THE BRIDGE

CYBER SECURITY

OSINT

Fuentes de Datos

- Las **fuentes de datos** son esenciales para cualquier análisis en el proceso de investigación. Estas fuentes almacenan información en **tablas de datos**, objetos de datos u otros formatos de almacenamiento.

- **Fuentes abiertas**: Cualquier vía de la que se puedan obtener datos y que sea accesible o pública. Esto incluye información gratuita o de bajo costo que no está cifrada y es de dominio público.

https://universoabierto.org/2018/03/24/manual-de-fuentes-de-informacion-de-la-uoc/

OSINT

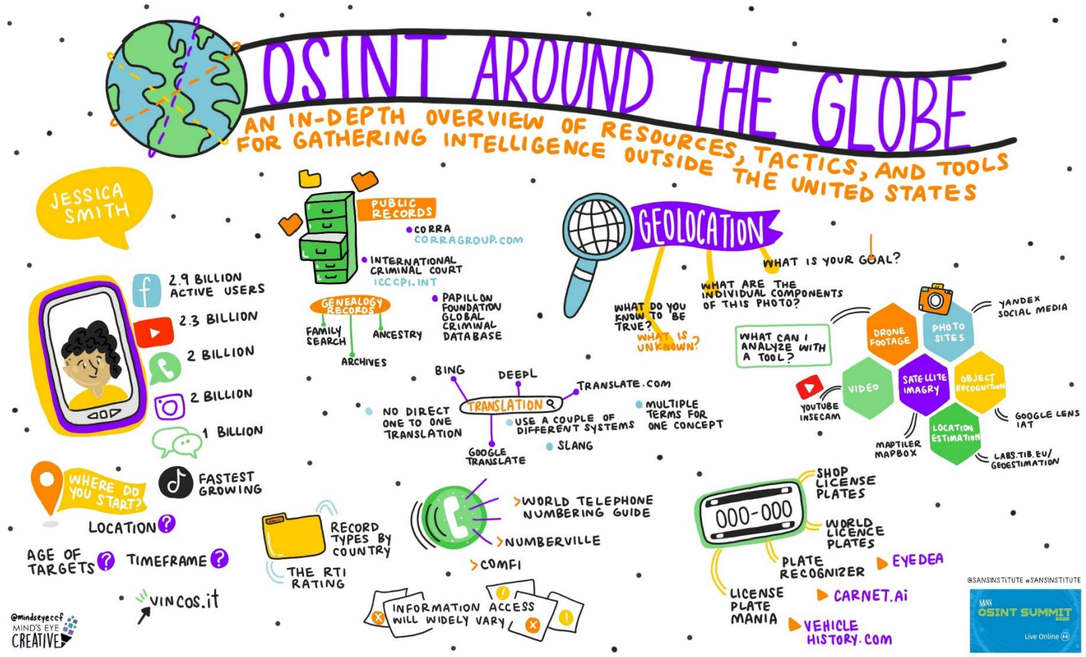
- **Inteligencia de Fuentes Abiertas** se refiere al conjunto de técnicas y herramientas utilizadas para recopilar información que es pública, analizar datos y relacionarlos para convertirlos en conocimiento útil.

- En otras palabras, **OSINT** permite obtener datos de fuentes abiertas, especialmente en Internet, y se utiliza en áreas como la ciberseguridad y la investigación.

- Beneficios de **OSINT**:
  - **Respuestas rápidas**: Permite obtener respuestas a través de motores de búsqueda como Google.
  - **Aceleración de investigaciones**: Facilita el proceso de investigación al proporcionar datos relevantes.

- Los cibercriminales también hacen uso de estas técnicas

- Ejemplo de Aplicaciones del **OSINT**:
  - **Reconocimiento de un pentesting**: Descubrir hosts en una organización, información de IP, subdominios, información de DNS, ficheros de configuración, claves, correos, etc.
  - **Ingeniería social**: Buscar toda la información sobre un usuario (en redes sociales, documentos, etc.) y ser consciente de la información que hay disponible en abierto para evitar "picar" en un ataque de phishing.
  - **Prevención de ciberataques**: Obtener información que nos haga estar alerta ante una amenaza o un potencial ciberataque que pueda sufrir nuestra organización.



https://www.sans.org/blog/visual-summary-sans-osint-summit-2022/

Formas de Obtener Información

Usar fuentes públicas. No interactuar con el objetivo. Técnica más utilizada.

