TEMA 1

- Seguridad: Protección de Activos frente a amenazas
  - Conjunto de Servicios y mecanismos que protegen y aseguran integridad, privacidad, Políticas que aseguran seguridad Protocolos que aseguran que el sistema está libre intrusos
  - Comunicaciones basadas en TCP/IP
- Seguridad Clásica → Fortificación (Protección del Perímetro)
  - SOA, VPN...
  - Mercado de Vulnerabilidades
- Prevención, Detección y Respuesta.
  - Seguridad absoluta = imposible
  - Medidas proporcionales a los riesgos
  - Compromiso, nivel de seguridad, recursos y funcionalidad.
  - Mínimo Privilegio - Mínima Superficie - Defensa Profundidad.
- 3 PILARES: Disponibilidad - Integridad - Confidencialidad
  - Disponibilidad: Siempre que un usuario autorizado quiera acceso lo tendrá.
  - Integridad: Los activos no pueden ser modificados por personas no autorizadas
  - Confidencialidad: Privacidad de activos/información ante quien no está autorizado
  - Control de Acceso: Uso no autorizado
  - No repudio: Prevenir de que el emisor niege su participación

- Modelos que aborden de distinta forma esto → Horizontales y verticales (DOMINIOS)

- Factor Humano
  - Componente más débil
  - CSO o CISO → Definir el entorno de políticas y procedimientos
  - Plan Director de Seguridad
  - NO seguridad por Oscuridad, NO seguridad con prohibiciones
  - Política: Enunciado corto que se aplica a toda la organización y que proporciona una línea de acción
  - Estándares: Traducción Políticas a HW y SW
  - Procedimientos: Instrucciones concretas de como cumplir las políticas
  - Guías y Mejores Prácticas: Completan a los procedimientos con sugerencias que no son obligado cumplimiento
  - Plan director: La definición y priorización de un conjunto de proyectos en materia de seguridad de la información dirigido a reducir los riesgos.
    Cumplir 3ª también.

- Ley Orgánica de protección de Datos (LOPD)
  - Inscripción de datos en Registro General
  - Auditoría, Cláusulas de protección

NIVEL BASE: (Nombre, Apellido, Direcciones) Dejar de fumar y dirigirse del personal

⋮

TEMA 2. CONCEPTOS Y DEFINICIONES

- RIESGO: Probabilidad de que ocurra un incidente de seguridad
- AMENAZA: Acción que podría tener un potencial efecto negativo sobre un activo (Es necesario que exista vulnerabilidad o fallo para provocar daño)
- VULNERABILIDAD: Debilidades, fallos o agujeros. De Diseño, Arquitectura, o Estándares

  - Ciclo de Vida: CVE
    - Detección y Descripción CVE-ID
    - Implementación de la explotación de la vulnerabilidad
    - Solución
    - Crear parche
  - Zero Day: Día de la vulnerabilidad se hace pública.
  - CVSS: Common Vulnerability Scoring System → Criticidad
  - Aceptarlo, Mitigarlo, Evitarlo, Transferirlo

- Evaluación del Riesgo

METODOLOGÍAS Y HERRAMIENTAS

- Establecer objetivos, Evaluar Riesgo, Contramedidas

↓	↓	↓
Activos (HW)	Amenazas	Inversión
Datos	Frecuencia	En función del Riesgo
Impacto $	Vulnerabilidades	

- ANÁLISIS VULNERABILIDADES

CAJA NEGRA	GRIS	BLANCA
No conoces Objetivo	⟷	Conoces el Objetivo
Simula el Ataque		Más Completa
Evalua comportamiento		Origen Vulnerabilidad
Requiere menos conocimiento		Más eficiente
+ Falsos negativos		+ Falsos Positivos

- RESPUESTA A INCIDENTES
  - Crear un Computer Security Incident Response Team
  - Definir un plan de respuesta a incidentes
  - Contener daños y gestionar riesgos

- CSIRT
  - Estar al Día
  - Auditorias
  - Minimizar vulnerabilidades
  - Documentar y catalogar incidentes

- EXPLOIT: Fragmento de Software utilizado con el fin de aprovechar una vulnerabilidad de seguridad para conseguir un comportamiento no deseado

TEMA 3: Anatomía de un ataque

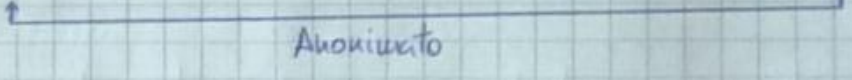
1. Introducción.

