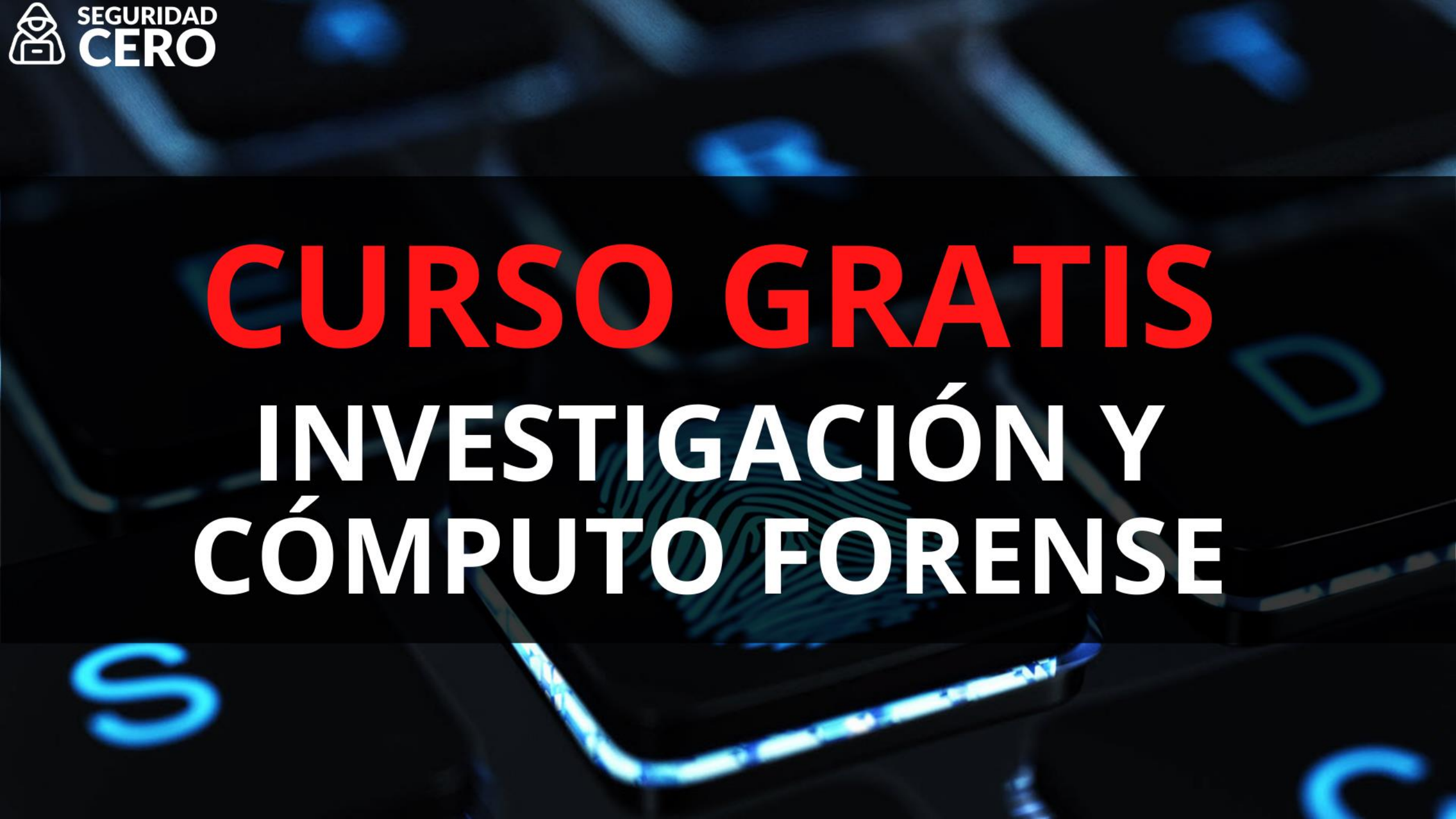

SEGURIDAD
CERO
CURSO GRATIS
INVESTIGACIÓN Y
CÓMPUTO FORENSE

SEGURIDAD CERO

PROGRAMA COMPLETO

INVESTIGACIÓN Y CÓMPUTO FORENSE

~~600 USD~~ 239USD

Presiona aquí

SEGURIDAD CERO

CLASE #4

Descubriendo al Criminal

JUEVES 26 NOVIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	6:00 PM	7:00 PM
				

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	9:00 PM
				

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM
				

SEGURIDAD CERO

Fernando Conislla

Cybersecurity Expert

- Años de experiencia en servicios de ciberseguridad para entidades gubernamentales, bancarias, medios de pago, etc.
- Instructor SEGURIDAD CERO e instructor oficial ISO 27001
- Expositor en eventos internacionales
- Master en gestión y dirección de la ciberseguridad
- Certificaciones internacionales CEH, ISO 27001 LA, LCSPC.