Interactuar de forma discreta con el sistema o persona objetivo, sin generar alarmas.

Interactuar directamente con el objetivo. Uso de herramientas como NMAP

https://es.slideshare.net/pcolomes/open-source-intelligence-osint

Análisis de Objetivos

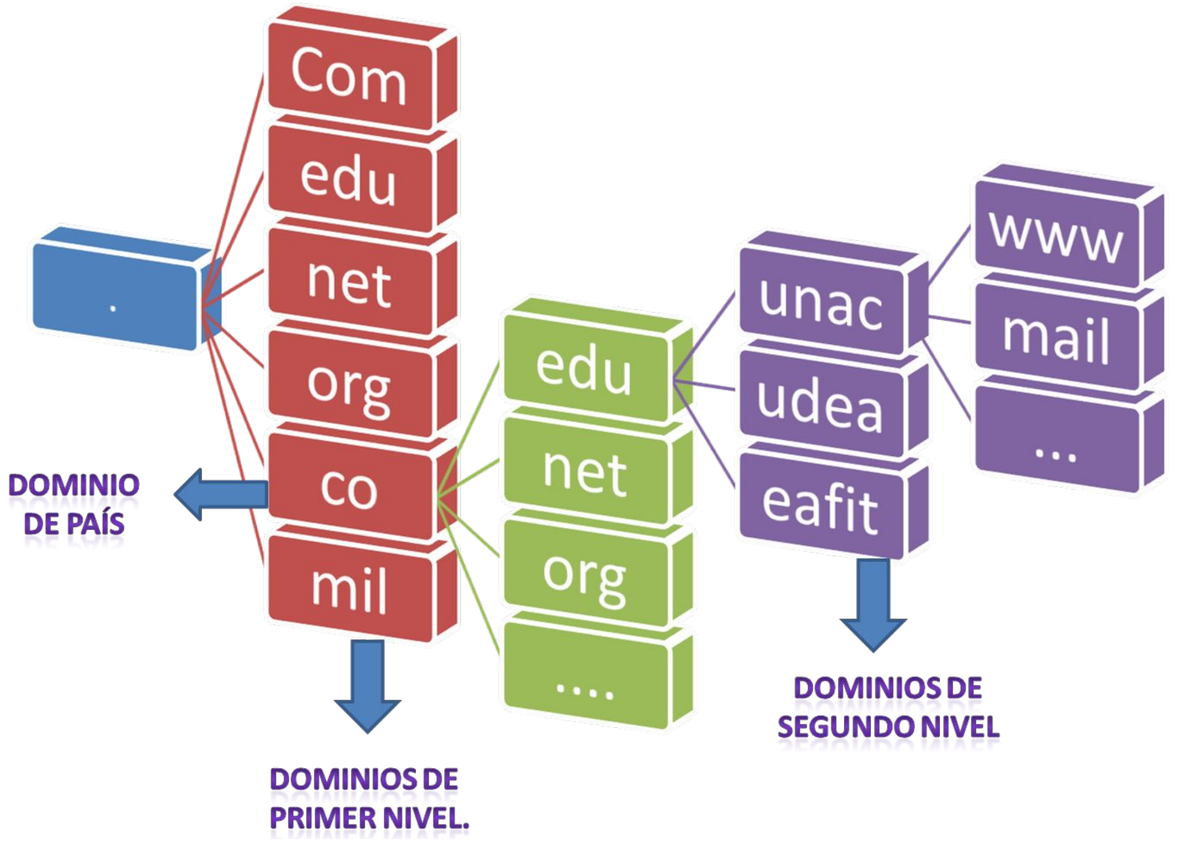
- En esta fase se busca recopilar toda la información básica acerca del objetivo para poder definir un plan de ataque.