- Tipos de ataque en función de acción/objetivo
  - Intercepción: Espionaje o redirección de comunicaciones
  - Fabricación: Creación de usuarios/activo falso → Engaño
  - Interrupción: Bloqueo del normal funcionamiento
  - Modificación: Alteración no autorizada

- Black Hat Hackers: Atacantes que aprovechan vulnerabilidades, tienen en común alta destreza y no revelan los agujeros
- White Hat Hackers: Siempre informan de las vulnerabilidades, y colaboran. Interesados en hacer avanzar la ciencia.
- Script Kiddies: Aficionados que se aprovechan de herramientas automatizadas y recetas → Consecuencias desconocen.
- Crackers: Romper los sistemas criptográficos, alto conocimiento en matemáticas y algoritmia

2. Fases de un Ataque

- Recogida Info → Construcción → Repetición → Obtención Resultados



3. Técnicas para la recogida de Información.

- FOOTPRINTING: Obtener toda la info posible de la red, Sistema, o usuario
  - Primero info general Metadatos e info pública
  - Mensajes de error específicos

- Operadores en el buscador → SHODAN
- Metadatos → Autor, S.O, aplicación ... incluso IP y localización GPS

- FINGERPRINTING: Más específicos, datos sobre pila TCP/IP de la red o sistema en concreto
  - Topologías, nombres, puertos, S.O ...
  - Info no pública → Phising, Ing. Social, Sniffing...
    - Phising: Jugar con la probabilidad (Contraseña y usuario) Spear Phising y Whaling
    - Sniffing: Capturar datos que circulan por la red → Obtener info (Wireshark)
    - Scanning: Analizar el estado de una red y de los dispositivos de esta (Nmap)
      Escaner Puertos y Vulnerabilidades
  - Para Prevenir
    - Planes de Concienciación → Importancia seguridad
    - Definir y mantener actualizadas las políticas
    - Limitar la info pública
    - Utilizar autentificación.

4. Anonimato: Importante para el atacante.
   - Oculta su identidad en las fases iniciales (legales) y borra sus huellas para posibles análisis.

- Tipos de Anonimato:

- Anonimato FISICO: Acceso desde Red Pública.
- Anonimato BOUNCER: Toma control sobre sistema y lo usa de puerta → Se explota una vulnerabilidad con un troyano o similar
- Anonimato PROXY: Máquina mediante NAT hace de intermediario
  - No solo oculta IP, sino dirección y puerto
  - Se puede cambiar continuamente de Proxy → matriz

RECOGIDA INFO - CONSTRUCCIÓN - REPETICIÓN - RESULTADOS

↑ ANONIMATO ↑

TEMA 4: ATAQUES A REDES IP Y PROTOCOLOS

1. Introducción y Recordatorio.
   - Pila TCP/IP

Nivel Aplicación (HTTP)
Nivel Transporte (TCP)
Nivel Red (IP) → ARP
Nivel Enlace (MAC)
Nivel Físico (Binario)

2. ARP Poisoning, ARP spoofing y MitM
   - Toda la pila se basa en identificadores a distintos niveles
   - Protocolos permiten traducciones entre ellos

     Nombre Dominio - Dirección IP - Dirección MAC

   - Poisoning = Usar protocolos dinámicos para envenenar traducción.

     ARP = Traducciones MAC a IP (Enviar tramas falsas de ARP Reply)

     Al ser dinámico hay que enviarlo continuamente.

   - Spoofing: Siempre implican suplantación de identidad a diferentes niveles (En este caso, en capa Enlace)
   - MitM: (Man in the Middel): Interceptar y modificar todas las comunicaciones entre dos equipos que se encuentren en el mismo servicio de red.

     Denominado Janus también.