SEGURIDAD CERO

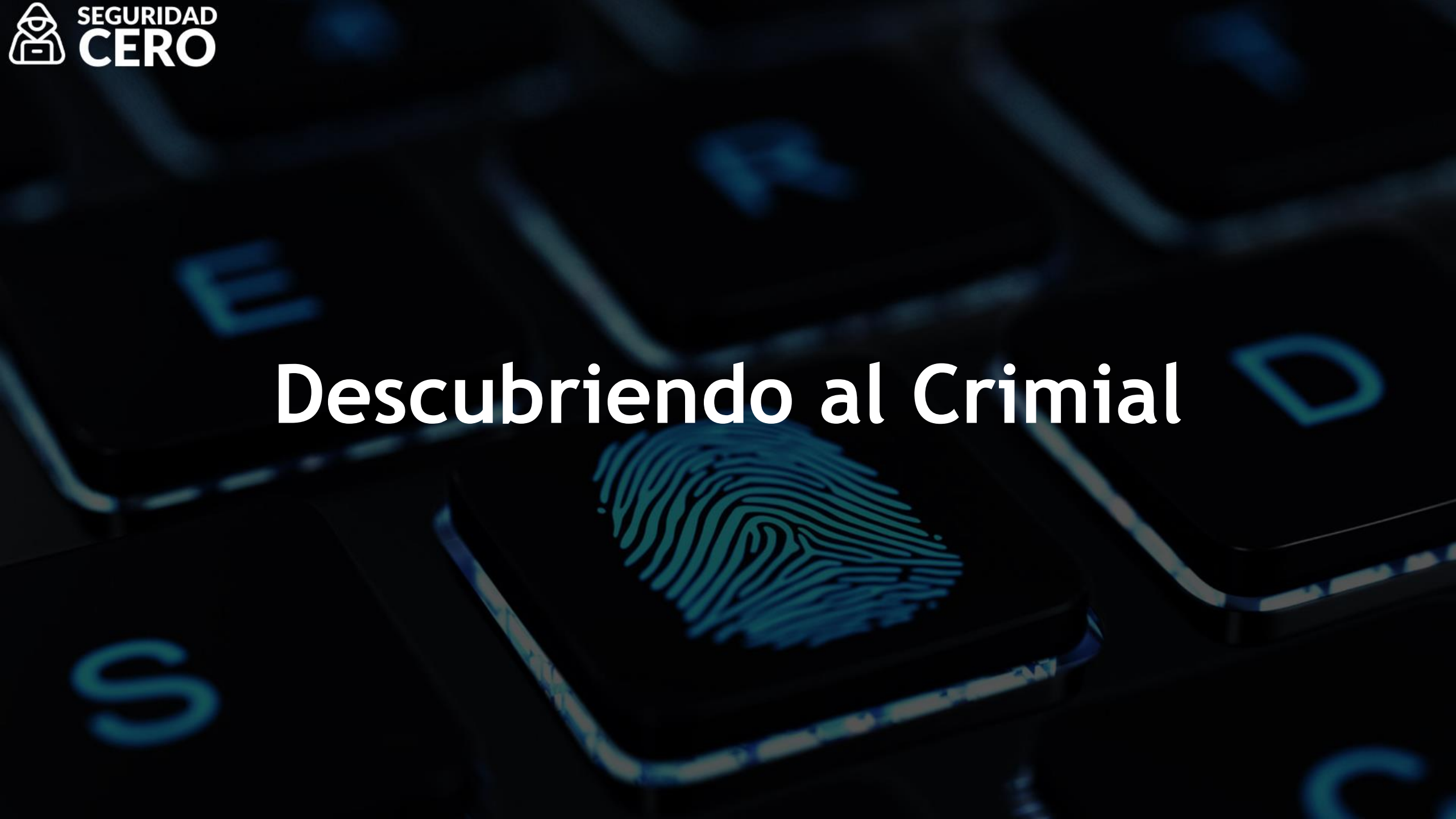
Ingrid Santisteban

Computer Forensic Investigator

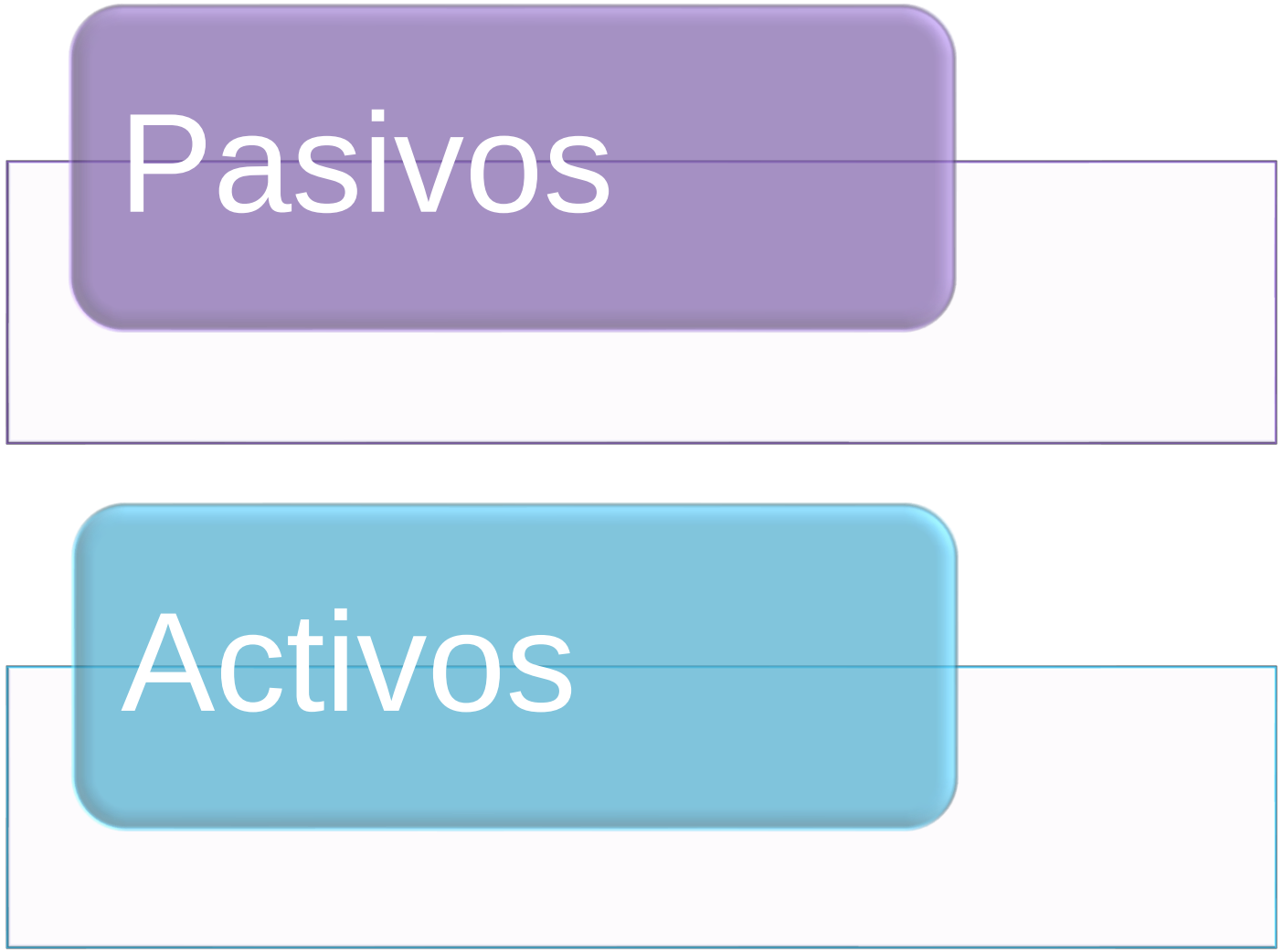
- Experta en la investigación de delitos informáticos, forense digital, auditoria y riesgos de TI.
- Instructor en SEGURIDAD CERO
- Maestría en Informática Forense y Seguridad de la Información
- Certificada internacionalmente como Investigador Digital Forense (IDF)

SEGURIDAD CERO

Descubriendo al Crimial



Tipos de Atacante



Los atacantes pasivos son los que se encargan de observar el sistema sin modificar ni destruir nada.

Los atacantes activos tienen como propósito dañar el objeto que ataca y modifican a su favor

Algunos tipos de atacantes

Personal de la Organización:

El propio personal de trabajo de cualquier compañía o empresa puede producir un ataque intencionado para sabotear algún sistema a su favor, aprovechándose de los privilegios de acceso que le han sido concedidos o de privilegios de cuentas de usuario prestadas o a las que pudo tener acceso por su vulnerabilidad.

Hacker

Es un experto en encontrar las vulnerabilidades de los sistemas, y se encarga de solventarlos, por lo regular los hackers trabajan del lado del bien, pero al buscar el lado oscuro pueden aprovechar sus conocimientos para explotar las vulnerabilidades que encuentran.

Cracker

Es un experto en informática que utiliza sus conocimientos con objetivos ilegales (robo de contraseñas, difundir virus, vulnerar sistemas, etc.), por lo regular realiza estas actividades ilícitas para obtener beneficios económicos.

¿Qué es un Ataque Informático?

