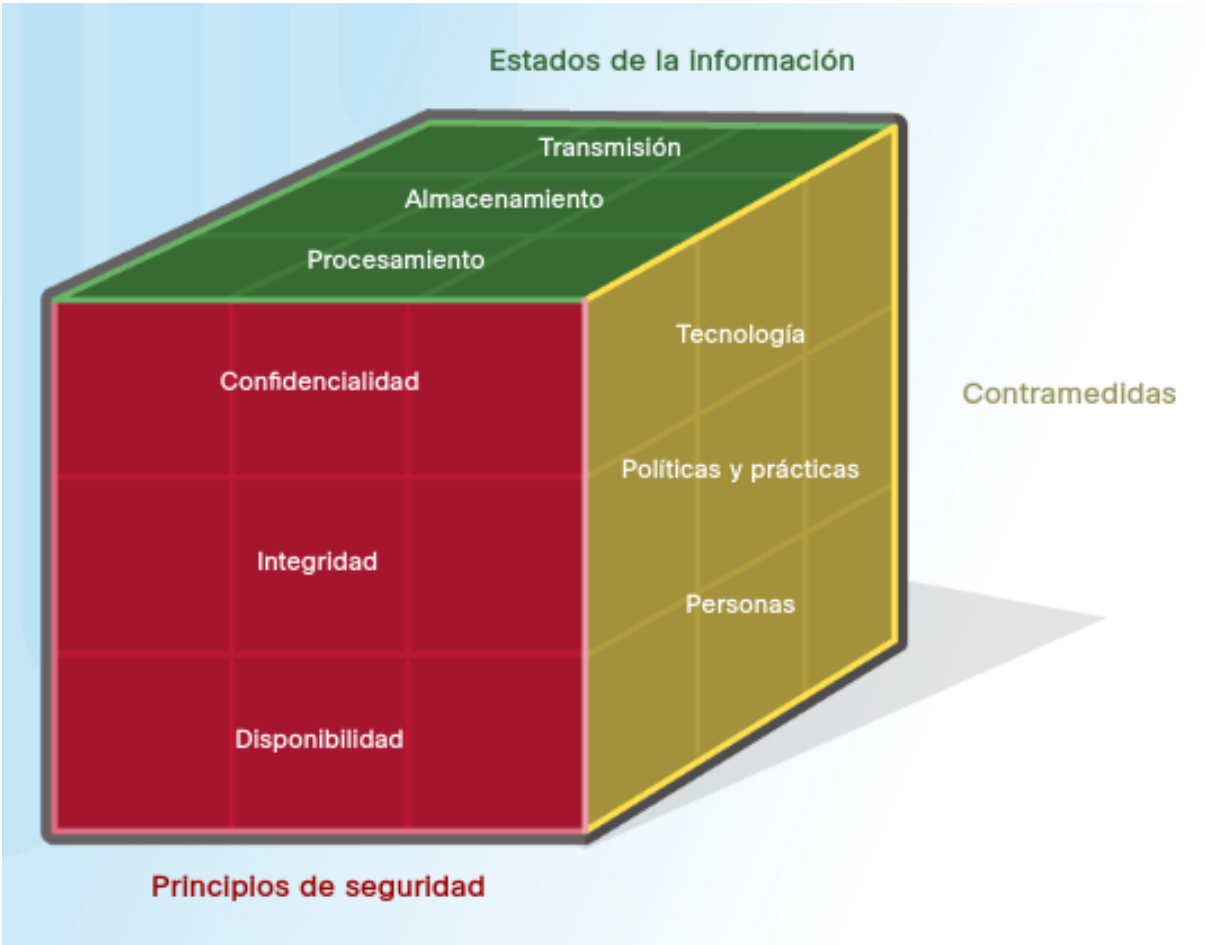
Ministerio de Desarrollo Productivo Argentina

UTD Unidades de Transformación Digital

FCEFyN FACULTAD DE CIENCIAS EXACTAS, FÍSICAS y NATURALES

SECRETARÍA DE EXTENSIÓN

Cubo de destrezas de ciberseguridad



Principios de seguridad

Confidencialidad

Impide el acceso a la información a las personas/recursos/procesos no autorizados. Otro término para la confidencialidad es el de privacidad.

Principios de seguridad

Confidencialidad

Impide el acceso a la información a las personas/recursos/procesos no autorizados. Otro término para la confidencialidad es el de privacidad.

