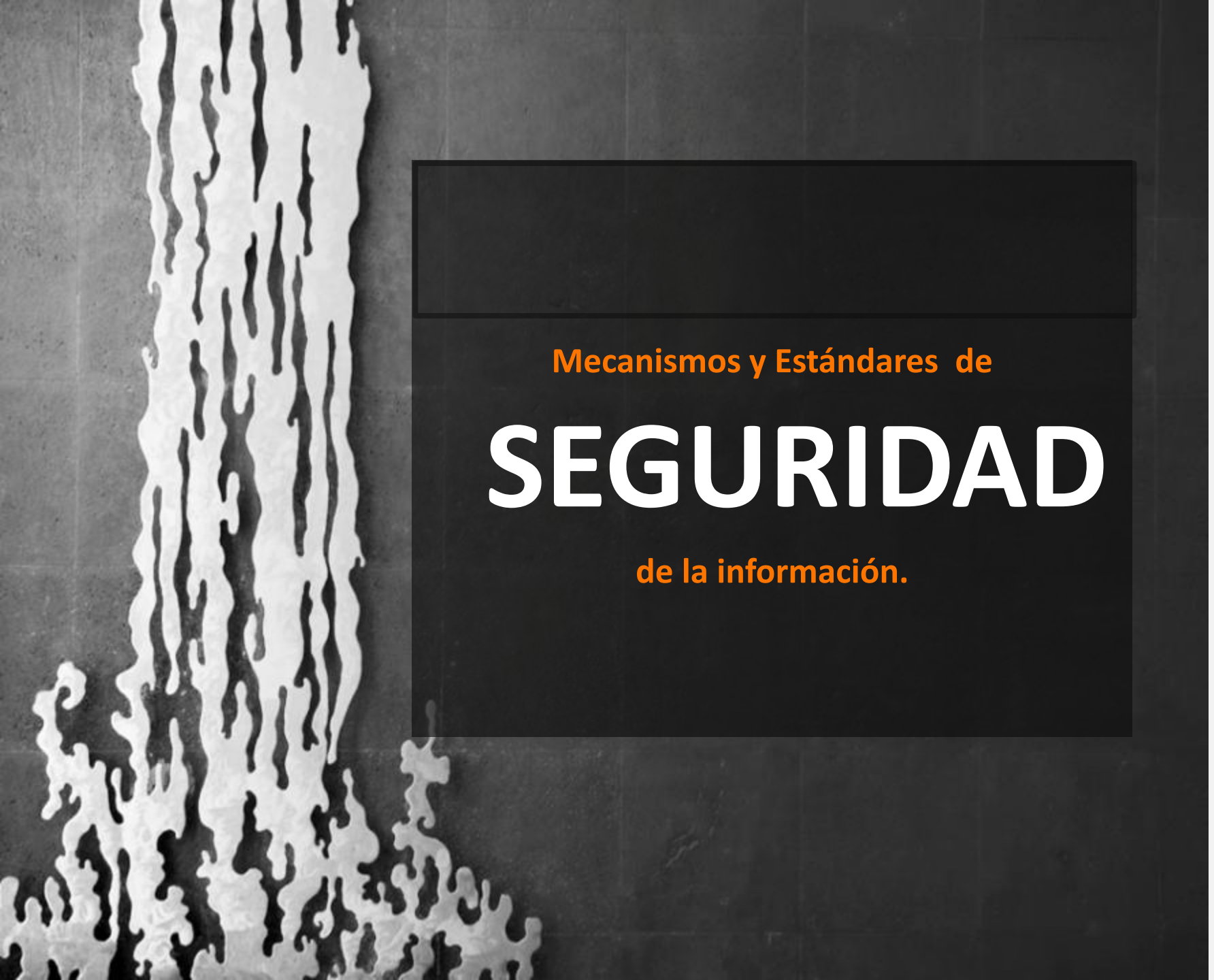


Mecanismos y Estándares de

SEGURIDAD

de la información.