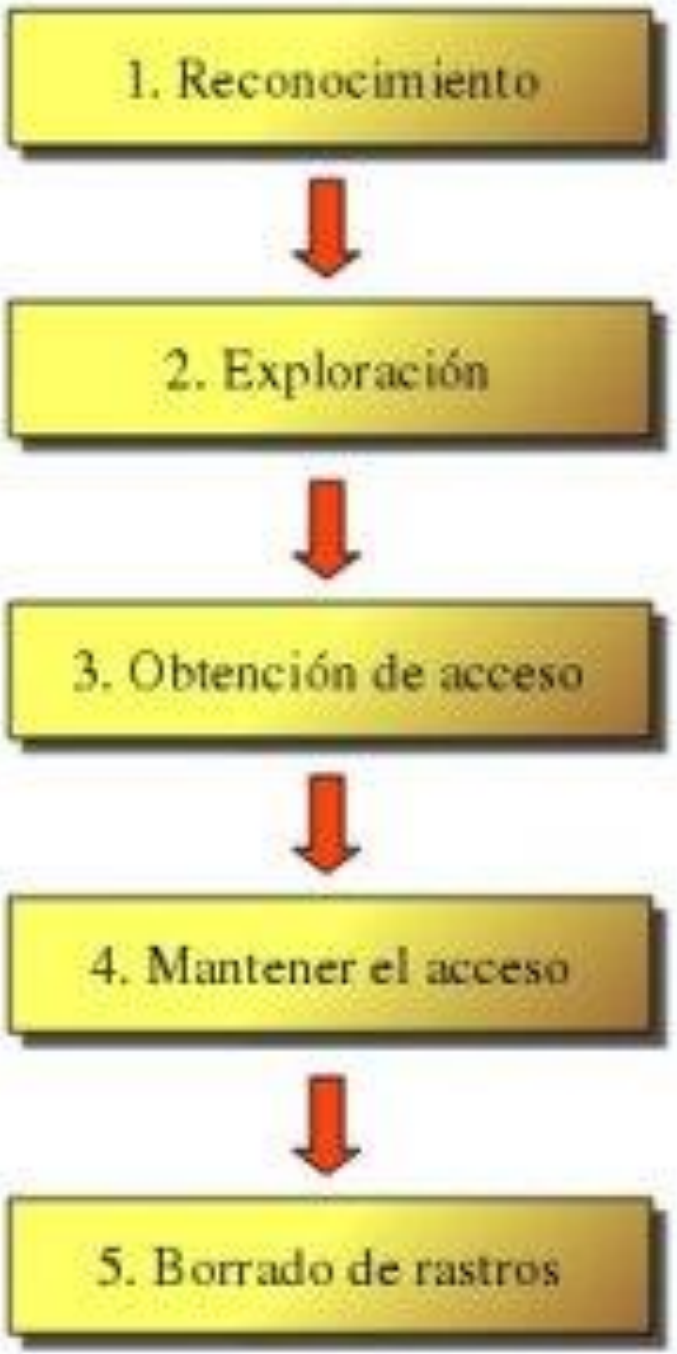
- Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) existente en un sistema o en el hardware, e incluso, en las personas o usuarios,; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

- Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques. Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas

Anatomía de un ataque informático

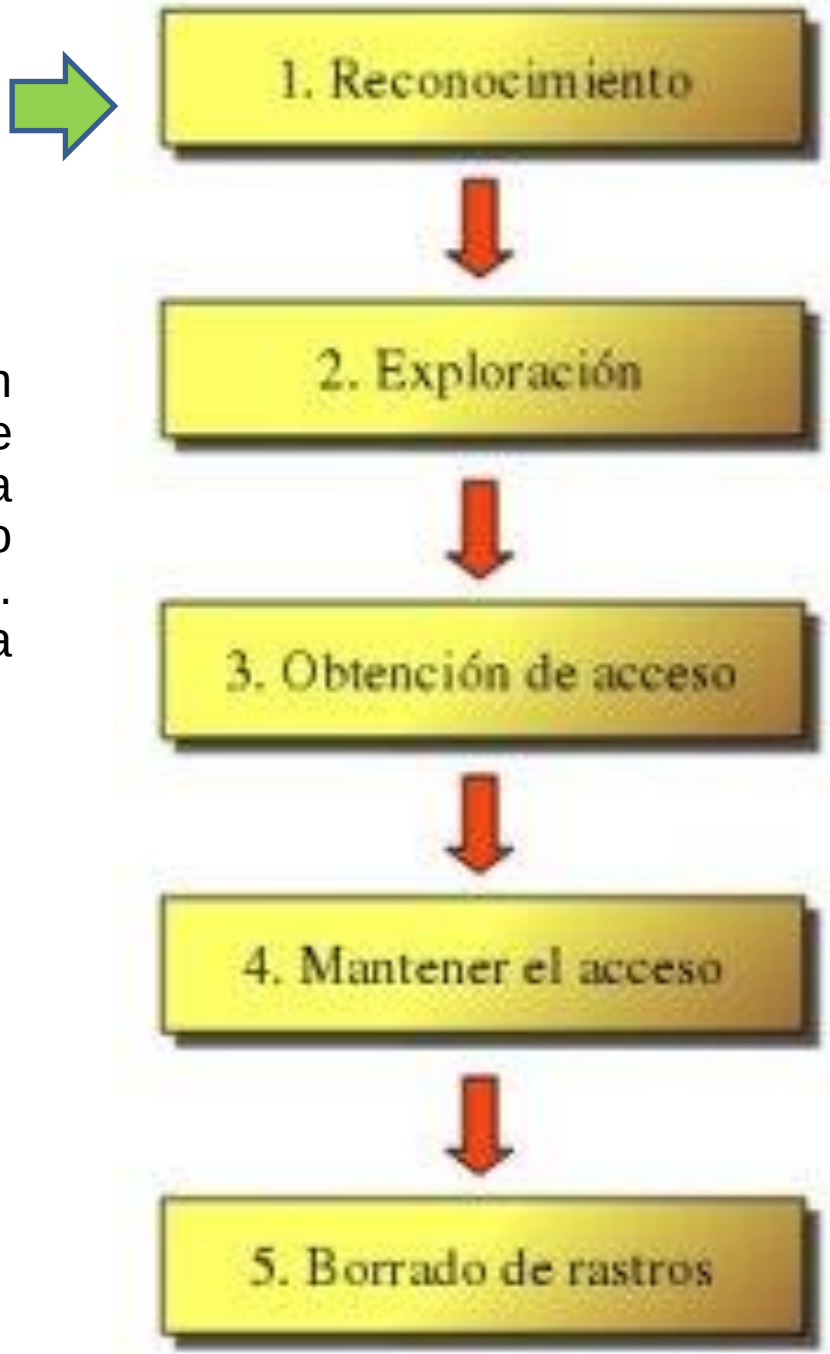
Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad.

Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.



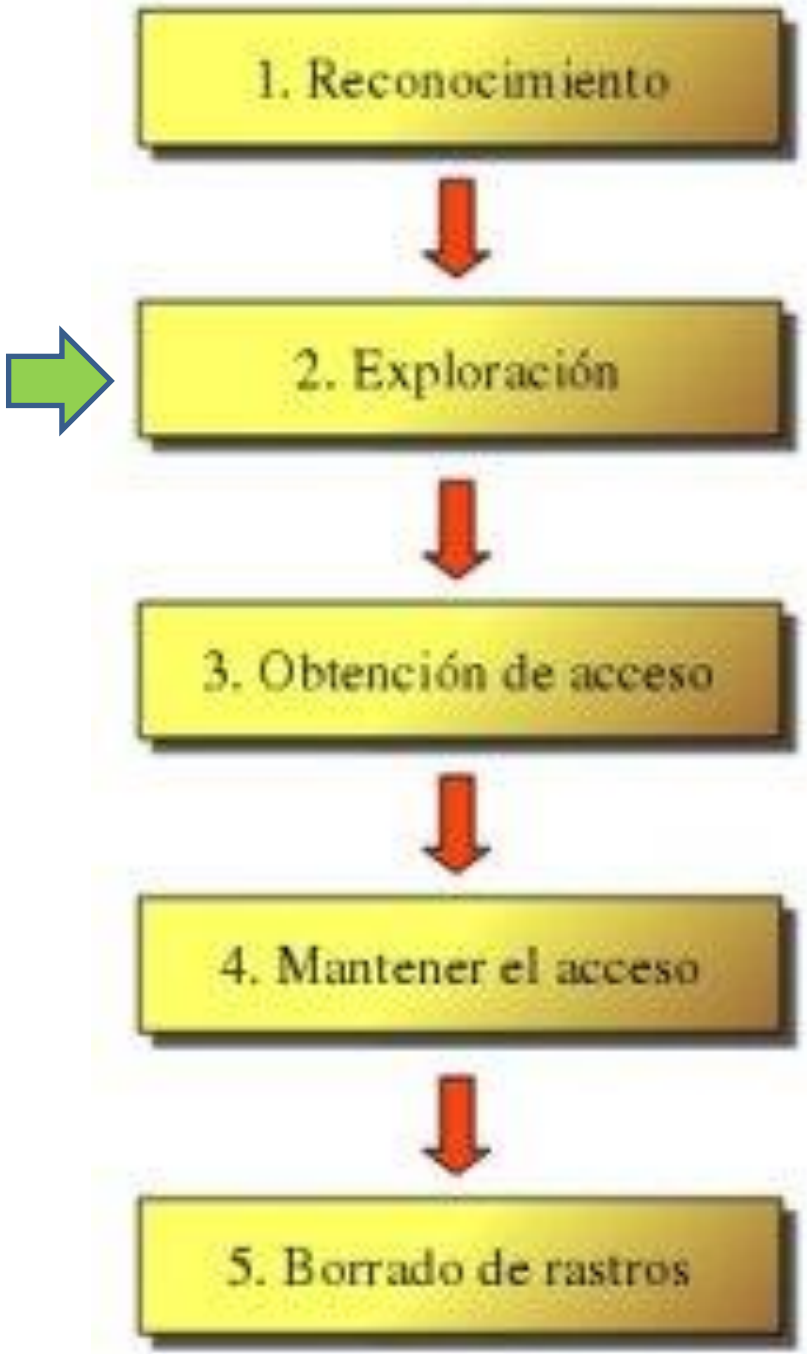
1. Reconocimiento

Esta etapa involucra la obtención de información (Information Gathering) con respecto a una potencial víctima que puede ser una persona u organización. Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving, el sniffing.



