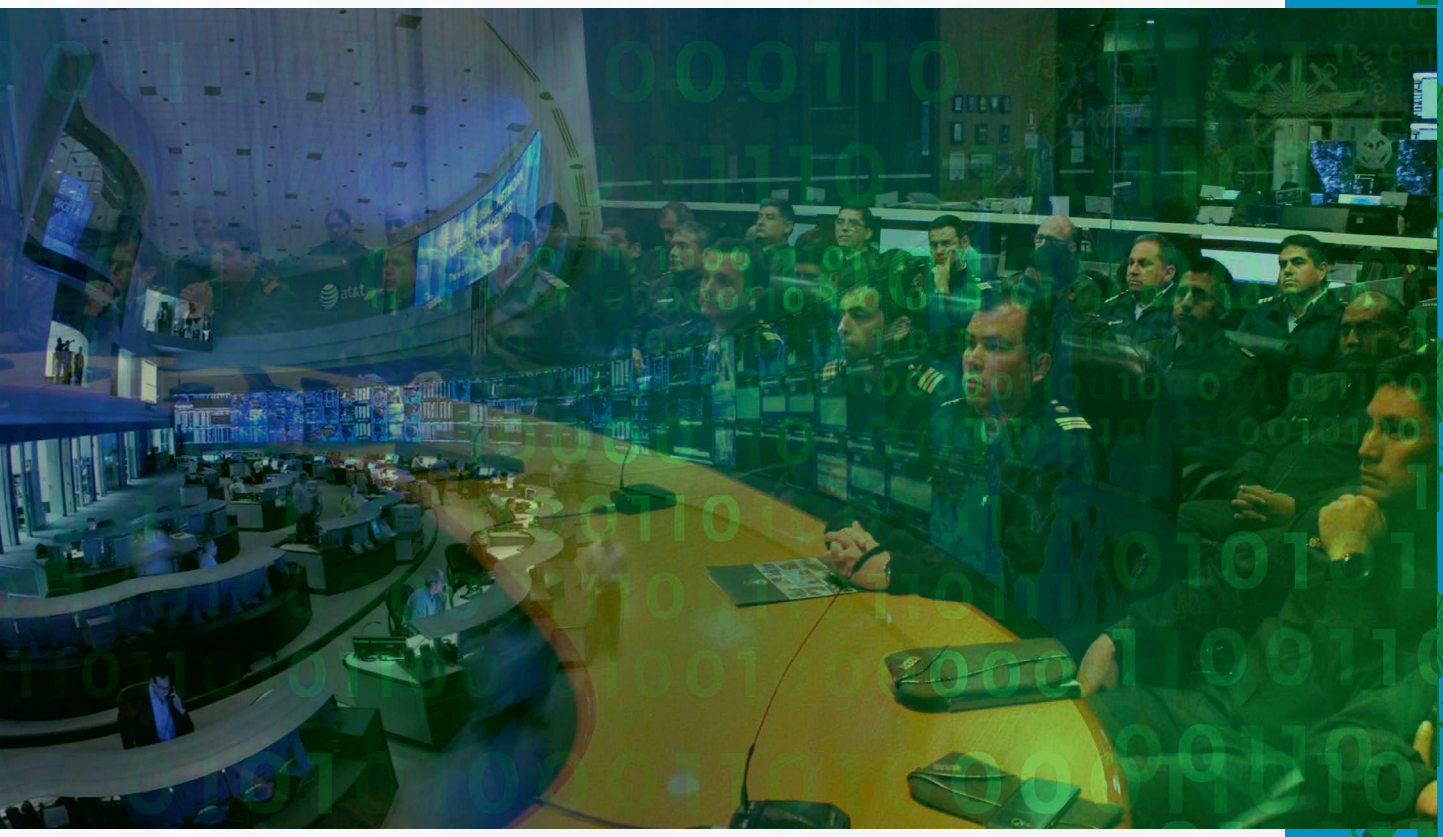
El autor presenta una breve descripción de las lecciones aprendidas en operaciones de Ciberdefensa, y el poco conocimiento de las Fuerzas que participan en ellas, sobre las intenciones, el accionar y pensamiento de los actores de la amenaza a la seguridad digital, los mismos que pretenden romper el eslabón más débil de las infraestructuras digitales que son los usuarios.