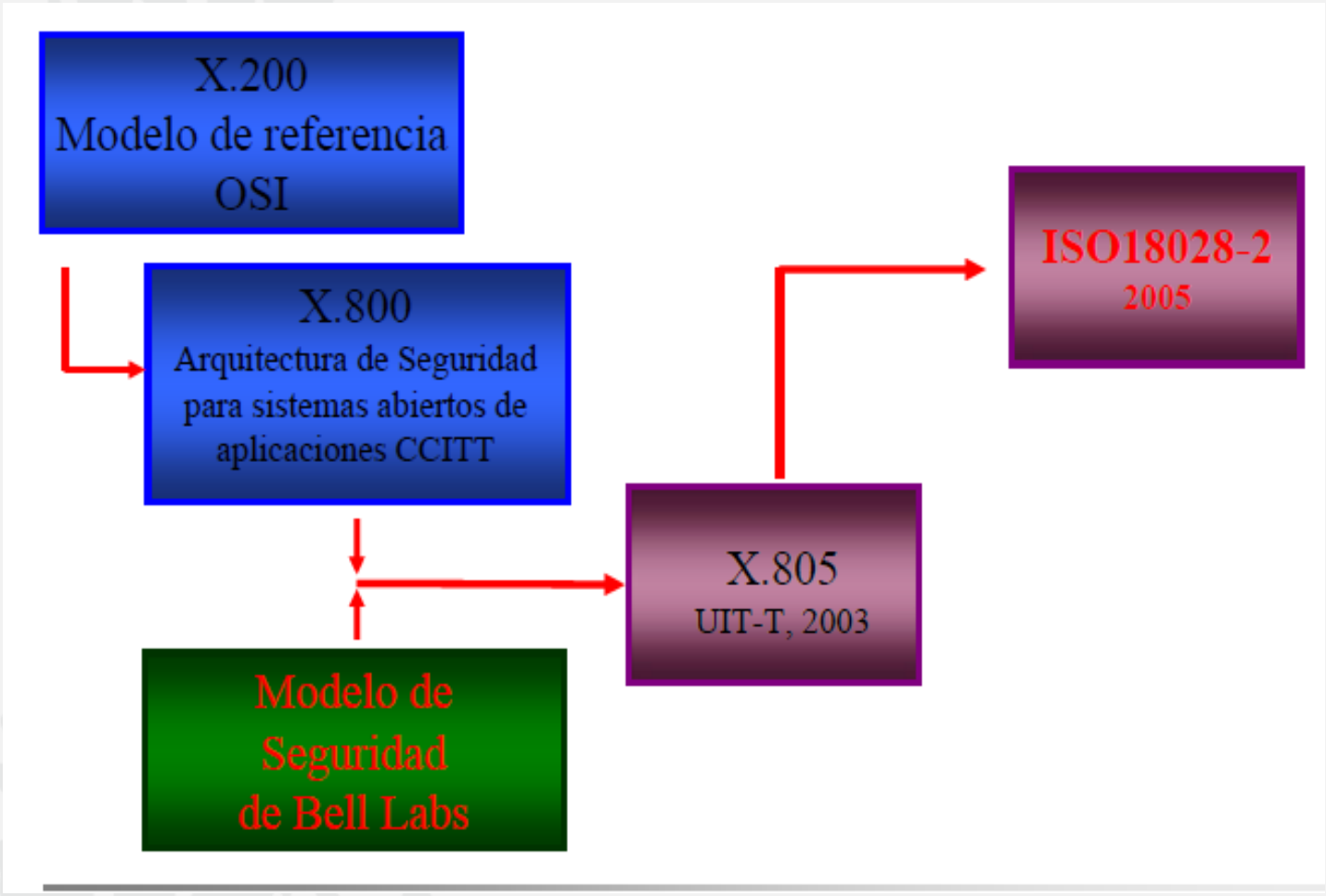
Estándar

X.805

Estándar X.805

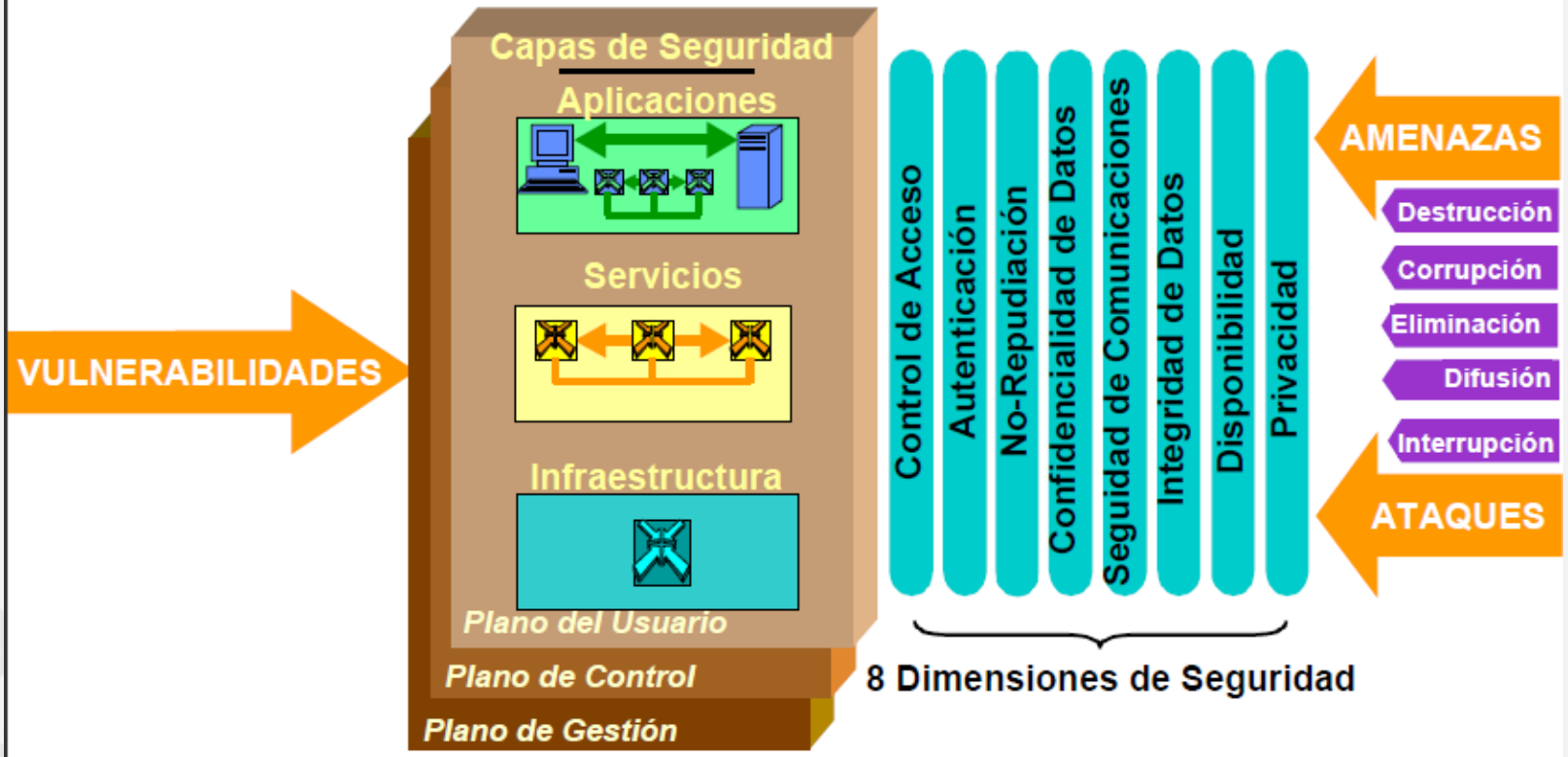
En la Rec. UIT-T X.805 se define el marco para la arquitectura y las dimensiones que garantizan la seguridad extremo a extremo de aplicaciones distribuidas. Si bien los principios y definiciones generales allí tratados son válidos para todas las aplicaciones, los detalles relativos a, por ejemplo, las amenazas y vulnerabilidades y las medidas para contrarrestarlas o preverlas dependen de cada aplicación.

