



**MANUEL BOT**

- 🇪🇸 Analista de Ciberinteligencia
- 💻 Desarrollador de Plataformas OSINT
- 🎤 Ponente y Docente OSINT y SOCMINT
- 🔍 Analista e Investigador #RedesSociales

# TEMARIO GENERAL

## INTELIGENCIA EN FUENTES ABIERTAS Y REDES SOCIALES (OSINT/SOCMINT)

DOCENTE:

**MANUEL TRAVEZAÑO**

# PRESENTACIÓN

Manuel Travezaño (“Manuel Bot”) es un analista OSINT de Perú, Investigador de Ciberinteligencia, Desarrollador de diversas Herramientas y Plataformas OSINT, CEO de “[OsintManuelBot](#)” (Comunidad OSINT de habla hispana en Telegram), Ponente y Docente en Inteligencia de Fuentes Abiertas (OSINT) con experiencia en Redes Sociales (SOCMINT).

En la actualidad, a través de su cuenta oficial en Twitter ([@ManuelBot59](#)), viene difundiendo investigaciones denominados (“El poder de los datos para OSINT”), con el único fin de llegar a la concienciación de usuarios sobre la mala exposición de sus huellas digitales y de los riesgos que podrían tener en el ciberespacio.

Asimismo, viene difundiendo herramientas, técnicas y utilitarios OSINT en todas sus plataformas digitales, permitiendo a los usuarios obtener conocimiento útil y eficaz para el desarrollo de sus ciberinvestigaciones.

Por lo señalado, Manuel Travezaño, presenta este temario general de todos los cursos publicados a través de la plataforma digital de UDEMY.

¡Muchas Gracias!

**Atentamente.**





## Conectividad

Conectados siempre con nuestra comunidad OSINT de habla hispana (a través de nuestros canales y grupos en Telegram)

## Certificación

A través de la plataforma de UDEMY, obtendrás un certificado de finalización de todos estos cursos OSINT y SOCMINT.



## Videos en HD

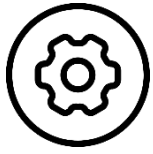
Clases pregrabadas o asíncronos con horas de video bajo demanda y con recursos descargables (presentaciones, proyectos y/o laboratorios).



## Valoraciones y Reseñas

A través de la plataforma de UDEMY podrás observar que, Manuel Bot, cuenta con más de 1000 estudiantes, recibiendo así buenas valoraciones y reseñas.





Aprende a proteger su identidad virtual a través de la creación de avatares digitales. Planifica, crea, analiza e investiga objetivos (emails, usernames, teléfonos, entre otros), realice Hacking con Buscadores, use Bots de Telegram para realizar OSINT, culminando con la formulación de un Informe de Inteligencia.

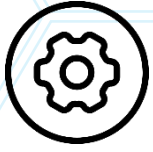
## TEMARIO

- Introducción al OSINT y SOCMINT.
- Securización de nuestra identidad, sistema operativo y entorno de trabajo.
- Uso del Google Cloud Shell para investigaciones OSINT.
- Protección, planificación y creación de avatares digitales.
- **OSINT.** Investigación ***básica*** de Objetivos (correos electrónicos, nombres de usuario, números telefónicos, entre otros).
- **SOCMINT.** Investigación ***básica y avanzada*** de personas en las redes sociales (Facebook, Instagram, Twitter y Youtube)
- Hacking con Buscadores, metabuscadores y personalizados.
- Uso de Bots de Telegram para ciberinvestigaciones.
- Redacción de Informe de Inteligencia.

[IR AL CURSO](#)



**MANUEL BOT**



En este curso conocerás desde 0 a investigar en las diferentes redes sociales, comprenderás los ciberriesgos y ciberamenazas existentes, aprenderás a proteger su identidad digital, sistema operativo y entorno de trabajo, con el uso de servicios VPN y en la nube; además utilizarás sistemas operativos virtuales como el Kali Linux y emuladores Android para la ejecución de herramientas OSINT. Asimismo, aprenderás a realizar el monitoreo de información de forma Activa y Pasiva, el uso de metadatos, uso de Bots de Telegram y muchos más.

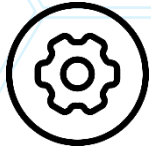
## TEMARIO

- **Bienvenida y primeros pasos.**
- **Introducción al OSINT y SOCMINT.**
- **Límites legales para la práctica del SOCMINT.**
- **Ciberriesgos y ciberamenazas para el Analista e Investigador.**
- **Securización de nuestra identidad, sistema operativo y entorno de trabajo.**
- **Uso del Google Cloud Shell y Máquinas virtuales.**
- **Uso de Red Privada Virtual - VPN.**
- **Uso de Emuladores Android para OSINT.**
- **Búsqueda de personas a través de OSINT y SOCMINT.**
- **OSINT. Búsqueda reversa de imágenes.**
- **Hacking con Buscadores y Metabuscaores.**
- **Niveles de navegación e indexación: Surface Web, Deep Web y Dark Web.**
- **Monitoreo de Información con Herramientas OSINT.**
- **Técnicas y Herramientas de búsquedas avanzadas de:**
  - **Datos e información de Targets (correos electrónicos, nombres de usuario, números telefónicos, entre otros).**
  - **Redes Sociales (Facebook, Instagram, Twitter, LinkedIn, YouTube, TikTok, Discord, Skype, entre otros).**
  - **Metadatos**
  - **Aplicaciones de Mensajería (WhatsApp, Telegram, WeChat)**
  - **Targets a través de Bots de Telegram.**

