T2.1: Arquitecturas, Servicios y mecanismos de seguridad

Garantía y Seguridad de la Información.

T2.1: Arquitecturas, Servicios y mecanismos de seguridad

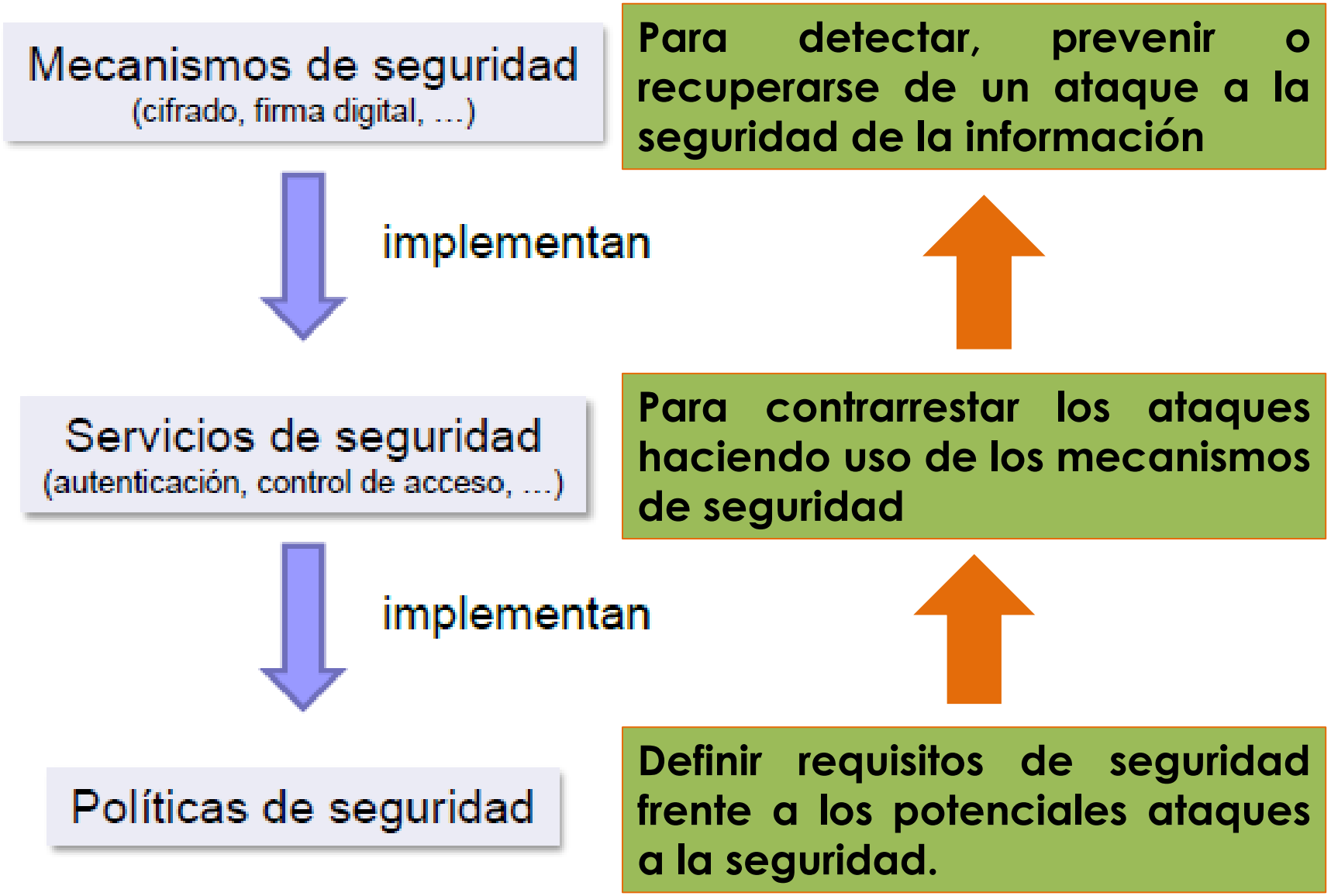
Introducción: Arquitecturas

Arquitecturas de Seguridad

- Las organizaciones y las empresas:
  - Manejan información confidencial que almacenan en sus SI..
  - Desean proporcionar acceso personalizado, confidencial y protegido.
  - Proporcionan acceso a través de red a sus SI para que los clientes, proveedores, inversores, puedan disponer de información o productos.
  - Facilitan ventas a través de internet que deberían ser seguras: confidencialidad, integridad, autenticación, disponibilidad.
  - Deben disponer de infraestructura basada en certificación electrónica para poder emitir facturas.