     - Envenena ambas cachés, así todos los mensajes tienen un intermediario.
     - Solo se puede percibir → Enviar periodicamente trazar (Latencia) y más tráfico de Red
     - No hay grandes alteraciones

- En ocasiones no está en el mismo segmento de Red pero sí en el mismo puerto de enlace (Mismo Router)
  - En este caso se produce un robo de Puerto, se interceptan las comunicaciones, pero no puedes envenenar caché.
  - Sirve para producir denegaciones de servicio, saturando el router

3. TCP Hijacking
- Combinación de Sniffing, ARP poisoning/spoofing y MitM se consige Login/Pass
- Esto TCP/UDP pretende secuestrar a un nivel más alto
  - Tomar comunicación establecida una vez tenga el usuario ya ha introducido el login/pass
  - Diferencia con Spoofing → Se suplanta desde el principio. En el Hijacking te adueñas una vez logeado
- Secuencia TCP/IP se basa en paquetes → <u>Nº Secuencia</u>
  - Con UDP no hay nº de Secuencia → Inmediato.
  - TCP no prove mecanismos para probar los extremos
- 4 parámetros → Conexión TCP
  - Dirección IP del Emisor
  - Dirección IP del Receptor
  - Puerto TCP emisor
  - Puerto TCP receptor

- Todos los paquetes tienen 2 números que los identifican
  - SEQ (32 bits) Se inicializa aleatoriamente
  - ACK: Valor numérico de secuencia que espera recibir.

- Realizar Secuestro.
  - Monitoriza tráfico → Sniffer
  - Esperar que negocien el inicio de sesión.
  - Intercepta números de sesión.
  - Haciendo Spoofing / MitM el atacante envía datos al otro extremo (Con el ACK que corresponda)
  - Los de la víctima serán rechazados y la sesión ya ha sido secuestrada.
  - Si no puedes monitorizar → A ciegas (Predecir números)

4 Ataques en la capa de Aplicación. (Poisoning, Spoofing... a más nivel)

- DNS Spoofing y Server Spoofing
  - Se construye sobre un MitM
  - Intercepta la consulta a su servidor DNS
  - Devolver traducción Dominio - IP falsa, redirigiendo al servidor que tú quieras
  - Otra → Rogue DHCP (Servidor falso)
    - Conseguir que el Offer del servidor DHCP llegue a la víctima

- DNS Poisoning
  - Aprovecha que el protocolo DNS se basa en la utilización de cachés intermedias para resolver nombre de traducciones anteriores

- Typosquatting y Bitsquating
  - Aprovechar los errores tipográficos de teclear un dominio

5. Ataques a IPv6
   - Convive con IP v.4
   - Desaparece ARP para convertirse a SLAAC
   - IPsec de forma nativa

TEMA 5 - DENEGACIÓN DE SERVICIO VOLUMÉTRICA

1. Introducción.

- Casi siempre basados en fuerza bruta, poco sofisticados
- Dirigidos a perjudicar la disponibilidad → Grandes pérdidas $
  - Ataques Distribuidos (DDoS Distributed Denial of Service)
  - Red de BotNets...

- DDoS as a Service
  - Principales sectores son financieros, tecnologicos, industrial y sector público → Hacer perder $ o confianza

2. Patrones Basados en protocolos de la capa de infraestructura

- Selección del Protocolo - Selección Victimas - Spoofing - Ampliación del Tamaño - Ampliación Distribución - Automático

- Spoofing solo si lo haces por reflejo (Suplantar)
- Conseguir victimas colabores (Amplificación Distribución)
  - Por BotNet → Flood
  - Suplantan (Spoofing) ataque por reflejo.

3. Patrones Basados en protocolos de capa Aplicación.

- Mucho menos frecuentes → Solo un 10%
- Vector HTTP → Get y Post (HTTP flood)
  - GET: Solo amplificación por Distribución.
  - POST: Si haces que realice cuentas puedes acelerar la denegación
  - No es necesario Reflejo → Difícil detectar/Mitigar

1. Introducción

- Agente de Amenaza - Ataque - Debilidad - Control Segu
  - Función - Impacto
- Iniciativas que intetan generalizar y clasificar todas las vulnerabilidades conocidas
  - CWE (Common Weakness Enumeration)
  - CWSS (Common Weakness Scoring System)
  - CAPEC (Common Attack Pattern Enumeration and Classifica

2. Desbordamiento (Overflow)

- Aprovechan vulnerabilidad del Software que permite ejecutar cualquier código en el sistema. No comprueba el tamaño de los parámetros que se pasan a una función. (Buffer y Heap Overflow)
  - Heap (Montón): Se llena de Direcciones crecientes
  - Pila: Se llena de Direcciones decrecientes
    - Variable internas, Punteros, Dirección Retorno...
    - Al pasarle más caracteres de los permitidos sobrescribe estos datos, como la Dirección de Retorno
    - Objetivo: Que la Dirección de Retorno apunte al propio buffer → Código ensamblador (SHELL CODE)