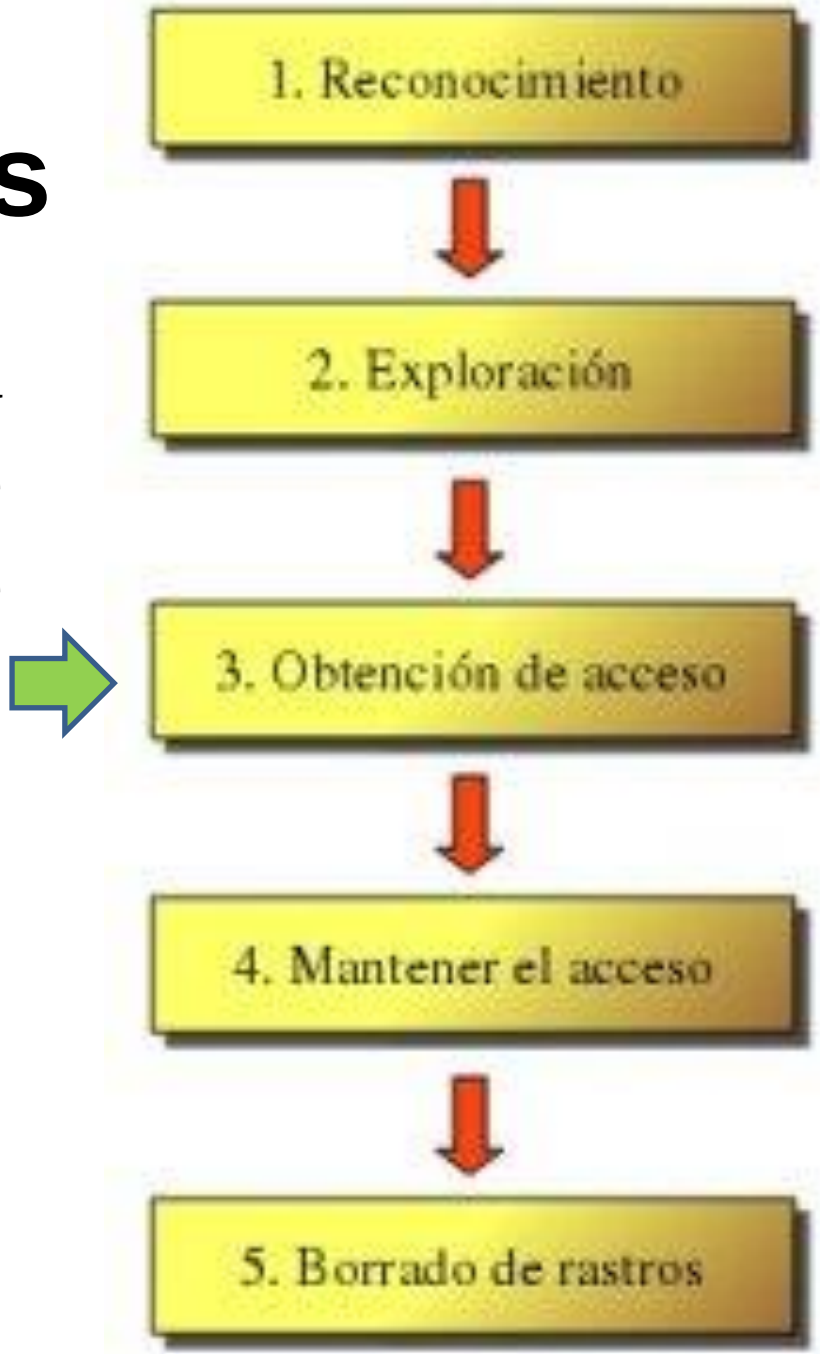
2. Exploración

En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros. Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.