[IR AL CURSO](#)



**MANUEL BOT**



Con este curso conocerás las técnicas de investigación e inteligencia aplicados al OSINT, desde la fase de recopilación de información (Brecha de datos, scraping, entre otras herramientas OSINT), para su posterior análisis, procesamiento de datos para crear inteligencia. Además, aprenderemos a visualizar los datos de forma múltiple con las diversas herramientas como Power BI y otros. Comprenderás la Teoría de grafos y su aplicación con el uso de herramientas de representación gráfica para crear relaciones y vínculos que se encuentran entre 2 o más usuarios de una red social y muchos más.

## TEMARIO

- **Bienvenida y primeros pasos.**
- **Análisis y clasificación de las diferentes Redes Sociales.**
- **Límites legales para la práctica del OSINT/SOCMINT.**
- **Brecha de datos (Online y Offline)**
  - **Conceptos generales de Data Breachs y Data Leaks.**
  - **Red Social Facebook.**
  - **Red Social Twitter.**
  - **Red Social Instagram.**
  - **Red Social LinkedIn.**
  - **Aplicación de Mensajería WhatsApp.**
- **Web Scraping y automatización de obtención de datos.**
- **Visualización de datos con Microsoft Power BI.**
- **Teoría de grafos aplicada al Análisis de Redes Sociales.**
- **Representación y técnicas de Esquematización de datos.**
- **Herramientas de Representación gráfica de datos.**
  - **Recursos Web**
  - **Gephi**
  - **IB2 Security I2 Analyst's NoteBook.**
- **Monitoreo de Información Activa/Pasiva con Herramientas OSINT.**

[IR AL CURSO](#)



**MANUEL BOT**



La aplicación de mensajería de Telegram es hoy una de las más utilizadas. Su popularidad creció gracias a la privacidad y seguridad que brinda dicha aplicación. Creando así aplicaciones denominados "Bots", que se ejecutan sin necesidad de instalar nada, lo cual nos ayuda muchísimo para realizar ciberinvestigaciones OSINT, obteniendo así información valiosa de targets como correos electrónicos, números de teléfono, nombre de usuario, cuentas de usuario en redes sociales, entre otros. Con este curso aprenderás a investigar desde 0, empezando a securizar nuestra identidad, configuración y seguridad en Telegram, para el uso de estos Bots de Telegram.

## TEMARIO

- Breve Introducción al OSINT.
- Securización de nuestra identidad y entorno de trabajo para el uso de Bots de Telegram.
- Importancia de los Bots de Telegram para ciberinvestigaciones.
- Bots de Telegram para obtención de información:
  - Correos electrónicos, nombres de usuario, números telefónicos, Direcciones IP y geolocalización, búsqueda reversa de imágenes, entre otros.
  - Análisis de usuarios de Telegram (ID de usuario, Teléfonos vinculados, direcciones IP, Hora y Fecha de creación y conexión, modelo y marca del equipo móvil, ubicación, entre otros).
  - Exposición de contraseñas, números de teléfonos y correos electrónicos en Bases de Datos públicas.
  - Brecha de datos (Data Leaks y Data Breachs)
  - Vinculación de Targets con distintas Redes Sociales.
  - Verificación de Targets en Servicios Digitales.
  - Bots identificadores de llamadas, generadores de correos temporales.
  - Descargas de documentos, fotos y videos de sitios electrónicos y redes sociales.
  - Otros.

[IR AL CURSO](#)



**MANUEL BOT**



En la era digital actual, el concepto de **egosurfing** y la noción de huella digital se vuelven cada vez más relevantes y fascinantes. Egosurfearse implica la exploración de nuestra propia identidad en internet, mientras que la huella digital representa el rastro dejado por nuestras interacciones en la red. Estos dos temas son cruciales para entender cómo nuestra presencia en línea impacta nuestra identidad, privacidad y reputación en el mundo digital.

Con este curso, te capacitarás para gestionar tu presencia en línea de manera más efectiva y segura, aprendiendo a reducir tu huella digital y construir una imagen positiva en la web. Desde configurar opciones de privacidad hasta defenderte contra amenazas cibernéticas, esta experiencia formativa te sumergirá en el conocimiento necesario para navegar el mundo digital con mayor conciencia y control.