Integridad

Previene que personas/recursos/procesos no autorizados modifiquen la información. Precisión, uniformidad y confiabilidad de los datos durante su ciclo de vida.

Principios de seguridad

Confidencialidad

Impide el acceso a la información a las personas/recursos/procesos no autorizados. Otro término para la confidencialidad es el de privacidad.

Integridad

Previene que personas/recursos/procesos no autorizados modifiquen la información. Precisión, uniformidad y confiabilidad de los datos durante su ciclo de vida.

Disponibilidad

Es el principio que se utiliza para describir la necesidad de mantener la disponibilidad de los sistemas y servicios de información en todo momento.

Estados de la información

Tránsito

La información esencialmente se comunica a través de internet. Redes SOHO, empresas, wifi, datos inalámbrico, WAN, Starlink, etc...

Estados de la información

Tránsito

La información esencialmente se comunica a través de internet. Redes SOHO, empresas, wifi, datos inalámbrico, WAN, Starlink, etc...

Almacenamiento

Hace referencia a los diferentes medios donde puede almacenarse información. Desde un simple pendrive, RAM, discos de estado sólido, nube, celulares, GPS, autos, cámaras digitales, etc...

Estados de la información

Tránsito

La información esencialmente se comunica a través de internet. Redes SOHO, empresas, wifi, datos inalámbrico, WAN, Starlink, etc...

Almacenamiento

Hace referencia a los diferentes medios donde puede almacenarse información. Desde un simple pendrive, RAM, discos de estado sólido, nube, celulares, GPS, autos, cámaras digitales, etc...

Procesamiento

La información se procesa en diferentes dispositivos utilizando memoria RAM. PCs, notebook, celulares, servidores, autos, etc...

Contramedidas

Tecnología

Tecnología con base en el software, en el hardware, en la red o en la nube.

Contramedidas

Tecnología

Tecnología con base en el software, en el hardware, en la red o en la nube.

Políticas y buenas practicas

Las políticas de seguridad son un conjunto de objetivos de seguridad para una organizacoión que incluye entre otras cosas, reglas de comportamiento de usuarios y administradores y tratamiento de los datos.

Contramedidas

Tecnología

Tecnología con base en el software, en el hardware, en la red o en la nube.

Políticas y buenas practicas

Las políticas de seguridad son un conjunto de objetivos de seguridad para una organizacoión que incluye entre otras cosas, reglas de comportamiento de usuarios y administradores y tratamiento de los datos.

Personas

Es fundamental la capacitación de todas los recursos humanos dentro de una empresa.

Hablemos un poco mas de principios de seguridad

No se puede hablar genéricamente de "seguridad", sino de principios o servicios de seguridad:

Servicio de seguridad

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación
- Firma Digital

¿ Cómo materializar estos servicios ?

La criptografía es la solución

No nació con internet. Tiene mas de 2.000 años de desarrollo y lo que hoy utilizamos son algoritmos de criptografía moderna.

Tipos de criptografía

- Clave simétrica o clave secreta
- Clave asimétrica o clave pública
- Funciones de hash