- Es la metodología sistemática para implementar una red segura.
- Consta de tres capas, tres planos y 8 dimensiones de seguridad
- Organiza la complejidad de una red en requerimientos más gestionables
- Abarca la totalidad de la red, considerando todos sus elementos
- Un enfoque común conlleva a un entendimiento cabal
- Promueve la estandarización como factor esencial para lograr la
- interoperabilidad en un entorno de varios proveedores
- Tres interrogantes que reciben respuesta
- ¿Qué protección requiero y contra qué amenazas?
- ¿Qué tipos de elementos de red debo proteger y de qué manera?
- ¿Qué actividades en la red debo proteger?


X.200
Modelo de referencia OSI
X.800
Arquitectura de Seguridad para sistemas abiertos de aplicaciones CCITT
ISO18028-2
2005
X.805
UIT-T, 2003
Modelo de Seguridad de Bell Labs

ISO 18028-2 (X.805):

Un Esquema Completo de Seguridad de Redes



Los Bell Laboratories proporcionaron los cimientos para la elaboración de las normas de seguridad de la industria

CAPA DE INFRAESTRUCTURA

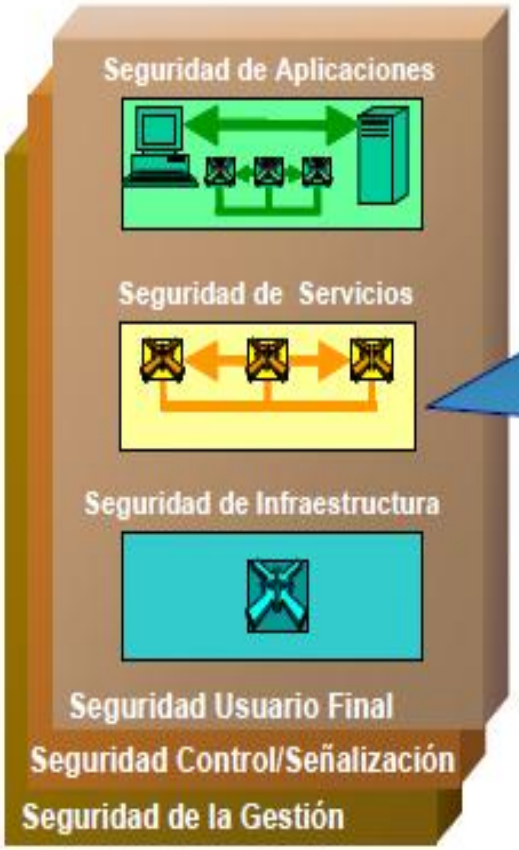
1 – Nivel de Infraestructura de Seguridad:

Estructura base para los servicios de red y aplicaciones.

Ejemplos:

- routers, switches, servidores
- Enlaces WAN punto a punto
- Enlaces Ethernet

- **Cada nivel de seguridad tiene vulnerabilidades y amenazas especificas**
- **La Infraestructura de seguridad habilita la seguridad de los servicios que a su vez habilita la seguridad en las aplicaciones**



2 - Nivel de Seguridad de Servicios:

Servicios a ser provistos para los usuarios finales.