3. Inyecciones

3. Inyecciones

- Aprovecha que no se comprueban los parámetros
- Más conocida SQL, otras LDAP o XPath
- Ataques directos o a ciegas (Blind SQL Injection)
- Se aprovecha los mensajes de error y su información
  - Adivinar motor de Búsqueda de Datos
  - Tablas que tiene
  - Interacción con S.O y usuarios
- Usos:
  - Procesos de Login
  - Averiguar cualquier tipo de información.
  - Agregar, eliminar tablas de una BBDD
- Se suele actualizar el proceso
- Con ser una Web dinámica ya podría hacer inyecciones
  - Cookie: Información de un sitio web y almacenada (por un sitio web) por el navegador, de manera que la web ya conoce la sesión.

4. Forgeries (Falsificación)

- Pretende crear, imitar o adaptar el entorno, con el objetivo de engañar.
- Más común XSS (Cross Site Scripting)
  - Las aplicaciones web se componen de elementos estáticos y dinámicos
  - Aprovechar elementos dinámicos para conseguir los objetivos → Atacante

- Tipos de Ataques XSS
  - LOCALES (tipo 0 o DOM)
    - Los contenidos se actualizan sin refrescar la página → JavaScript
    - En el servidor es segura pero en el lado del Cliente no.
    - En algún momento se inyecta este código
    - En el navegador de la víctima ocurre el ataque.
  - NO ALMACENADO (tipo 1 o no persistente)
    - Misma vulnerabilidad pero en el lado del servidor
      - Accede por JS a un parámetro de la URL y lo pega directamente en el HTML sin comprobarlo
  - ALMACENADO (tipo 2 o persistente)
    - Inyecta en un HTML y luego queda almacenado en el servidor
    - Luego puede infectar a más víctimas (Foros)

- XSRF (Cross Site Request Forgery)
  - Acceder a otra app o web que el usuario ya estuviera logeado

- Clickjacking → Robar el Click (Capas de HTML e iframe trasparentes)
  - Opacidad 0, hace que tú mismo hagas click

TEMA 7. MECANISMOS CRIPTOGRÁFICOS

1. Introducción

- Criptografía: Estudio de los principios y mecanismos necesarios para establecer procesos de cifrado, descifrado y generación de claves
- Criptoanálisis: Estudio de los principios y mecanismos necesarios para descifrar mensajes sin conocer las claves de cifrado.
- Afecta a los 7 principios de la seguridad menos "Disponibilidad"
- Características.
  - Recursos y esfuerzo para cifrar y descifrar deben ajustarse al grado de seguridad.
  - Mecanismos sencillos
  - Implementación Algoritmos deber ser sencilla
  - Un error en el cifrado no debería propagarse
  - Tamaño del cifrado no debería sobrepasar el original.
- Algoritmo de Bloque (IDEA, AES, RSA): Cifrado en bloque en el mismo algoritmo, a un bloque de información
- Algoritmo de Flujo (AS, SEAL): Flujo de clave, aleatoria, y de mayor longitud que el mensaje. (Más rápido y menos errores) Mayor pérdida de info.

2. Sistemas de Cifrado de Clave Pública y Privada

- Con un sistema de Clave Privada: Una clave privada única y el mensaje se cifra y se descifra con lo mismo. (DES, AES)
- Con clave pública cada usuario crea un par de claves, privada y pública, encriptación y desencriptado con las dos. (RSA)
  - Dificultad de obtener clave privada partiendo de la pública.
  - Más lento, fácil intercambio, y firma digital

- Por eso, intercambio de información se suele utilizar sistemas de clave privada, y el intercambio de claves se hace por pública

- Tercera Parte Confiable → Clave Pública
  TTP Trusted Third Party
  - Mejor forma de Distribuir las claves públicas.
  - Debe ser segura contra un MitM
  - Se basa en definición de infraestructuras
    ICPs o PKIs Public key Infrastructures
    (Suele usar Certificados)

3. DES, AES y RSA

- Des: Clave Privada, con bloques de 64 bits y claves de 56 bits
  - Se basa en operaciones de sustitución y transposición.
    16 ciclos
  - Doble DES y triple DES