Criptografía simétrica

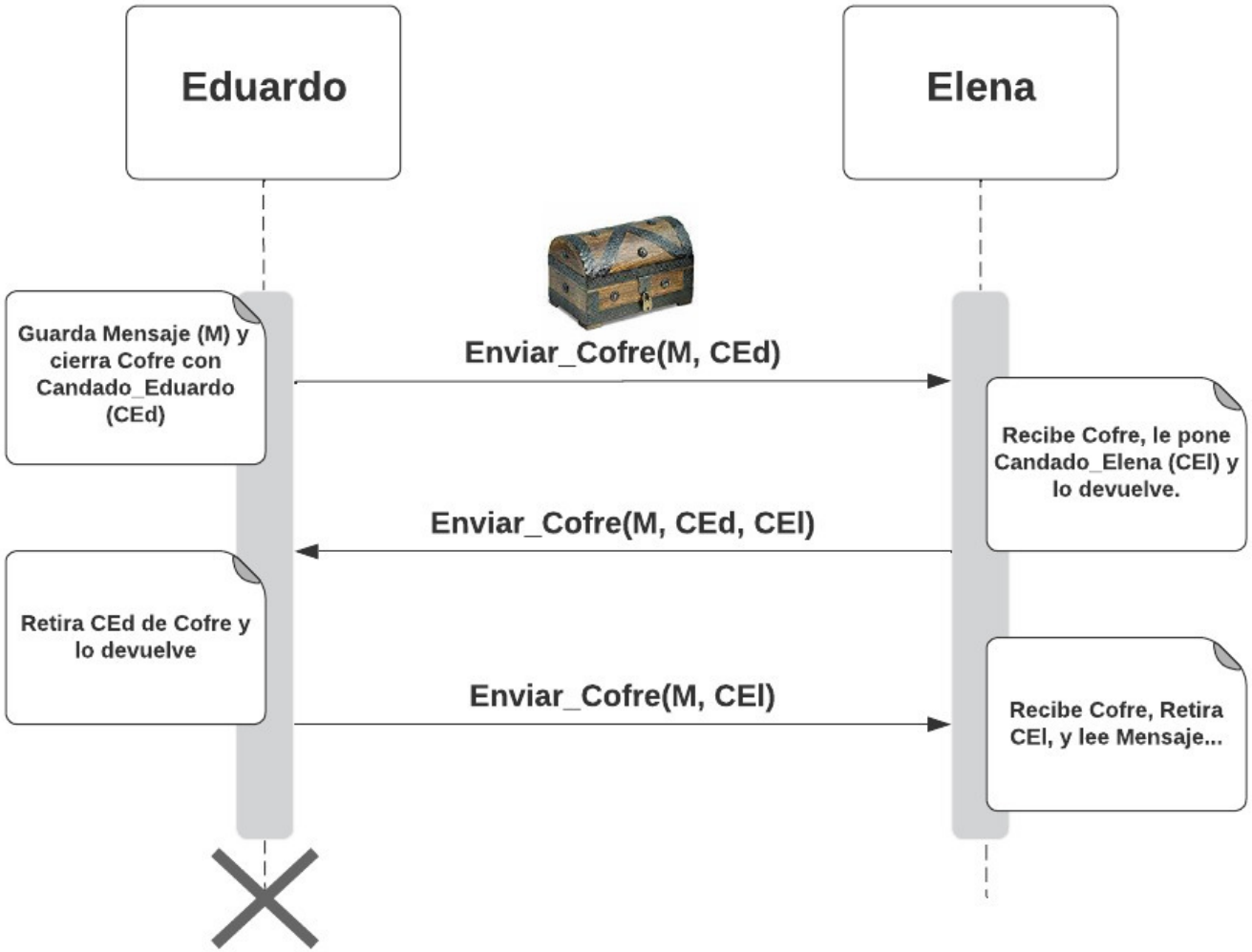
Uno de los primeros registros criptográficos corresponden a la Cifra del Cesar utilizada en la guerra de las Galias 50 a.C.

Algoritmos y principios

- Cifra Cesar, Vignerere, Enigma
- DES, 3DES, IDEA, AES, Blowfish, Camellia
- La seguridad no reside en ocultar los principios del algoritmo
- La clave es la fortaleza
- Distribuir claves no es un problema menor
- N(N-1)/2
- Uso de AESCrypt
- https://encode-decode.com/

Confidencialidad sin intercambio de clave

¿ Es posible intercambiar mensajes de forma confidencial s/utilizar clave ?



Criptografía asimétrica

Oficialmente nace a finales de los '70 con trabajos de investigación de **Whitfield Diffie**, Martin Hellman, Ralph Merkle, Taher Elgamal. Ron Rivest, Adi Shamir y Leonard Adleman crean el algoritmo RSA.

Algoritmos y principios

- Cada usuario se suma al "sistema" con dos claves
- Una pública y una privada

Criptografía asimétrica

Oficialmente nace a finales de los '70 con trabajos de investigación de **Whitfield Diffie**, Martin Hellman, Ralph Merkle, Taher Elgamal. Ron Rivest, Adi Shamir y Leonard Adleman crean el algoritmo RSA.

Algoritmos y principios

- Cada usuario se suma al "sistema" con dos claves
- Una pública y una privada
- Ambas claves están vinculadas matemáticamente
- La clave privada se guarda en un lugar seguro
- La clave pública se hace pública

Criptografía asimétrica

Oficialmente nace a finales de los '70 con trabajos de investigación de **Whitfield Diffie**, Martin Hellman, Ralph Merkle, Taher Elgamal. Ron Rivest, Adi Shamir y Leonard Adleman crean el algoritmo RSA.