Ejemplos:

- Frame Relay, ATM, IP
- Celular, Wi-Fi,
- VoIP, QoS, IM,
- Toll free call services

3 – Nivel de Seguridad de Aplicaciones:

Aplicaciones basadas en red accedidas por los usuarios finales

Ejemplos:

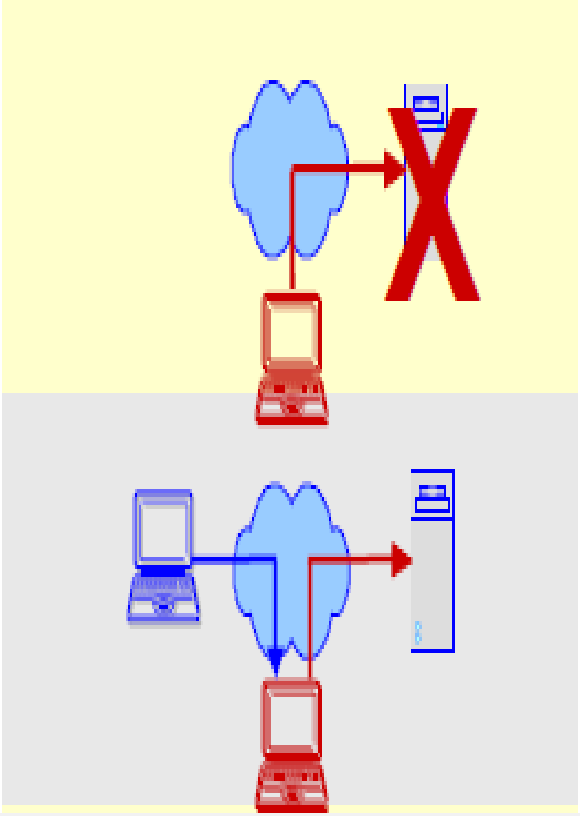
- Web browsing
- Email
- E-commerce

- Cuales son los diferentes tipos de actividades de red que requieren protección?

Modelos de Amenaza

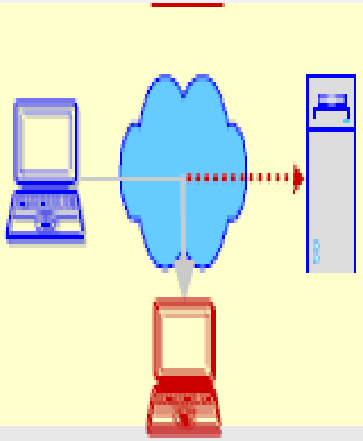
1. Destrucción (Se ataca la disponibilidad):
   - Destrucción de la información y/o de otro recursos de la red
   - Ejemplo: (1) Destrucción de un equipo

2. Corrupción (Se ataca la integridad):
   - Acceso no autorizado a un activo
   - Ejemplos: (1) Cambios a la configuración de la red
     (2) Cambios a los datos transmitidos



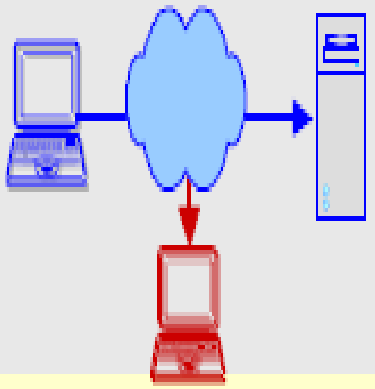
3. Eliminación (Se ataca la disponibilidad):

- Robo, retiro o pérdida de información y/o de otro recurso de la red
- Ejemplo: (1) Robo de laptop o de información confidencial



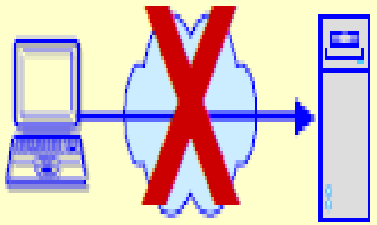
4. Difusión (Se ataca la confidencialidad):

- Acceso no autorizado a un activo
- Ejemplos: (1) Captura no autorizada de datos (data sniffing)
  (2) Uso no autorizado de puntos WLAN



5. Interrupción (Se ataca la disponibilidad):

- La red no se puede utilizar
- Ejemplos: (1) Corte de un enlace o cable
  (2) Ataque de denegación de servicio de la red



DIMENSIONES DE SEGURIDAD

CONTROL DE ACCESO

Protege contra la utilización de recursos de red sin autorización.

El control de acceso garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y aplicaciones.

AUTENTICACIÓN

Permite comprobar la identidad de las entidades comunicantes.

La autenticación garantiza la validez de las identidades que anuncian las entidades que participan en la comunicación (persona, dispositivo, servicio o aplicación)

Garantiza que ninguna de estas entidades ha usurpado una identidad o está reproduciendo una comunicación anterior sin autorización.

NO REPUDIACIÓN

Impide que una persona o una entidad nieguen haber realizado una acción concreta en relación con los datos, presentando las pruebas de esas acciones en la red.