- Ejemplos de información a recopilar :
  - Localización de la compañía
  - Residencia de la persona
  - Trabajadores de la compañía
  - Lugar de trabajo de la persona
  - Correos electrónicos
  - Infraestructura informática
  - Dominios
  - Subdominios
  - Direcciones IPs
  - Servidores
  - Ordenadores
  - Correos
  - Etc.
  - Metadatos en documentos públicos

https://intereconomia.com/noticia/empresas/recopilacion-de-informacion-sobre-empresas-base-para-generar-una-estrategia-empresarial-optima-20180321-1236/

Dominio

- Un **dominio web** es una dirección única para un **sitio web**.
- Es como la dirección física de tu sitio en Internet, permitiendo que los usuarios lo encuentren fácilmente sin necesidad de recordar direcciones IP complicadas.
- Un dominio web está formado por partes:
  - Dominio de Primer Nivel:
    - .com
    - .es
  - Dominio de Segundo Nivel:
    - Google
    - thebridge
  - Sub Dominios:
    - www
    - mail
    - ftp
- Por ejemplo,
  - www.Google.com
  - www.thebridge.tech

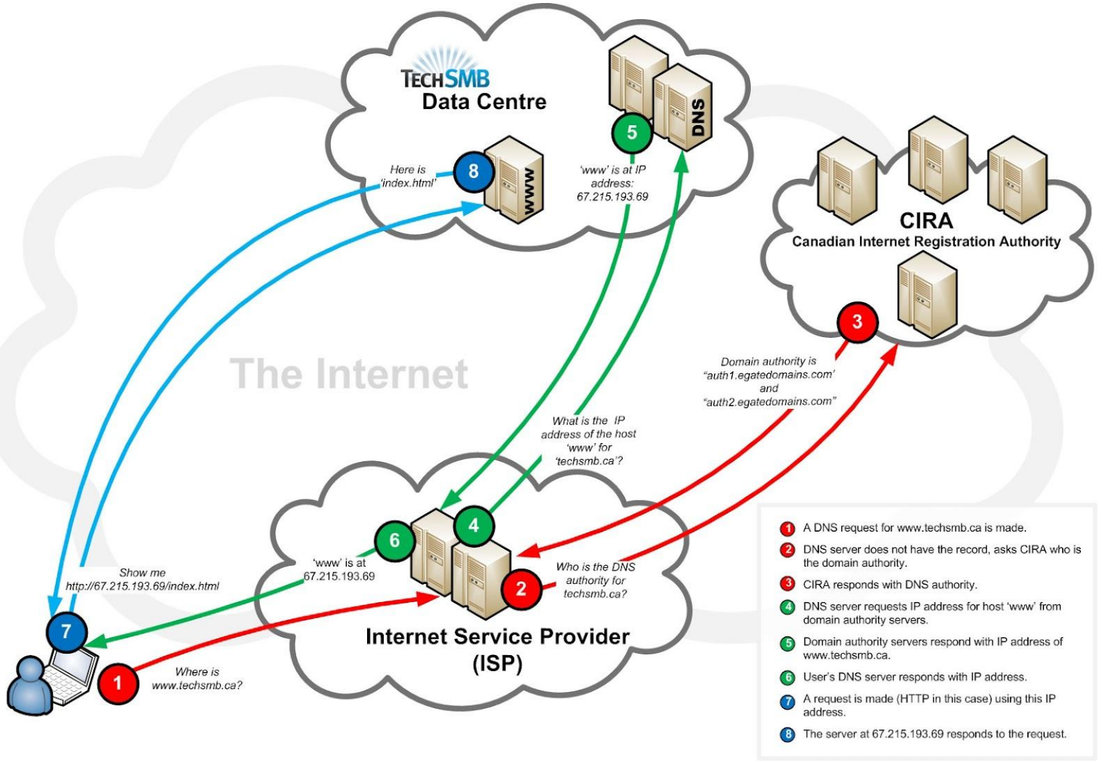


https://jhonjevisvergara.blogspot.com/2010/04/dominios-y-su-jerarquia.html

DNS

- El sistema de nombres de dominio (**Domain Name System** o **DNS**, por sus siglas en inglés) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

- Su función más importante es la resolución de nombres, «traducir» nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.