- **La implantación y gestión de la seguridad en los sistemas de información es una necesidad**.

- **Es necesario diseñar una arquitectura que dé soporte a estas necesidades de seguridad.**


Mecanismos de seguridad
(cifrado, firma digital, …)
implementan
Para detectar, prevenir o recuperarse de un ataque a la seguridad de la información
Servicios de seguridad
(autenticación, control de acceso, …)
implementan
Para contrarrestar los ataques haciendo uso de los mecanismos de seguridad
Políticas de seguridad
Definir requisitos de seguridad frente a los potenciales ataques a la seguridad.

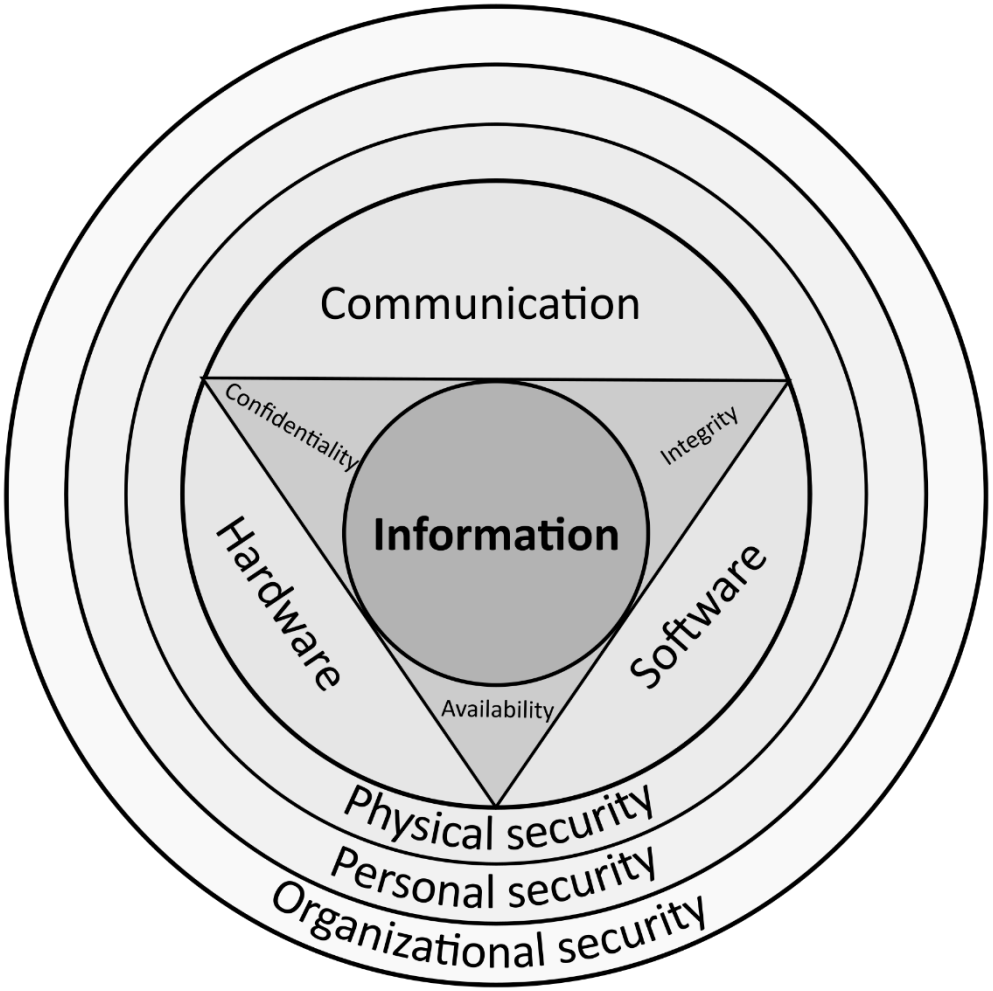
Arquitectura de seguridad: Definición

- Representaciones Físicas y Lógicas de un Sistema (Vistas) (NIST-800)
  - Relevantes para la seguridad:
  - Muestran cómo se estructura el sistema en dominios
  - Muestran cómo se hace uso de elementos relevantes para la seguridad para garantizar políticas de seguridad dentro y entre los dominios, basándose en cómo se deben proteger datos e información.

- La arquitectura de seguridad representa:
  - Los dominios de seguridad
  - La ubicación de los elementos relevantes para la seguridad dentro de esos dominios
  - Las interconexiones y relaciones de confianza entre elementos de seguridad
  - Comportamiento e interacción entre elementos de seguridad.