- AES (Advanced Encryption Standard) se basa en el algoritmo de Rijndael
  - Bloques de 128 bits y claves 128, 192, 256
  - 10, 12, 14 rondas de transposición, sustitución ...
- RSA (Rivert-Shamir-Adleman): Factorizar números enteros
  - Producto de dos números primos al azar (10^{200})

4. Mecanismo de Autentificación.
   - Permite Verificar la identidad digital del remitente de un mensaje o petición.
   - Categorías (Hasdar 2)
     - Sistemas basados en algo conocido (Palabra clave)
     - Sistemas basados en algo poseído (Llave)
     - Sistemas basados en algo que se es (Huella)
   - Mecanismos
     - Autentificación con criptografía simétrica: Garantizar la confidencialidad, integridad y autenticidad
       Compartir clave simétrica segura (?) → Kerberos
     - Autentificación con HMAC o Checksum: A y B extremos, comparten clave secreta y además aplica el HMAC
       - Clave compartida entre ambos
       - Integridad, Autentificación
       - Mucho uso en TLS
     - Autentificación por función Hash

- Autentificación por función Hash
  - No diseñadas para esto, pero son rápidas y conocidas
  - SSL y TLS

- Autentificación con criptografía asimétrica (Pública)
  - Mecanismos de firmas digitales
  - RSA, DSS, Rabin...

5. Firma Digital y Funciones Hash
- Sistemas de clave pública → Verificar la autentificación y autenticidad del origen, así como que no ha sido modificada (Integridad)
  - Integridad, No repudio y autentificación.
- Se firma solo un resumen del mensaje → sino muy lento
  - Función Hash, como $h(m)$
    - Unidireccional: Si conoces h no puedes sacar m entonces
    - Compresión: $h(m)$ menor que el Mensaje (m)
    - Facilidad: fácil calcular $h(m)$ de (M)
  - MD5 y SHA-3

6. Kerberos
- Mejorar criptografía simétrica (Clave Secreta)
- Propone un KDC (Key Distribution Center)
  - Tercera parte confianza

6. Kerberos

- Cada parte de la comunicación comparte clave secreta y única con el KDC
- KDC se ocupa de distribuir la clave de sesión que va a ser utilizada en la conexión entre dos partes
  - Clave se protege con clave maestra de las dos partes

- Funcionalidad de KDC
  - Authetication Service (AS)
  - Ticket Granting Service (TGS)

Diapos 50

7. Sistemas de Certificados

- Para garantizar la unicidad de las claves privadas se suele recorrir a soportes físicos → Tarjetas inteligentes
- Para asegurar que una clave pública pertenece a un usuario existen los certificados digitales
  - Confiar en un certificado por las PKIs Autoridades de Certificación.

- Funciones de PKI
  - Selección de Claves: Publicación claves públicas
  - Registro de Claves: Emisión certificados
  - Recuperación de Claves
  - Evaluación de Confianza: Validez de un certificado
  - Revocación de Certificados

TEMA 8: CONTRAMEDIDAS DE RED Y PROTOCOLO

1. Introducción

- Diferentes tipos de topologías: Anillo, Malla ...
- Permitir proteger el perímetro y segmentar las diferentes redes internas (Nuevo significado de perímetro)

2. Firewalls y DMZs

- Separación de las redes con distintos mecanismos: Switches, Tablas Diodos de Datos, Firewalls y DMZs
  - Firewall: Dispositivo hardware/software que tiene como objetivo proteger una red de otras redes (Se Sitúa donde recoja todo el tráfico entrante y saliente) → Configurarlo Bien
    - Monitoriza el tráfico
    - Se comparan las unidade de info con reglas
    - Tipos: por Funcionamiento
      - A nivel de Transporte: Examinan cabeceras, filtran por puerto
      - Firewall DPI: Más sofisticado puede filtar por protocolo
      - Proxy (Nivel Aplicación): Tiene en cuenta los parámetros específicos de cada aplicación
  - DMZ (Zona Desmilitarizada): Una red que se ubica entre la red de computadores interior y la red exterior
    - Permite que servidores interiores suministren Servicios a la exterior.