https://amar-linux.blogspot.com/2012/05/how-dns-works.html

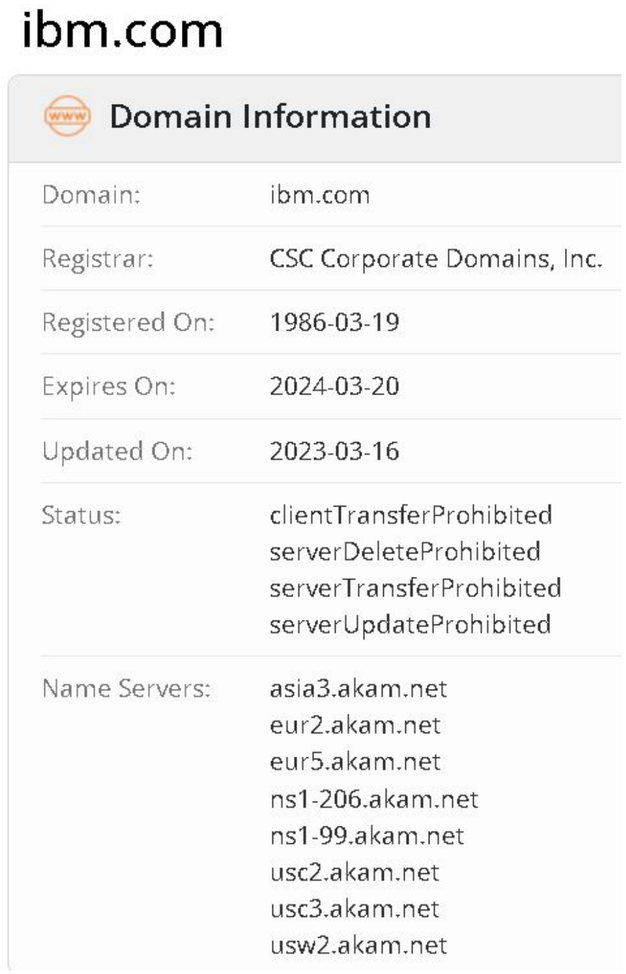
Registros del DNS

- Los **registros DNS** (también conocidos como archivos de zona) son instrucciones radicadas en servidores DNS autoritativos que proporcionan información sobre un dominio, como la dirección IP asociada con este y cómo gestionar solicitudes dirigidas a dicho dominio.
- Estos registros consisten en una serie de archivos de texto escritos en lo que se conoce como sintaxis DNS.
- La sintaxis DNS es simplemente una cadena de caracteres utilizados como comandos que dicen al servidor DNS qué hacer.

SOA	Inicio de autoridad. Fija los parámetros de la zona
NS	Servidor de Nombre. Nombre de un servidor autorizado para el dominio
A	Dirección de anfitrión. Asigna a un nombre una dirección
CNAME	Nombre canónico. Establece un alias para un nombre verdadero
MX	Intercambio de correo. Especifica qué máquinas intercambian correo
TXT	Texto arbitrario. Forma de añadir comentarios

REGISTROS WHOIS

- WHOIS (del inglés who is, «quién es») es un protocolo TCP basado en petición/respuesta para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet.
- Directorio gratuito y de acceso público que contiene la información técnica y los datos de registro del dominio
- Riesgo para la confidencialidad de datos personales
- Desde hace tiempo se aplican protecciones para garantizar la confidencialidad.
- Las consultas WHOIS se pueden realizar bien a través de una utilidad para línea de comandos, o bien a través de una multitud de páginas web públicas que permiten realizar estas consultas.