Algoritmos y principios

- Cada usuario se suma al "sistema" con dos claves
- Una pública y una privada
- Ambas claves están vinculadas matemáticamente
- La clave privada se guarda en un lugar seguro
- La clave pública se hace pública
- N*2 vs N(N-1)/2

Criptografía asimétrica

Oficialmente nace a finales de los '70 con trabajos de investigación de **Whitfield Diffie**, Martin Hellman, Ralph Merkle, Taher Elgamal. Ron Rivest, Adi Shamir y Leonard Adleman crean el algoritmo RSA.

Algoritmos y principios

- Cada usuario se suma al "sistema" con dos claves
- Una pública y una privada
- Ambas claves están vinculadas matemáticamente
- La clave privada se guarda en un lugar seguro
- La clave pública se hace pública
- N*2 vs N(N-1)/2
- Es la base del comercio electrónico
- ¿ Han escuchado hablar de Certificados Digitales ?

Criptografía asimétrica

Oficialmente nace a finales de los '70 con trabajos de investigación de **Whitfield Diffie**, Martin Hellman, Ralph Merkle, Taher Elgamal. Ron Rivest, Adi Shamir y Leonard Adleman crean el algoritmo RSA.

Algoritmos y principios

- Cada usuario se suma al "sistema" con dos claves
- Una pública y una privada
- Ambas claves están vinculadas matemáticamente
- La clave privada se guarda en un lugar seguro
- La clave pública se hace pública
- N*2 vs N(N-1)/2
- Es la base del comercio electrónico
- ¿ Han escuchado hablar de Certificados Digitales ?
- Veamos un CD con el navegador.!!

Funciones de HASH

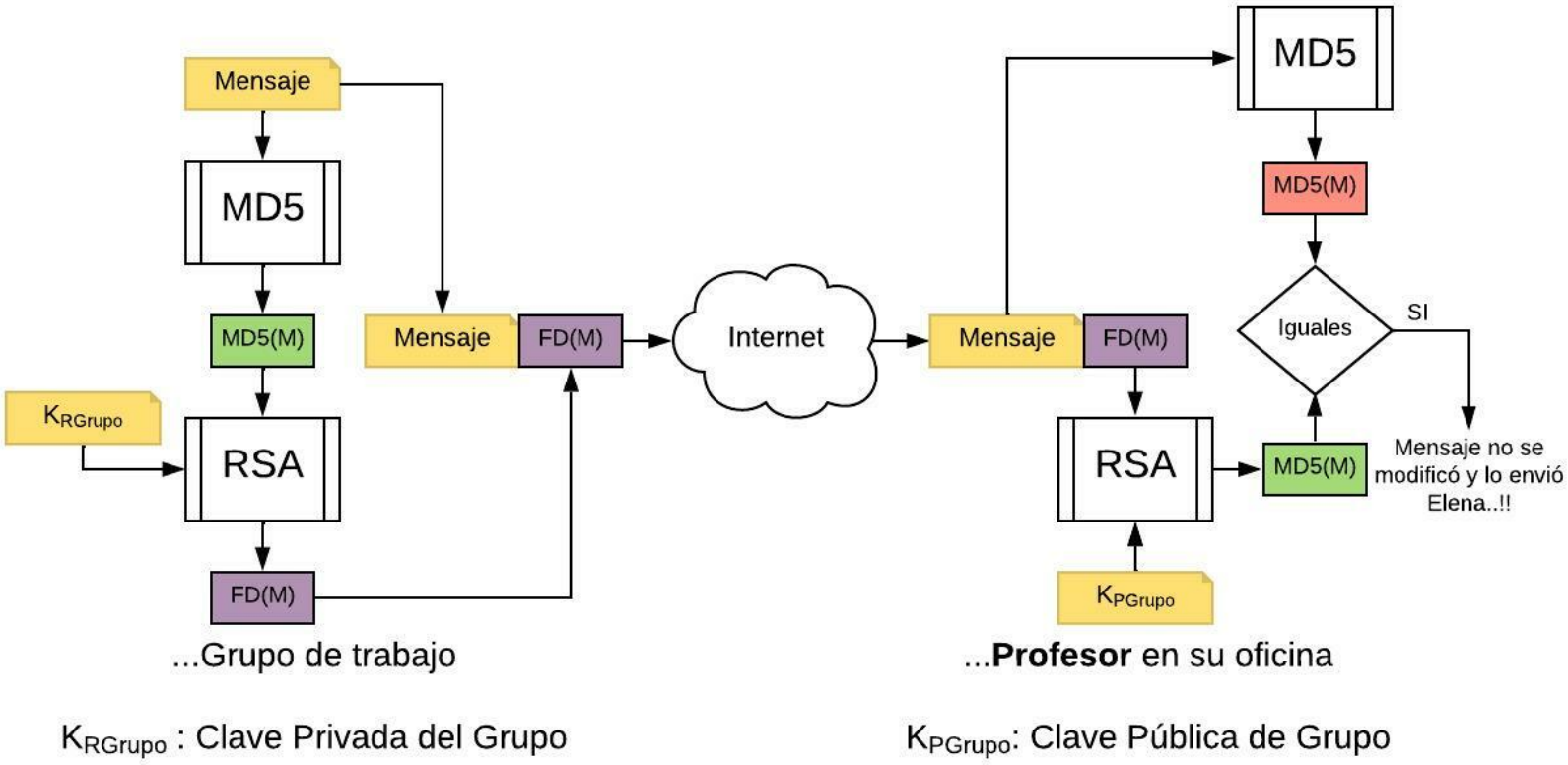
Son funciones matemáticas que reducen un mensaje a un digesto pequeño de longitud fija.