Garantiza la disponibilidad de pruebas que pueden presentarse a terceros y que permiten demostrar que ha ocurrido algún tipo de evento o acción.

CONFIDENCIALIDAD DE DATOS

Impide la divulgación no autorizada de los datos.

La confidencialidad de los datos garantiza que las entidades no autorizadas no pueden entender el contenido de los datos.

A menudo se utilizan métodos tales como la criptación, listas de control de acceso y permisos de acceso a ficheros para garantizar la confidencialidad de datos.

SEGURIDAD DE COMUNICACIONES

Garantiza que los flujos de información sólo tienen lugar entre puntos extremos autorizados (la información no puede desviarse ni ser interceptada cuando fluye entre estos dos puntos extremos).

INTEGRIDAD DE LOS DATOS

Garantiza que los datos son correctos y exactos.

Los datos están protegidos contra las acciones no autorizadas de modificación, supresión, creación y copia, y en su caso se señalan estas acciones no autorizadas.

DISPONIBILIDAD

Garantiza que ningún evento que pueda ocurrir en la red impedirá el acceso autorizado a los elementos, la información almacenada, los flujos de información, los servicios y las aplicaciones de la red.

Las soluciones de recuperación en caso de desastre y para restablecimiento de la red se incluyen en esta categoría.

PRIVACIDAD

Impide conocer información observando las actividades de la red.

Por ejemplo los sitios web que un usuario ha visitado, la ubicación geográfica del usuario y las direcciones IP y los nombres DNS de los dispositivos de una red del proveedor de servicios.

La arquitectura de seguridad X.805 es una referencia para definir políticas de seguridad globales, planes de respuesta ante incidentes y recuperación, y arquitecturas tecnológicas teniendo en cuenta cada una de las dimensiones de seguridad en cada una de las capas y planos durante la fase de definición y planificación.

La arquitectura de seguridad X.805 también puede servir de base para una evaluación de la seguridad, para determinar los efectos del programa de seguridad en las dimensiones, capas y planos de seguridad, cuando se aplican las políticas y procedimientos y se hace efectiva la tecnología.

Una vez implantado, es necesario mantener el programa de seguridad, es decir, adaptarlo al entorno de seguridad cambiante.

Estándar

OSSTMM

OSSTMM

The **O**pen **S**ource **S**ecurity **T**esting **M**ethodology **M**anual

Manual de la Metodología Abierta de Testeo de Seguridad

OSSTMM

La organización ISECOM, el Instituto para la Seguridad y las Metodologías Abiertas, acaba de publicar la versión en castellano de la metodología abierta para la verificación de la seguridad, la OSSTMM. Por otra parte, también se ha publicado una sección especial de esta metodología especializada para el análisis de redes inalámbricas.

El "Manual de la Metodología Abierta de Testeo (sic) de Seguridad" es un documento que reúne, de forma estandarizada y ordenada, las diversas verificaciones y pruebas que debe realizar un profesional de la seguridad informática durante el desarrollo de las auditorías y verificaciones de la seguridad. Es un documento en constante evolución, fruto del trabajo conjunto de más de 150 colaboradores de todo el mundo.

Proceso

El proceso de un análisis de seguridad, se concentra en evaluar las siguientes áreas, que reflejan los niveles de seguridad presentes, siendo estos el ambiente definido para el análisis de seguridad. Estos son conocidos como las Dimensiones de Seguridad:

Visibilidad

La visibilidad es lo que puede verse, registrarse, o monitorearse en el nivel de seguridad con o sin la ayuda de dispositivos electrónicos.

Acceso

El acceso es el punto de entrada al nivel de seguridad. Un punto de acceso no requiere ser una barrera física.

Confianza

La confianza es una ruta especializada en relación con el nivel de seguridad.

Autenticación

La autenticación es la medida por la cual cada interacción en el proceso está privilegiada.

No-repudio

El no-repudio provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma.

Confidencialidad

La confidencialidad es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo.

Privacidad

La privacidad implica que el proceso es conocido únicamente por los sistemas o partes involucradas.

Autorización

La autorización es la certeza que el proceso tiene una razón o justificación de negocios y es administrado responsablemente dando acceso permitido a los sistemas.

Integridad

La integridad es la certeza que el proceso tiene finalidad y que no puede ser cambiado, continuado, redirigido o reversado sin el conocimiento de los sistemas o partes involucradas.