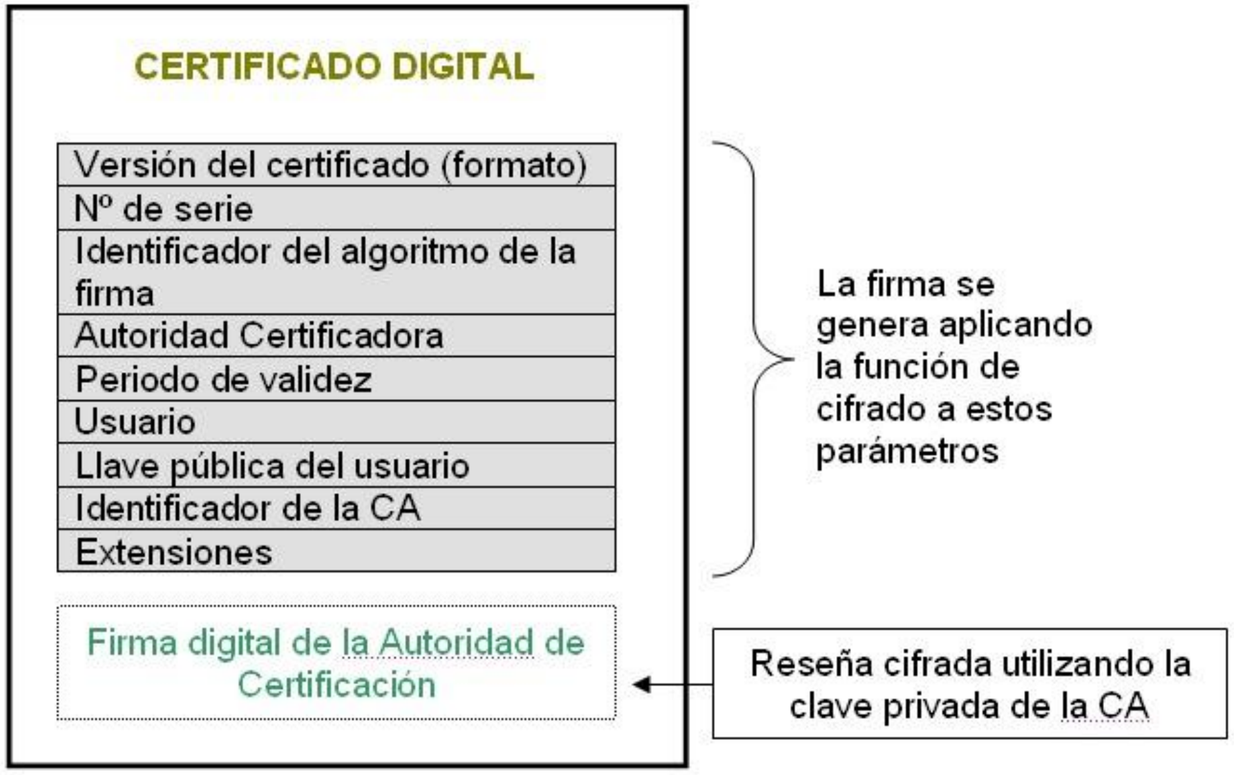
Certificado Digital

- El **certificado digital** es un archivo o documento en formato electrónico que se vincula con una determinada persona u organización y sirve para identificarla, a través de una clave pública y de forma fehaciente.

- Se emiten por parte de una autoridad de certificación.

- Información que almacena un certificado
  - Dominio al que identifica
  - Organización que lo emite.
  - Validez
  - Tamaño de la clave
  - Algoritmo de la firma

- Mediante el protocolo **OCSP** se confirma que un certificado es válido



http://rafasec.blogspot.com/2008/04/certificados-digitales.html

INTERNET SUPERFICIAL VS INTERNET PROFUNDA

- **Surface WEB**: Es la parte más conocida y utilizada de Internet. También se le llama "**Internet visible**" o "**Internet superficial**" y es todo lo que conseguimos con Google, Pilot, ChatGP, etc.

- **Deep Web** o **Web profunda** se refiere a todo el contenido en línea que no está indexado por los motores de búsqueda convencionales.

  - Esto incluye información privada como lo son:
    - bases de datos (Medica, Financieras, etc.)
    - Correos electrónicos.
    - archivos protegidos por contraseña (en la nube).
    - y otros recursos que no son accesibles directamente a través de búsquedas en Google o Bing.

- **Dark Web** o **Web oscura** es una parte específica de la **Deep Web** que requiere navegar a través de **redes anónimas** y utilizar herramientas como **Tor** para acceder.
  - Encontrarás sitios web y servicios que no están disponibles en la web convencional.
  - Algunos de estos sitios son legales, pero muchos otros están relacionados con actividades ilegales o cuestionables.