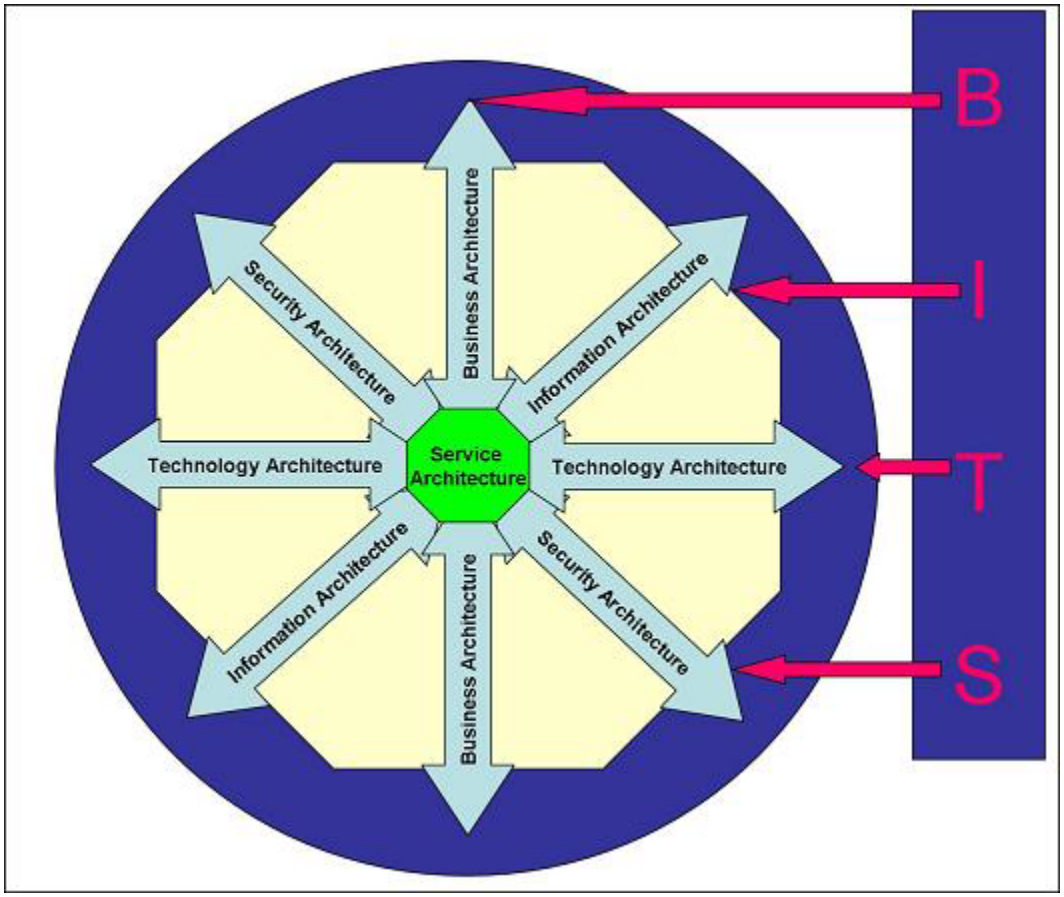
- Puede expresarse a diferentes niveles de abstracción y alcances.

EJ: InfoSec Architectural View



By Michel Bakni - This file was derived from: CIAJMK1209.png, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=114986828

EJ2: BITS: EISA (Enterprise Information Security Architecture)



T2.1: Arquitecturas, Servicios y mecanismos de seguridad

Arquitecturas de Referencia: OSI X.800

Arquitectura de seguridad de Internet

- Internet se diseñó con el foco puesto en **garantizar conectividad**.
- **Arquitectura de capas TCP/IP**:
  - Cuatro niveles: Físico-Enlace > Red > Transporte > Aplicación
  - Facilita la **interconexión de redes locales a través de encaminadores (routers)**.
    - Cada una de las capas de la arquitectura TCP/IP tiene una misión en el transporte de la información.
    - Hay mecanismos y servicios de comunicaciones en cada nivel de la arquitectura
  - **No diseñado para soportar servicios de seguridad.**
  - Hay que especificar una arquitectura de seguridad que permita utilizar la arquitectura TCP/IP para la incorporación de servicios de seguridad.