Seguridad

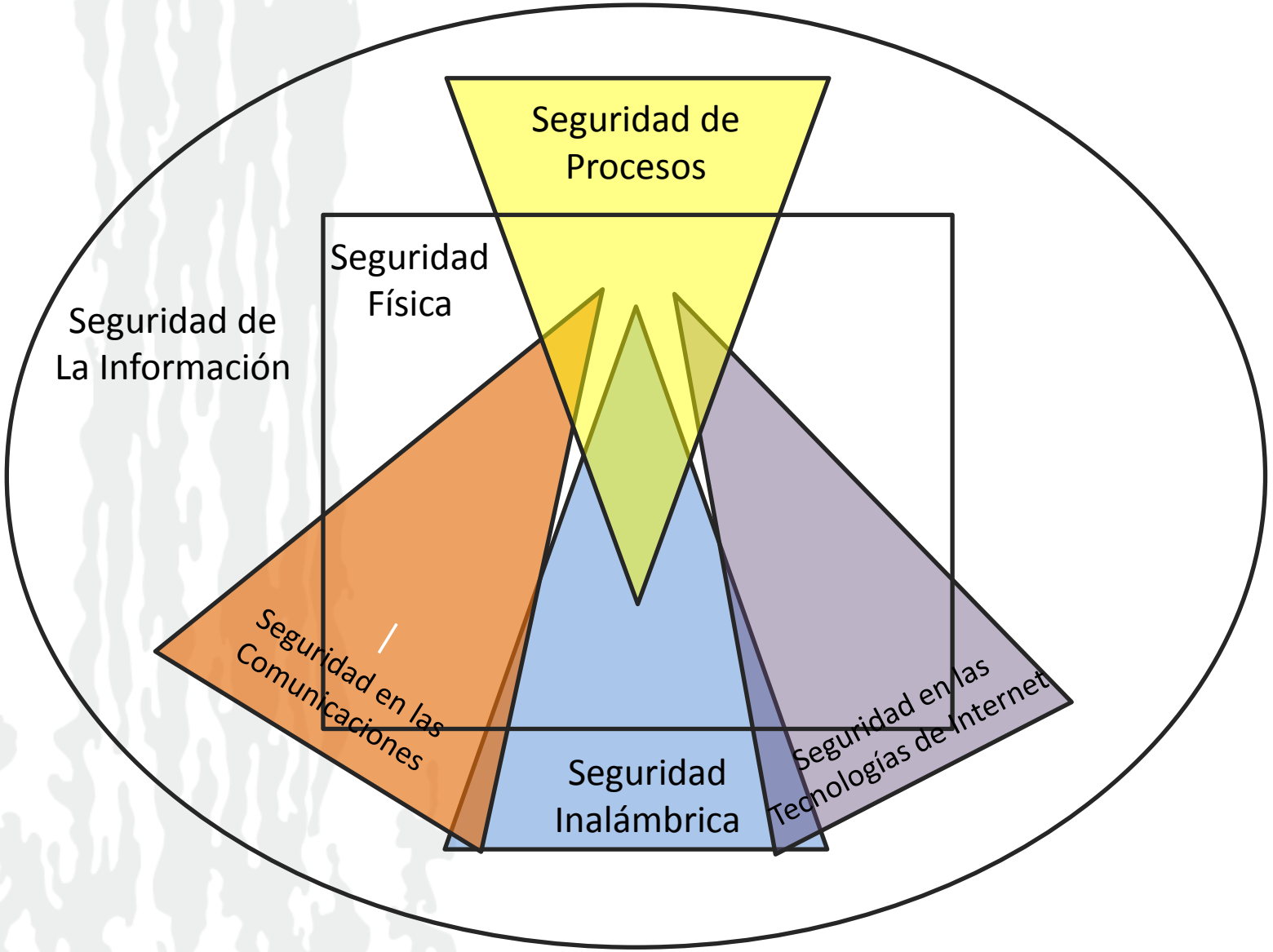
La seguridad son los medios por los cuales un proceso no puede dañar otros sistemas, o procesos incluso en caso de falla total del mismo.

Mapa de seguridad

El mapa de seguridad es un imagen de la presencia de seguridad. Esta corresponde al ambiente de un análisis de seguridad y está compuesta por seis secciones equivalentes a las de este manual. Las secciones se superponen entre si y contienen elementos de todas las otras secciones. Un análisis apropiado de cualquier sección debe incluir los elementos de todas las otras secciones, directa o indirectamente.

Las secciones el OSSTMM:

1. Seguridad de la Información
2. Seguridad de los Procesos
3. Seguridad en las tecnologías de Internet
4. Seguridad en las Comunicaciones
5. Seguridad Inalámbrica
6. Seguridad Física


Seguridad de
Procesos
Seguridad
Física
Seguridad de
La Información
Seguridad en las
Comunicaciones
Seguridad
Inalámbrica
Seguridad en las
Tecnologías de Internet

OSSTMM

Seguridad de la Información

- **Revisión de la Inteligencia Competitiva**

Resultados Esperados:

- ✓ Una medicion de las justificaciones de negocio de la red de la organización
- ✓ Tamaño y alcance de la presencia en Internet
- ✓ Una medicion de la política de seguridad a planes futuros de la red

Test

- ✓ Realizar un mapa y medir la estructura de directorio de los servidores web.
- ✓ Realizar un mapa y medir la estrutura de directorio de los servidores de FTP.
- ✓ Determinar el costo de TI de la infraestructura de Internet basados en SO, Aplicaciones y Hardware.