  - La **Dark Web** es un lugar **peligroso** y no se recomienda explorarla sin tomar precauciones adecuadas.

http://blogmoocencontrandotesoros.blogspot.com/2015/11/web-superficial-y-web-profunda.html

PERFIL TECNOLÓGICO VS PERFIL SOCIAL

- **PERFIL TECNOLÓGICO**
  - Datos tecnológicos :
    - Direcciones de correos electrónicos
    - Servidores
    - blogs
    - Dirección IPs
    - dominios
    - usuarios
    - etc.

- **PERFIL SOCIAL**
  - Identificación de datos sociales
    - Dirección de vivienda
    - usuarios de redes sociales
    - familia
    - etc.

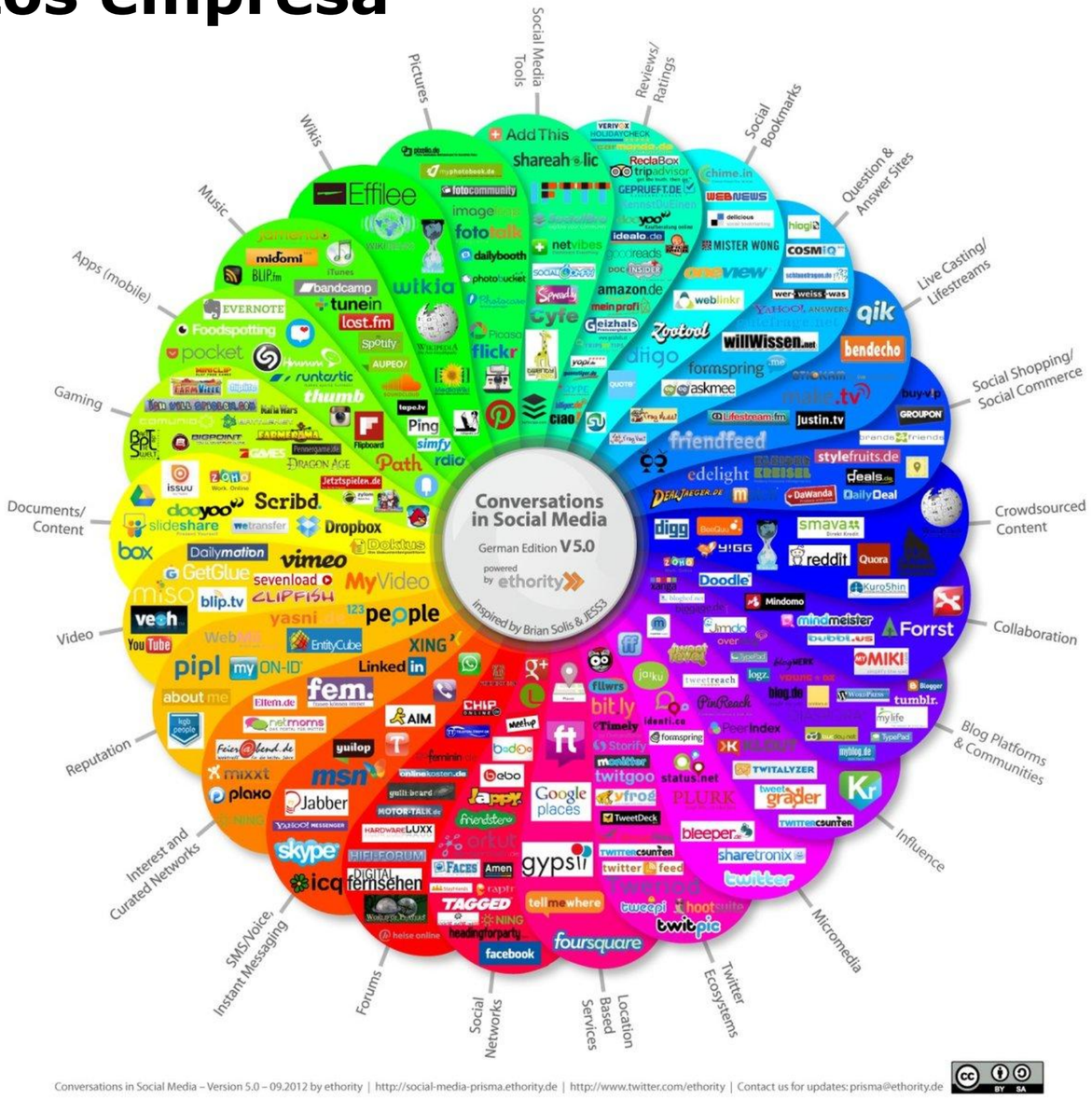
- **PERFIL FINANCIERO:**
  - Búsqueda en distintas herramientas del estado
    - Estados Financieros
    - BOE
    - Etc.