Arquitectura de seguridad: Definiciones

- Arquitectura de las comunicaciones
  - Servicios de seguridad a las aplicaciones distribuidas.
- Servicios de seguridad
  - Los servicios de seguridad son capacidades funcionales que intentan contrarrestar las amenazas a la seguridad
  - Protegen la información en tránsito procedente de esas aplicaciones.
  - Se implementan mediante mecanismos de seguridad.
- Los mecanismos de seguridad son los medios para proporcionar estos servicios de seguridad

OSI X.800: Arquitectura de Seguridad Estándar OSI

- Contenida en el OSI X.800 y el estândar ISO 7498
  - Define los elementos que deben incorporarse para que las comunicaciones entre **sistemas abiertos** estén protegidas.
  - Proporciona **descripción de los servicios de seguridad** y de **los mecanismos asociados.**
    - Son los proporcionados por el modelo de referencia OSI.
  - Define el **nivel dentro del modelo de referencia** donde se deberían proporcionar los mecanismos y servicios OSI.

T2.1: Arquitecturas, Servicios y mecanismos de seguridad

Servicios de Seguridad

Servicios de seguridad

- Definición (NIST):
  - **Una capacidad que sirve de soporte para uno o más objetivos de seguridad.**

- Los **servicios de seguridad clave** (históricos) son:
  - autenticación
  - autorización (control de acceso)
  - integridad de datos
  - confidencialidad
  - no repudio

  - Disponibilidad (compuesto)

- Otros:
  - Gestión de claves

Servicios Seguridad: Autenticación

- Garantiza que alguien es quien dice ser (auténtico).

- Mecanismos:
  - login/password
  - huella dactilar, otros rasgos biométricos
  - certificado digital, …

  - Composición de varios mecanismos

Servicios Seguridad: Autenticación …

- Seguridad de que una comunicación es auténtica.
- Comunicación no orientada a conexión

  (un mensaje de correo)
  - asegurar al receptor que el mensaje viene de la fuente que dice ser.
- Comunicación orientada a conexión

  (una conexión TCP)
  - Al iniciarse la comunicación, cada entidad es la que reclama ser.
  - Durante la conexión, las unidades de datos no son suplantadas por un intruso.

- Mecanismos de firma digital e intercambio de autenticación.

Servicios de Autenticación

- Autenticación PAR–ENTIDAD
  - Autenticación de las identidades de los sujetos que se comunican (en el establecimiento de la comunicación).
- Autenticación DE ORIGEN DE LOS DATOS
  - Confirma el sujeto de donde provienen los datos (es de carácter unilateral, al contrario que el anterior).
- Autenticación DE USUARIO
  - Confirma/valida la identidad de un sujeto humano cuando se conecta a un sistema informático.

Autenticación completa

- Además, es garantía de que las unidades de datos intercambiadas son *actuales*
  - no son un retransmisión de unidades de datos capturadas anteriormente por un intruso.

- Mecanismos como el desafío-respuesta y sellos de tiempo

Servicios Seguridad: Autorización/Control de acceso

- Evita el acceso no autorizado a un recurso

- Mecanismos
  - Grupos
  - Roles
  - Matrices de acceso
  - Directorios
  - Listas de control de acceso: ACLs

Servicios Seguridad: Autorización/Control de acceso

- Capacidad de limitar y controlar el acceso a los sistemas y aplicaciones a través de los enlaces de comunicaciones.
- Cada entidad debe ser identificada o autentificada.
- Los derechos de acceso se confeccionan de forma individual.

Servicios de Control de acceso

- Debe de proporcionar tres servicios esenciales (**triple A**)
  - Autenticación (Authentication)
    - Quién puede acceder
  - Autorización (Authorization)
    - Qué puede hacer un usuario
  - Trazabilidad (Accountability)
    - Identificar qué ha hecho un usuario

Servicios Seguridad: Integridad de los datos

- Garantiza que los datos se reciben tal y como son enviados.
  - no duplicación, no inserción, no modificación, no reordenación ni destrucción.

- Mecanismos:
  - Hash
  - Firma digital

Integridad

- No alteración de la información en tránsito.
  - Aplicable a un flujo de mensajes, un solo mensaje o un conjunto de campos dentro de un mensaje.
- Orientada a conexión
  - Los mensajes son recibidos tal y como son enviados, sin duplicación, inserción, modificación, reordenamiento, retransmisiones ni destrucción.
- No orientada a conexión (mensajes individuales)
  - Sólo protección frente a las modificaciones.
- Detección mas que prevención.