## TEMARIO

- **BIENVENIDA Y PRIMEROS PASOS.**
- **SIMULACIÓN DE CASO REAL PARA ESTE CURSO.**
- **DATOS GENERALES DE EGOSURFING Y HERRAMIENTAS DE RECOLECCIÓN DE INFORMACIÓN.**
- **INTRODUCCIÓN A LOS CONCEPTOS BÁSICOS:** Fuentes Abiertas, OSINT, Identidad digital, rastro o huella digital, Egosurfing y Doxing.
- **DATOS PERSONALES:** Normativa, límites legales, RGPD y LOPDGDD.
- **PROTECCIÓN DE LA PRIVACIDAD Y SEGURIDAD EN LÍNEA:** Avatares digitales, Securización de nuestros navegadores y OSINT en la nube.
- **TARGETS Y OTROS SERVICIOS DIGITALES:** Recopilación de datos de Nombres completos, emails, teléfonos y redes sociales.
- **GUÍA DE ELIMINACIÓN Y PRIVACIDAD EN LÍNEA:** Configuración de privacidad en GMAIL, FACEBOOK, X, entre otros.
- **Derecho de supresión al olvido, supresión en buscadores tradicionales, redes sociales, páginas adultas y acceso a soporte de sitios webs.**
- **TÉCNICAS DE ELIMINACIÓN EN LÍNEA:** Información histórica, exposición de credenciales y listas completas de eliminación de registros.
- **Directorios de eliminación de DATOS OBSOLETOS EN GOOGLE.**
- **MONITOREO ACTIVO/PASIVO DE REPUTACIÓN EN LÍNEA:** Consideraciones previas, beneficios del monitoreo de información.
- **HERRAMIENTAS DE MONITOREO:** registros, correos electrónicos y monitorización de personas en la DarkWeb.

[IR AL CURSO](#)



**MANUEL BOT**





Conocer la Importancia en el empleo del OSINT y SOCMINT para resolver ciberinvestigación es muy indispensable, porque permite abrir panoramas de análisis, estrategia, y procesamiento de datos a través de sus registros digitales.

El empleo de métodos, técnicas y herramientas OSINT dedicados exclusivamente a las redes sociales (SOCMINT) se ha visto incrementado de manera exponencial, todo esto es debido a que su uso está cada vez más extendido en distintos campos de: Ciberinteligencia y Ciberseguridad.

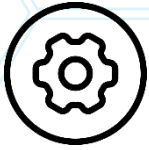
## TEMARIO

- **Bienvenida e Introducción.**
- **Introducción a los conceptos básicos de Inteligencia y Ciberinteligencia, OSINT y SOCMINT.**
- **Introducción a los conceptos básicos de Huellas Digitales**
- **Formas de Huellas Digitales.**
- **Objetivos de Investigación en OSINT y SOCMINT.**
- **La importancia del OSINT y SOCMINT en las ciberinvestigaciones.**
- **Casos reales en el empleo del OSINT y SOCMINT.**
- **Casos reales de GEOINT, IMINT.**
- **Aplicando el uso del OSINT en las ciberinvestigaciones.**
  - **Nombres de usuarios**
  - **Correos electrónicos**
  - **Números de teléfonos**
- **Aplicando el uso del SOCMINT en las ciberinvestigaciones.**
  - **Facebook**
  - **Instagram**
  - **Twitter**
  - **WhatsApp**
  - **Telegram**
- **Compilación de herramientas OSINT y SOCMINT.**

[IR AL CURSO](#)



**MANUEL BOT**



En el mundo actual, la información es poder. Para los analistas e investigadores, la capacidad de recopilar información e inteligencia es esencial para su trabajo. Una herramienta que se ha hecho cada vez más popular entre los investigadores son los bots OSINT de Telegram.

Estos bots están diseñados para recopilar información de diversas fuentes en Telegram, una popular aplicación de mensajería. En este artículo, exploraremos por qué los investigadores y analistas utilizan los bots OSINT de Telegram y cómo pueden beneficiar a las ciberinvestigaciones.

## TEMARIO

- **¿Qué son los bots Telegram OSINT?**
- **¿Cómo funcionan los bots Telegram OSINT?**
- **¿Por qué los investigadores usan bots Telegram OSINT?**
- **Beneficios y posibles inconvenientes en el uso de bots Telegram para OSINT.**
- **Preguntas frecuentes sobre los bots Telegram OSINT.**
  - **¿Es legal el uso de bots de Telegram para las investigaciones?**
  - **¿Son precisos los bots Telegram OSINT?**
  - **¿Pueden los Bots de Telegram OSINT acceder a canales o mensajes privados?**
  - **¿Cómo elijo el Bot de Telegram OSINT adecuado para mi investigación?**
- **TIPS para mejorar la calidad de información usando Telegram BOTS para OSINT.**
- **OSINT en sectores privados**
- **Puntos a tomar en cuenta.**
- **Conclusiones**

[IR AL CURSO](#)



**MANUEL BOT**



# MANUEL BOT

♥ Analista e Investigador 🇪🇸 | 🧑‍💻 Analista Táctico de Ciberinteligencia | 🗣️ Ponente y Docente OSINT / SOCMINT | 🌟 #RedesSociales 🔗 |