- **Revisión de Privacidad**

Resultados Esperados:

- ✓ Lista de cualquier revelacion
- ✓ Lista de las fallas de conformidad entre la politica publica y la practica actual
- ✓ Lista de los sistemas involucrados en la recoleccion de datos

Test

- ✓ Comparar publicamente la politica accessible con la practica actual
- ✓ Comparar la practica actual con el fraude regional y las leyes de privacidad o cumplimiento
- ✓ Identificar el tipo y tamano de la base de datos para el almacenamiento de los datos

- **Recolección de Documentos**

Resultados Esperados:

- ✓ Un perfil de la organización
- ✓ Un perfil de los empleados
- ✓ Un perfil de la red de la organización
- ✓ Un perfil de las tecnologías de la organización
- ✓ Un perfil de los socios, alianzas y estrategias de la organización

Test

- ✓ Examinar las bases de datos web y los caches pertenecientes a objetivos y personal clave de la organización.
- ✓ Investigar personas claves via paginas personales, curriculums publicados, afiliaciones organizacionales, información de directorios, datos de compañías, y el registro electoral.
- ✓ Recopilar direcciones de email de la organización y direcciones personales de personas claves.

OSSTMM

Seguridad de los Procesos

- **Testeo de Solicitud**

Resultados Esperados:

- ✓ Lista de los metodos de código de acceso
- ✓ Lista de los códigos validos
- ✓ Nombres de las personas de entrada

Test

- ✓ Seleccionar una persona de entrada desde la información ya obtenida sobre el personal
- ✓ Examinar los métodos de contacto con la persona de entrada desde el objetivo de la organización
- ✓ Obtener información acerca de la persona de entrada (posición, hábitos, preferencias)

- **Testeo de Sugerencia Dirigida**

Resultados Esperados:

- ✓ Lista de los puntos de acceso
- ✓ Lista de las direcciones IP internas
- ✓ Métodos de obtención de esta información
- ✓ Lista de la información obtenida

Test

- ✓ Seleccionar una persona o personas a partir de la información ya obtenida sobre el personal
- ✓ Examinar los métodos de contacto a las personas de la organización objetivo
- ✓ Invitar a las personas a usar / visitar una ubicación

OSSTMM

- **Testeo de las Personas Confiables**

Resultados Esperados:

- ✓ Lista de las personas de confianza
- ✓ Lista de las posiciones de confianza
- ✓ Métodos de obtención de esta información
- ✓ Lista de la información obtenida

Test

- ✓ Seleccionar una persona o personas a partir de la información ya obtenida sobre el personal
- ✓ Examinar los métodos de contacto a las personas de la organización objetivo
- ✓ Contactar a la persona interna desde una posición de confianza

- **Identificación de los Servicios de Sistemas**

Resultados Esperados:

- ✓ Puertos abiertos, cerrados y filtrados
- ✓ Direcciones IP de los sistemas activos
- ✓ Direccionamiento de los sistemas de la red interna
- ✓ Lista de los protocolos descubiertos de tunelizado y encapsulado

Test

- ✓ Recoger respuestas de broadcast desde la red
- ✓ Intentar traspasar el cortafuegos con valores estratégicos de TTLs (Firewalking) para todas las direcciones IP.
- ✓ Emplear ICMP y resolución inversa de nombres con el objetivo de determinar la existencia de todos los sistemas en la red.

OSSTMM

- **Búsqueda de Información Competitiva**

Resultados Esperados:

- ✓ Una medida de las justificaciones de negocio sobre la red de la organización Tamaño y alcance de la presencia en Internet
- ✓ Una medicion de la politica de seguridad a planes futuros de la red

Test

- ✓ Realizar un mapa y medir la estructura de directorio de los servidores web.
- ✓ Realizar un mapa y medir la estrutura de directorio de los servidores de FTP.
- ✓ Examinar la base de datos WHOIS en busca de servicios relacionados con los nombres de los servidores.

- **Revisión de Privacidad**

Resultados Esperados:

- ✓ Listado de cualquier revelación
- ✓ Listado de las inconsistencias entre la política que se ha hecho pública y la práctica actual que se hace de ella
- ✓ Listado de los sistemas involucrados en la recolección de datos

Test

- ✓ Identificar la política de privacidad pública
- ✓ Identificar los formularios web
- ✓ Identificar el tipo y la localización de la base de datos donde se almacenan los datos recolectados

Seguridad en las Comunicaciones

1. Testeo de PBX
2. Testeo de Buzón de Voz
3. Revisión de los Faxes
4. Testeo de Módems

Testeo de PBX

Un PBX(siglas en inglés de *Private Branch Exchange) cuya traducción al español sería Central* secundaria privada automática, es cualquier central telefónica conectada directamente a la red pública de teléfono por medio de líneas troncales para gestionar, además de las llamadas internas, las entrantes y/o salientes con autonomía sobre cualquier otra central telefónica.

Algunas razones para hacer una revisión del PBX:

• Existen pocas empresas que se dediquen a fabricarlas, por lo que conociendo un par, conoces el 70% del mercado.

• Suele estar instalado en lugares poco utilizados, como en algún almacén poco transitado, por lo que hace que sea fácil de acercarse y manipularlo.

