1. Osint, Huminit, Sigint y Masint.

INFORMACIÓN	INTELIGENCIA
Noticia de un hecho en un sentido más amplio. Es el elemento inicial que debemos considerar para elaborar la inteligencia.	Es el resultado de valorar, analizar, integrar e interpretar la información.

CICLO DE INTELIGENCIA.

1. Obtención de la información → Transformación en Inteligencia.
2. **Dirección → Obtención → Elaboración → Difusión.**

2. Fingerprinting y Footprinting.

OSINT → Inteligencia de fuentes abiertas (Open Source Intelligence).

Fuentes de información:

- Medios de comunicación.
- Datos públicos; datos oficiales emitidos por entidades gubernamentales o Administraciones Públicas.
- Material de acceso controlado.
- Foros, redes sociales, blogs… etc.

Objetivos:

- Conocer reputación e identidad digital de usuarios y organizaciones.
- Realizar estudios psicológicos y sociológicos.
- Auditorías de empresas para evaluar las medidas de seguridad.
- Identificar y prevenir amenazas.
- Preparación de ataques (APTs).

HUMINIT → Inteligencia humana (Human Intelligence).

Recopilación oral o escrita originaria de una fuente humana. Se puede obtener abierta o confidencialmente. Tipos:

- Inteligencia de Alto Nivel → Seguridad nacional.
- Inteligencia específica → Información de naturaleza táctica.

SIGINT → Inteligencia de señales.

Se obtiene la información mediante las transmisiones de datos. Comprende la obtención de datos en ``bruto´´ y su posterior análisis.

- Inteligencia de comunicaciones (COMINT, Communications Intelligence).
- Inteligencia electrónica (ELINT, Electronic Intelligence).
- Inteligencia de señales de instrumentos extranjeros (FISINT, Foreign Instrumentation Signals Intelligence).

MASINT → Inteligencia de mediciones y firmas electrónicas (measurement and Signature Intelligence). Disciplina de análisis. Tipos:

- Inteligencia Acústica (ACINT).
- Inteligencia de Radar (RADINT).
- Inteligencia de Infrarrojos (IRINT).
- Inteligencia Láser (LASINT).
- Inteligencia Nuclear (NUCLINT).
- Inteligencia Óptica (OPINT).
- Inteligencia de Radiación no intencionada (URINT).

3. ingeniería Social. El phishing.

Footprinting

- Recopila y busca información pública de un objetivo.
- Información presente en internet de manera consciente o inconsciente por la organización o individuo.
- No es delito.

Fingerprinting

- Recopila y busca información mediante la interacción con el objetivo.
- Aprendemos los sistemas y sus posibles versiones y configuraciones.
- Escaneo de puertos en redes y sistemas.
- Ataques de hombre en el medio.
- Se considera delito.

Ingeniería Social. El phishing.

¿Qué es la ingeniería Social? → Método para engañar y manipular a las personas para que revelen información confidencial. Y el usuario es el más débil de la cadena.
¿Qué es el Phishing? → Técnica que consiste en suplantar la identidad para obtener un rédito o beneficio.

- Beneficio económico.
- Credenciales de acceso.
- Información confidencial.

Métodos de ingeniería social

MÉTODOS	EJEMPLOS
Pasivas	Observación (mirar contraseñas, espionaje)
No presenciales	Correo electrónico, teléfono, cartas.
In situ no agresivas	Hablar con personas, vigilancia, fake news.
In situ agresivas	Chantaje o extorsión, suplantación de identidad.

Ejemplos:

- Correo electrónico suplantando una entidad u organización.
- USBs manipulados → Rubber Ducky (es un pendrive modificado).
- Suplantar web → Clonar web en repositorio distinto.

Phising – Estafas.

Ciclo del Phising

- SMSs fraudulentos: **Smishing.**
- Llamadas fraudulentas: **Vishing.**
- Pesca dirigida: **Whaling.**
- Malware
  - Keyloggers.
  - Screenloggers.
  - Troyanos bancarios.
  - Alteración de DNS: Pharming.

4. Hacking con buscadores

Navegadores

- Software (app) que traduce la información de los sitios web para una visibilidad mejor.
- El navegador es el ``cliente´´, que realiza una consulta a un sitio web y este le proporciona la información.
- Variedad de navegadores. (Chrome, Explorer, Firefox).

Motores de búsqueda o buscadores.

- Algoritmos que optimizan y facilitan las búsquedas en internet por parte del usuario.
- Uso de robots y spiders para el rastreo de páginas web.
- Uso de operadores y dorks.
- Hacking con buscadores.
  Ejemplos:
  - duck duck go → historial privado, bloqueo de rastreadores publicitarios y controla tus datos personales.
  - Shodan → detecta sistemas y servicios conectados, el acceso sin autorización es un delito.
  - Bing → buscador de Microsoft.
  - Google.

DORKS

BING → diferentes a Google, útiles en la búsqueda de IP.

Operador	Ejemplo
Feed	Feed: Chema Alonso
IP	IP: 35.206.174.19
	IP: 46.231.127.182
Contains	Contains: ciberseguridad
Domain	Domain: ufv.es

Google → Operadores lógicos.

Operador	Descripción	Ejemplo
AND (intersección)	Reduce y especifica la búsqueda	Hacking AND Kevin Mitnick
OR (unión)	Amplía la búsqueda	Gasolinera OR Kevin Mitnick
NOT (exclusión)	El término o expresión que le sigue	Contabilidad NOT auditoría
"Texto a Buscar"	Busca exactamente el contenido del texto entre comillas	"Grado en Gestión de la Ciberseguridad"

Operador	Descripción	Ejemplo
Site	Muestra resultados del dominio indicado	Site:ufv.es
-	Término que se va a omitir	Hacking – Kevin Mitnick
+	Como el comando AND	Hacking + Kevin Mitnick
Link	Todas las páginas que tengan un link al establecido	Link:ufv.es
Info	Información de la página web, caché de Google	Info:www.ufv.es
Inurl	Muestra las páginas que incluyan el término de búsqueda en la url.	Inurl:ufv
Intitle	Páginas que tengan el término en el título	Intitle:ufv
Cache	Cache almacenada por Google	www.ufv.es
Filetype	Extensión de archivos específica	Filetype:pdf
Intext	Término que se encuentre dentro de la web	Intext:ufv