https://dagara.net/consejos-para-descargar-aplicaciones-de-forma-segura/

Informes Datos Personas vs Datos empresa

- **Personas**
  - Lugar de trabajo
  - Datos familiares
  - Lugares visitados
  - Amistades
  - Gustos personales
  - Gastos
  - Datos fiscales
  - Plantilla de Informe Personal

- **Empresas**
  - Sede social
  - Datos fiscales
  - Empleados
  - Cuentas de correo
  - Tecnologías utilizadas
  - Plantilla Informe empresas



https://hsb-akademie.de/warum-unternehme-social-media-brauchen/

Fases de gestión de OSINT

- **Requisitos**
  - es la fase en la que se establecen todos los requerimientos que se deben cumplir, es decir, aquellas condiciones que deben satisfacerse para conseguir el objetivo o resolver el problema que ha originado el desarrollo del sistema OSINT

- **Fuentes de información.**
  - Consiste en especificar, a partir de los requisitos establecidos, las fuentes de interés que serán recopiladas.
  - Hay que tener presente que el volumen de información disponible en Internet es prácticamente inabordable por lo que se deben identificar y concretar las fuentes de información relevante con el fin de optimizar el proceso de adquisición

- **Adquisición**.
  - Etapa en la que se obtiene la información a partir de los orígenes indicados

https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

Fases de gestión de OSINT

- **Procesamiento**.
  - Consiste en dar formato a toda la información recopilada de manera que posteriormente pueda ser analizada

- **Análisis**
  - Se genera inteligencia a partir de los datos recopilados y procesados.
  - El objetivo es relacionar la información de distintos orígenes buscando patrones que permitan llegar a alguna conclusión significativa

- **Presentación de Inteligencia**
  - consiste en presentar la información obtenida de una manera eficaz, potencialmente útil y comprensible, de manera que pueda ser correctamente explotada
  - Ejemplo: informeosint.pdf

https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

Metadatos

- En informática, también conocidos como "**datos sobre datos**", los **metadatos** se pueden definir como aquellos datos adicionales almacenados en un fichero, básicamente.

- Se clasifican en
  - **Contenido**: **Detallan el recurso en sí** y, por otro lado, se encuentran los metadatos que **describen el contenido de dicho recurso**