Algoritmos y principios

- MD5, SHA-0, SHA-1, SHA-256
- No es posible recuperar el mensaje original a partir del digesto
- Se utilizan para brindar servicios de INTEGRIDAD
- Uso de GtkHash, HashCalc (W), otros para controlar integridad de archivos
- https://encode-decode.com/

Firma Digital

Ahora podemos comprender que Firma Digital es un servicio que brinda autenticación e integridad..!!



Veamos un ejemplo con los CD del navegador.!!

Infraestructuras de Clave Pública

Para desplegar el funcionamiento de un sistema de clave pública es necesario una PKI.

Componentes de una PKI

- Autoridad de Certificación (AC)
- Autoridad de Registro (AR)

Infraestructuras de Clave Pública

Para desplegar el funcionamiento de un sistema de clave pública es necesario una PKI.

Componentes de una PKI

- Autoridad de Certificación (AC)
- Autoridad de Registro (AR)
- Lista de Certificados Revocados (CRL)
- Online Certificate Status Protocol (OCSP)

Infraestructuras de Clave Pública

Para desplegar el funcionamiento de un sistema de clave pública es necesario una PKI.

Componentes de una PKI

- Autoridad de Certificación (AC)
- Autoridad de Registro (AR)
- Lista de Certificados Revocados (CRL)
- Online Certificate Status Protocol (OCSP)
- Un marco legal (Ley de Firma Digital AR - 25.506)

Infraestructuras de Clave Pública

Para desplegar el funcionamiento de un sistema de clave pública es necesario una PKI.

Componentes de una PKI

- Autoridad de Certificación (AC)
- Autoridad de Registro (AR)
- Lista de Certificados Revocados (CRL)
- Online Certificate Status Protocol (OCSP)
- Un marco legal (Ley de Firma Digital AR - 25.506)
- Un Framework Open Source como EJBCA
- Un paper para comenzar : **Implementación de una PKI con herramientas de software libre** en ResearchGate

Infraestructuras de Clave Pública

Para desplegar el funcionamiento de un sistema de clave pública es necesario una PKI.

Componentes de una PKI

- Autoridad de Certificación (AC)
- Autoridad de Registro (AR)
- Lista de Certificados Revocados (CRL)
- Online Certificate Status Protocol (OCSP)
- Un marco legal (Ley de Firma Digital AR - 25.506)
- Un Framework Open Source como EJBCA
- Un paper para comenzar : **Implementación de una PKI con herramientas de software libre** en ResearchGate
- ¿ Hay entidades licenciadas en AR ? Si, **aquí**..!!

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) es una extensión del protocolo Hypertext Transfer Protocol (HTTP).

¿ Qué tiene que ver con PKI ?

- Trabajando con el navegador preferido
- Visitemos un sitio seguro
- Busquemos el "candado" en la barra de navegación
- Intentemos encontrar el CD asociado
- Identifiquemos a quién pertenece
- Fecha de vigencia, clave pública, emisor
- Vamos a encontrar una firma digital
- ¿ podemos explicar de qué se trata y cómo la utiliza el navegador ?

Resumen de lo visto

1. Cubo de destrezas de ciberseguridad
2. Principios de seguridad
3. Estados de la información
4. Contramedidas
5. Principios/servicios de seguridad
6. Criptografía
7. Criptografía simétrica
8. Criptografía sin claves
9. Criptografía asimétrica
10. Funciones de HASH
11. Firma Digital
12. Infraestructura de Clave Pública o PKI
13. HTTPS

Muchas gracias