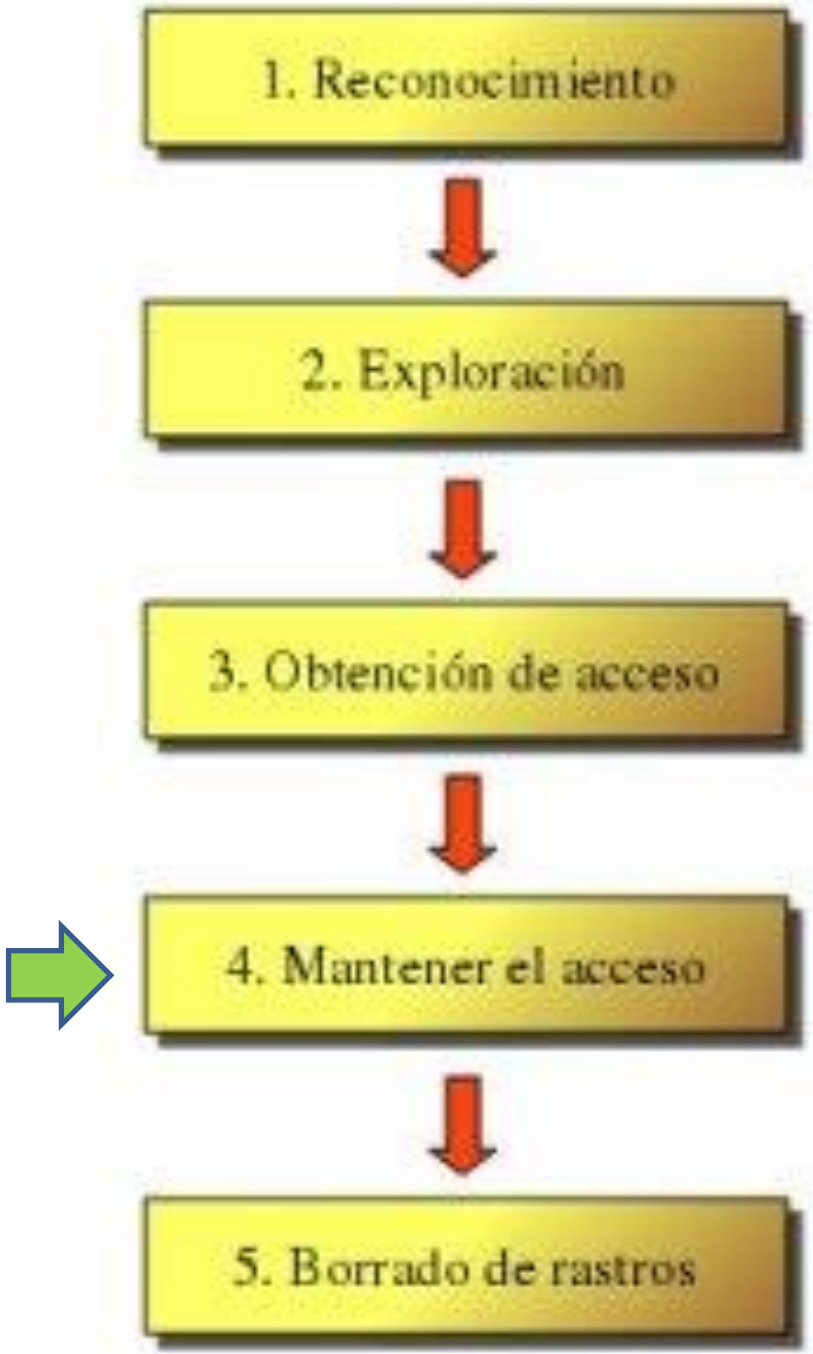
3. Obtención de accesos

En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento y exploración. Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking.



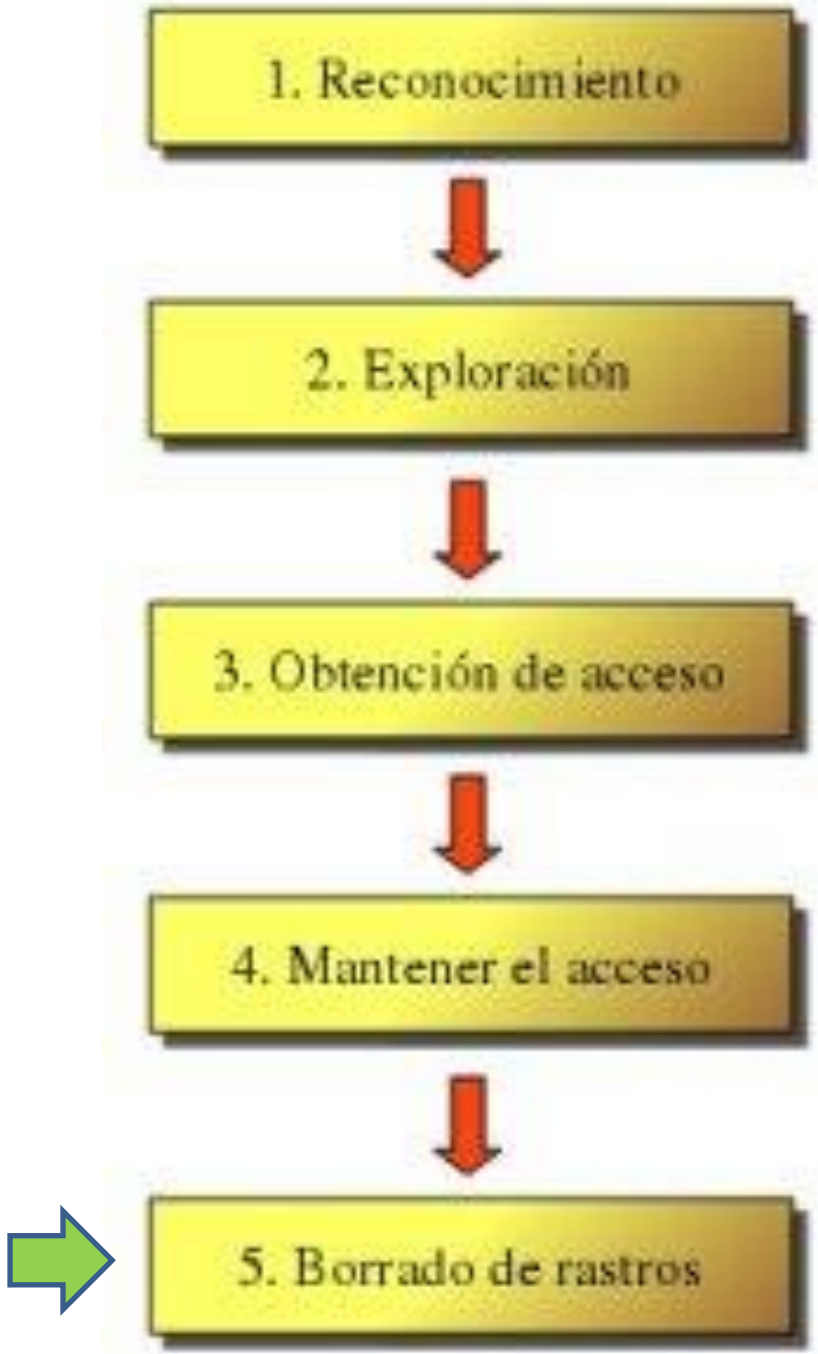
4. Mantener el acceso

Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos



5. Borrando los rastros

Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS)