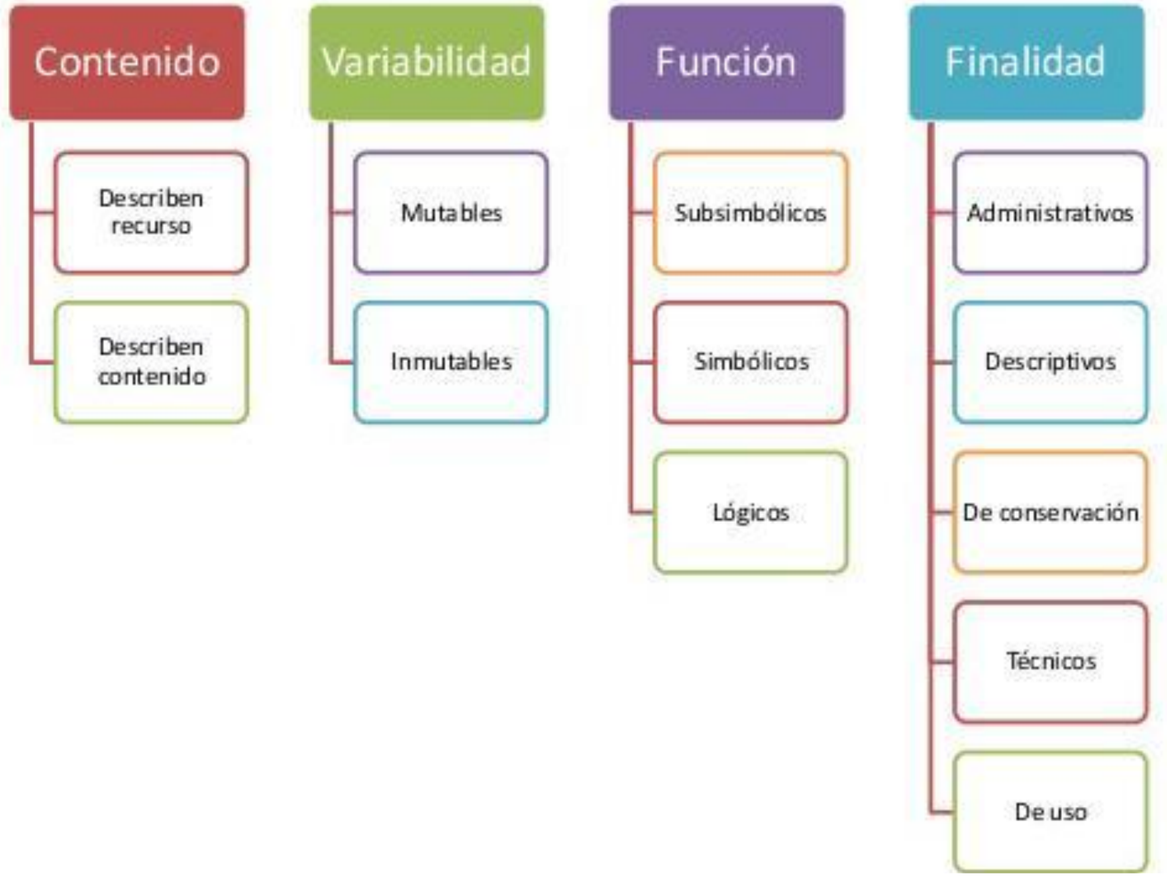
  - **Variabilidad:** hace referencia a los metadatos que son **inmutables** y no cambian, independientemente de la parte del recurso que sea visible. Y los **mutables** que se definen como aquellos que difieren de parte a parte y son diferentes de los demás

  - **Lógicos**: En el caso de los metadatos lógicos, se caracterizan por la compresión y son datos que explican cómo los datos simbólicos pueden emplearse para realizar deducciones de resultados lógicos.

  - **Simbólicos**: Son todos aquellos que agregan sentido y se ocupan de detallar los datos subsimbólicos.

  - **Subsimbólicos**: Estos últimos, sencillamente, no contienen ninguna información acerca de su significado.

  - Adicionalmente, se conoce otra clasificación que, aunque es la menos manejada, también es importante considerarla. Esta, secciona los metadatos dependiendo de su **finalidad** y contiene los siguientes tipos: De uso, de conservación, administrativos, descriptivos y técnicos.



https://internetpasoapaso.com/metadatos/

Framework

- **Ciber Patrulla**
  - Es una valiosa fuente de conocimiento para aquellos interesados en la inteligencia de fuentes abiertas y la investigación en línea.
  - Tiene un listado de herramientas open source que puedes usar en tus investigaciones.
  - https://ciberpatrulla.com/links/

- **OSINT Framework**
  - El Framework de OSINT es un recurso valioso para llevar a cabo investigaciones de inteligencia de fuentes abiertas (OSINT). Ya seas un profesional de la seguridad de la información, un investigador o simplemente curioso, esta plataforma ofrece una colección de herramientas y recursos para ayudarte a recopilar, analizar y visualizar datos de diversas fuentes.
  - Esto es lo que puedes encontrar en el Framework de OSINT:
    - Seguridad de la Información: Herramientas para OSINT relacionado con la seguridad.
    - Moneda Digital: Recursos relacionados con criptomonedas.
    - Motores de Búsqueda: Recopila información de motores de búsqueda populares.
    - Redes Sociales: Extrae datos de plataformas de redes sociales.
    - Direcciones de Correo Electrónico: Investiga cuentas de correo electrónico.
    - Y muchas otras categorías.
  - https://osintframework.com/


THE
BRIDGE