• Las actualizaciones de software de los PBX se suelen hacer remotamente, por lo que es posible interceptarlas y corromperlas, introduciendo caballos de Troya

Testeo de Módems

La técnica más importante que se utiliza para comprometer la seguridad de los módems, es la conocida como *wardialing.*

Wardialing fue una técnica utilizada principalmente en las décadas de los 80 y 90, cuando los módems de marcación por tonos eran la forma más común de conexión a internet.

Consistía principalmente en hacer llamadas a una serie de números de teléfono automáticamente con el fin de encontrar módems conectados que permitieran la conexión con algún ordenador.

Con la llegada de las nuevas tecnologías, unas herramientas quedan desfasadas, y otras aparecen, y dentro del wardialing, aparece una herramienta novedosa

Seguridad Wireless

1. Testeo de Radiación Electromagnética
2. Testeo de Redes Wireless
3. Testeo de Redes Bluetooth
4. Testeo de Dispositivos Inalámbricos
5. Testeo de Dispositivos Inalámbricos de Mano
6. Testeo de Comunicaciones Inalámbricas
7. Dispositivos de Vigilancia Inalámbricos
8. Dispositivos de Transacciones Inalámbricas
9. Testeo de RFID
10. Testeo de Infrarrojos
11. Revisión de Privacidad

OSSTMM

Testeo de Redes Wireless

El estándar 802.11 fue desarrollado como un estándar abierto, es decir, que la facilidad de acceso y conexión fueron sus principales objetivos. Sin embargo, la seguridad no fue una de sus prioridades, y los mecanismos de seguridad que se desarrollaron fueron pensados más adelante, casi a modo de parche.

Existen dos tipos básicos de vulnerabilidades en WLAN:

1. Las que son resultado de una mala configuración
2. Las vulnerabilidades por mala codificación.

Testeo de Redes Bluetooth

Bluetooth, es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y globalmente libre (2,4 GHz.). Los principales objetivos que se pretenden conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

Dispositivos de Vigilancia Inalámbricos

OSSTMM

En este módulo, la atención se centra en dispositivos que sirvan de vigilancia, por ejemplo cámaras inalámbricas. Estas son muy fáciles de instalar, ya que no requiere cables. Además, se pueden instalar en lugares inaccesibles por la misma razón, y es por esto, por lo que muchas empresas deciden instalarlas.

- Escanear en busca de cámaras ocultas en menos de 5 segundos.
- Alcanza los 150 metros su exploración.
- Utilizada por profesionales para buscar en edificios enteros.
- Escanea frecuencias de 900 MHz a 2.52 GHz y busca un gran rango de cámaras incluyendo PAL/NTSC, CCIR/EIA.

Testeo de RFID

RFID (siglas de *Radio Frequency Identification o identificación por radiofrecuencia) es un sistema* de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas.

Las etiquetas RFID se basan en la emisión de unos pocos bits de información a lectores electrónicos especializados. La mayoría de los chips RFID comerciales son emisores pasivos, lo cual significa que no llevan alimentación (como batería o pilas): envían una señal solamente cuando las ondas recibidas los alimentan con un “chorro” de electrones.

Seguridad Física

1. Revisión de Perímetro
2. Revisión de Monitorización
3. Testeo de Controles de Acceso
4. Revisión de Respuesta ante Alarma
5. Revisión de Localización
6. Revisión del Entorno

1. Revisión de Perímetro

En este módulo se revisan todas las medidas de seguridad que existen para proteger los límites de la organización y sus activos. Se revisan medidas de protección tales como vallas, luces, muros etc...

2. Revisión de Monitorización

En este módulo se revisan dispositivos de monitorización de los puntos de acceso. Mas que la revisión de los propios dispositivos, se busca el comprobar que lugares están monitorizados, si los dispositivos están correctamente situados. Es decir, si hay lugares sin vigilar, otros demasiado vigilados etc...

3. Testeo de Controles de Acceso

En este módulo, se listan todos los lugares de acceso que tiene la organización físicamente hablando. Comprobando lo complejos que son, tipos de autenticación para darle privilegios de acceso a esa persona etc... Ejemplos podrían ser, el requerir una tarjeta de identificación que hay que mostrar a un vigilante jurado, escáner de retina, tipos de alarma etc...

4. Revisión de Respuesta ante Alarma

Aquí se comprueba el tipo de respuestas que tiene una organización ante una alarma. Se revisa qué personas deberían estar involucradas ante qué alarmas, y cómo deberían de actuar ante los distintos tipos de alarma que pueden activarse

5. Revisión de Localización

Éste es un método de ganar acceso a una organización a través de las debilidades de su localización y protección de elementos externos. Por ejemplo, comprobar líneas de visión que existen hasta la organización, posibles lugares desde los que es posible escuchar dentro de la organización (por ejemplo escuchas láser), horas de luz solar, clima etc... Es decir, se trata de revisar condiciones externas a la propia organización, y que pudieran afectar a su seguridad según donde se encuentra la empresa.

6. Revisión del Entorno

En este módulo se revisan condiciones alrededor de la organización, tales como las condiciones de desastres naturales de la empresa, políticas locales, costumbres y ética. Se comprueban condiciones que no dependen de la propia organización, y no solamente físicamente, sino a su contexto y entorno.

Gracias por su atención