SEGURIDAD CERO

CLASE #4

Descubriendo al Criminal

JUEVES 26 NOVIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	6:00 PM	7:00 PM
				

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	9:00 PM
				

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM
				

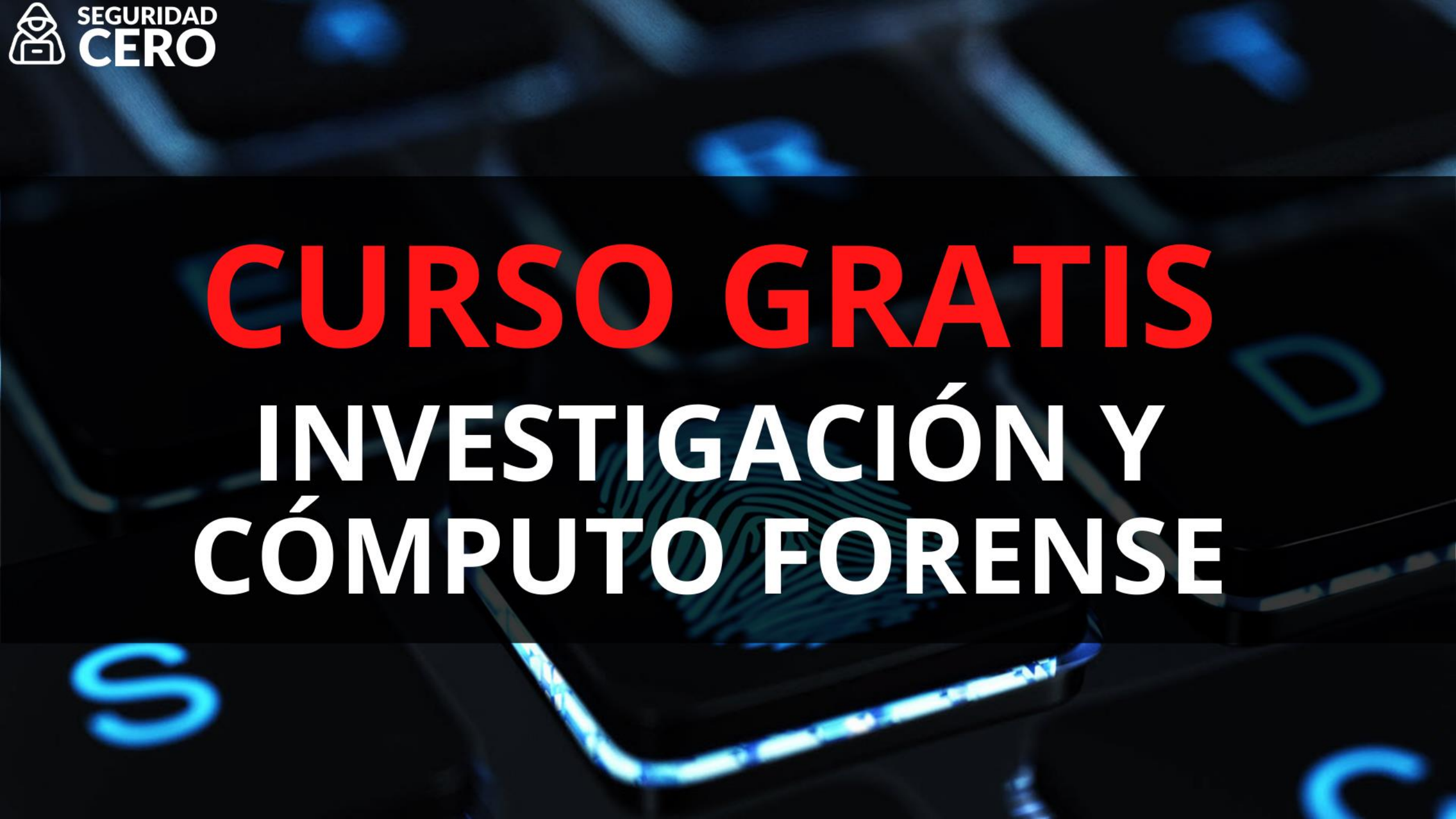
SEGURIDAD CERO

PROGRAMA COMPLETO

INVESTIGACIÓN Y CÓMPUTO FORENSE

~~600 USD~~ 239USD

Presiona aquí


SEGURIDAD
CERO
CURSO GRATIS
INVESTIGACIÓN Y
CÓMPUTO FORENSE