- Previene Intrusiones
- Se hace con Firewall de 3 vías o con 2 firewalls (3 tarjetas de Red)

3. Otros sistemas asociados a la protección del Perímetro.
   - HoneyPot: Poner a prueba ser atacado y/o comprometido
     - Traza de los distintos puntos de vista de los ataques
     - Recoletar información de las herramientas y tácticas
       - Ataques Zero-day → Aprender
     - Debe ser un sistema realista (Datos y procesos Falsos)
       - Separarlo de la red buena
       - Protegerlo lo justo
     - Tipos
       - Prodoction HoneyPot y Research HoneyPot
       - En función de la interacción (Con entorno)
         - Honey Pot de Baja interacción
         - Honey Pot de Alta interacción
     - HoneyNet: Conjunto de HoneyPots de alta interacción que configuran una red completa
       - HoneyNets Virtuales → Más asequible
     - Formar parte de IDPs (Intrusion Detection and Prevention System)
   - Otros: Firmas, Patrones, Estado protocolos, Detección de anomalías

4. IPSec

- Conjunto de mecanismos de seguridad que se pueden implementar en IPv4 y es nativo en IPv6
- Capacidad de asegurar comunicaciones via LAN y WAN
  - Se puede hacer encriptación a nivel de enlace (IP)
  - Administración centralizada.
- Servicios
  - Control de Acceso
  - Integridad de la Conexión
  - Autentificación del origen de la conexión
  - VPN seguros
  - Confidencialidad y Rechazo de Paquetes ya editados
- Autentificación mutua de los dos equipos, establecimiento de asociación de seguridad (S.A)
  - Cifrado DES, ~~EES~~, DSA, AES
- Componentes IPSEC
  - Protocolos IPSEC : ESP y AH
  - Administración automática de claves → Protocolo ISAKMP (Administración dinámica) Diffie-Helman
  - Usa ISAKMP para negociar dinámicamente la seguridad mutua.
- Directivas de Seguridad IPSec.

. Directivas de seguridad IPSec

- Son reglas de seguridad que definen el nivel de seguridad deseado
  . Definen también direcciones, protocolos, DNS
- Controlan cómo y cuando se invoca IPSec
  . Iniciar y controlar una comunicación segura

. Modos IPSec

- Transporte o Extremo a Extremo: Son los extremos los que se encargan del procesamiento de la información
- Modo túnel: Seguridad proporcionado por un único nodo central

	Modo Transporte	Modo Túnel
AH	Autentifica el datagrama IP, y la cabecera previamente seleccionada	Autentifica todo el datagrama Cabecera IP y sus extensiones
ESP	Encripta la información útil y las cabeceras IP/IPv6	Encripta todo el datagrama
ESP + Autentificación	Cifra ESP y luego autentifica solo info útil.	Encripta y autentifica todo

TEMA 9: CONTRAMEDIDAS DE USUARIO, ADMINISTRADOR Y DESARROLLADOR

1. Buenas Prácticas para el Usuario y Administrador

- Seguridad Física
- Formación y Concienciación
- Contraseñas Seguras
- Aplicaciones y S.O actualizado
- Antivirus antimalware
- Gestión de cuentas → Mínimo privilegio
- Permitir acceso remoto encriptado → clave pública/privada.
- Forzar uso de contraseñas seguras
- Controlar envejecimiento y expiración de contraseñas
- Shells restringidas
- Perfiles y Roles → Eliminar cuentas obsoletas
- Control acceso y autentificación
- Encriptar a varios niveles

2. Buenas Prácticas para el desarrollador

- Comprobar los operadores SIEMPRE
- Comprobar rangos antes de realizar conversión de tipos
- No ignorar valores de retorno ni excepciones
- Validar datos de entrada.
- Evitar identificadores públicos de clases, interfaces y paquetes
- No mostrar info sensible en las excepciones
- Liberar recursos
- Borrar ficheros temporales
- Generar nº aleatorios FUERTES. Conocer bien el lenguaje

3. Metodologías de Desarrollo seguro

- Analizadores de código estático → PMD (No ejecuta)
- Guías que recopilan "Mejores prácticas" por cada lenguaje

- Análisis dinámico
  - Ejecuta el código
  - Ve el comportamiento → Verificación formal requisitos

- Metodologías Completas
  - Software Security Framework (SSF)
    - 12 prácticas divididas en 4 dominios
  - OWASP SAMM
    - 13 prácticas, 4 funciones básicas
  - SDL (Security Development Lifecycle)
    - Training, Requirements, Design, Implementation, Verification, Release, Response

- Aspectos Comunes
  - Procesos repetibles
  - Resultados Medibles
  - Trazabilidad
  - Formación y concienciación desarrolladores
  - SDS + C (Security by Default, Design, Deployment, Community)