Servicios de Integridad

- EN CONEXIÓN, CON RECUPERACIÓN:
  - detecta fallo de integridad y recupera la información original.
- EN CONEXIÓN, SIN RECUPERACIÓN:
  - detecta únicamente el fallo de integridad.
- EN LA CONEXIÓN, POR CAMPOS:
  - aplica el servicio de integridad sólo a ciertas partes del mensaje.
- EN COMUNICACIONES, SIN CONEXIÓN:
  - servicio de integridad para un único bloque.
  - debería detectar problemas de reenvíos

Servicios Seguridad: Confidencialidad

- Protección de los datos de su revelación no autorizada

- Mecanismos:
  - Cifrado simétricos
  - Cifrado asimétrico

Confidencialidad

- Protección de los datos transmitidos de los ataques pasivos.
- Técnica de Prevención

- Comunicación orientada a conexión
  - protección de todos los datos transmitidos o sólo de un único mensaje o sólo de campos específicos dentro de un mensaje.
- Protección frente al análisis del flujo de tráfico.
  - Un intruso no puede observar el origen y el destino, la frecuencia, la longitud y otras características del tráfico.

- Mecanismos de cifrado, tráfico de relleno y control de encaminamiento

Servicios de Confidencialidad

- CON CONEXIÓN:
  - protege todos los datos en una conexión.
- SIN CONEXIÓN:
  - protege la información enviada en un único bloque de información.
- POR CAMPOS:
  - se selecciona qué partes de la comunicación se desea proteger
- DE FLUJO DE INFORMACIÓN:
  - protege el flujo de comunicación de ser observado y analizado.

Servicios Seguridad: No repudio

- Evita que emisor o receptor nieguen la transmisión o la recepción de un mensaje, respectivamente.

- Mecanismo:
  - Firma digital
  - Autoridades de Certificación (notarización)

No Repudio

- Evita que las entidades en una conexión nieguen haber transmitido o recibido un mensaje.
  - **No repudio en origen**: prueba que un mensaje ha sido enviado por una entidad específica.
  - **No repudio en destino**: prueba que el mensaje ha sido recibido por una entidad específica.
- Mecanismos de firma digital y autenticación

Disponibilidad (Availability)

- Propiedad de un sistema de ser accesible y utilizable bajo demanda por una entidad autorizada, de acuerdo con las especificaciones de rendimiento del sistema.

- X.800 trata a la disponibilidad como un propiedad asociada con varios servicios de seguridad.

Disponibilidad (Availability)

- Un servicio de *disponibilidad* protege un sistema para asegurar su *disponibilidad*.
  - Seguridad sobre los ataques por denegación de servicio.

- Depende del servicio de *control de acceso* y otros servicios de seguridad.

T2.1: Arquitecturas, Servicios y mecanismos de seguridad

Mecanismos de Seguridad

Mecanismos de seguridad: Definición

- Cualquier proceso (o un dispositivo que incorpora un proceso) que está diseñado para detectar, prevenir o recuperarse de un ataque de seguridad.

- No hay un único mecanismo que soporte todos los servicios de seguridad requeridos.

- Sin embargo, hay un elemento que es común a muchos de los mecanismos: las técnicas criptográficas.

Mecanismos de seguridad: Referencias (I)

- **Cifrado**: algoritmos matemáticos que transforman información a un formato no inteligible.
  - servicio de confidencialidad en la distribución de datos
  - servicio de no repudio
  - servicio de confidencialidad (la distribución de claves de sesión)
- **Firma digital**: adición de datos o transformación a una unidad de datos que permite que el receptor verifique el origen y la integridad de dicha unidad de datos
- **Control de acceso**: Variedad de mecanismos que refuerzan los derechos de acceso a los recursos

Mecanismos de seguridad: Referencias (II)

- **Integridad de datos**: variedad de mecanismos que aseguran la integridad de una unidad de datos o un flujo de unidades de datos

- **Mecanismos de autenticación**: Mecanismos que aseguran la identidad de todos los participantes en una interacción mediante el intercambio de información.
  - intercambio de una serie de información de control constituyendo un *protocolo de autenticación*

Mecanismos de seguridad: Referencias (y III)

- **Relleno de tráfico**: inserción de bits en huecos dentro de un flujo de datos para frustrar el análisis de tráfico

- **Control de *enrutamiento***: Selección de rutas **físicas** para el envío de información, propiciando el uso de rutas alternativas antes posibles brechas de seguridad

- **Notarización**: uso de un tercero confiable para asegurar ciertas propiedades en el intercambio de datos.

Servicios vs. mecanismos

	Cifrado	Firma Digital	Control Acceso	Integridad de datos	Interc. de autenticación	Relleno de tráfico	Control enrutamiento	Notarización
Autenticación	✓	✓			✓			
Control de Acceso			✓					
Confidencialidad	✓					✓	✓	
Integridad	✓	✓		✓				
No Repudio		✓		✓				✓
Disponibilidad				✓	✓			

Referencias

- Base:
  - Capítulo 3 del Jacobs
  - X.800 y NIST 800

- Ver Campus virtual