La Ciberdefensa, "Operaciones Invisibles"



The author presents a brief description of the relevance of the lessons learned in the Cyberdefense operations and the little knowledge of the Armed Forces and the National Police, about the actions and thinking of the actors of the threat to Digital security, which aims to break the Weakest link in digital infrastructures that are users.

Ronald Russo Valcárcel

Comandante de la Fuerza Aérea del Perú. Especialista en Inteligencia. Ostenta los grados académicos de bachiller en administración por la Universidad Nacional Federico Villarreal, maestro en Doctrina y Administración Aeroespacial por la Escuela Superior de Guerra Aérea. Ha sido profesor de cursos relacionados con Inteligencia y Ciberinteligencia en la Escuela Superior Conjunta de las Fuerzas Armadas, Escuela de Oficiales de la FAP, y en la Escuela de Inteligencia de la FAP. Actualmente es Oficial nombrado en la Dirección Nacional de Inteligencia (DINI).

Russo Valcárcel, R. (2020). "La Ciberdefensa, 'Operaciones Invisibles' ". *Pensamiento Conjunto,* Año 8, Núm 2, pp. 89-95.
ISSN° 2707-3661

"En el país de los ciegos el tuerto es el rey"
Erasmo de Rotterdam[1]

Antes de iniciar el tema, quería explicar el porqué del título, ya que a medida que se avance en la lectura se podría diluir un poco la comprensión de la misma. En alusión al título tendríamos que llamar a la frase "En el país de los ciegos el tuerto es el rey" de Erasmo de Rotterdam, hacen alusión a que gran parte de la población en el país y entre ella las Fuerzas de seguridad y defensa, desconoce el escenario operacional y el submundo que existe en el ciberespacio, ese desconocimiento es aprovechado por diferentes Actores (Gubernamentales o personas de mal vivir virtual), por ende este gran conocimiento (información) de este porcentaje de Actores, cumple con la teoría de él que cuenta con gran información de una persona de la calle como de una institución de gran prestigio, lo lleva a tener el control de la economía, política y otros factores de la vida cotidiana de la población, convirtiéndose en el rey en un país de ciegos.

1 ANTECEDENTES

Para entender este complicado escenario debemos empezar por conocer nuestras capacidades como las amenazas existentes contra la seguridad y defensa nacional; y en ese sentido pasaremos a describir algunos conceptos.

Los sistemas telemáticos están constituidos por una serie de componentes como son el personal especialista, software, hardware, comunicaciones, y entre ellos las redes de datos, que contienen una gama de información asociada a la Seguridad y Defensa Nacional, que es de suma importancia para

1 Desiderio Erasmo, su verdadero fue Geert Geertsz, se caracterizó por la independencia de pensamiento. https://sites.oxy.edu/guillenf/espanol302/recursos/galeria%20de%20im%C3%A1genes/personajeshist%C3%B3ricos/erasmo%20de%20rotterdam.html

PALABRAS CLAVE: INFRAESTRUCTURA DIGITAL, NIVELES DE SEGURIDAD, AMENAZA A LA SEGURIDAD DIGITAL, ACTOR, OPERACIONES DE CIBERDEFENSA.
KEYWORDS: DIGITAL INFRASTRUCTURE, SECURITY LEVELS, THREAT TO DIGITAL SECURITY, ACTOR, CYBER DEFENSE OPERATIONS.

la adecuada gestión y toma de decisiones en los diferentes niveles de la organización Institucional; por tal razón, podrían existir muchas entidades o personas ajenas a las Fuerzas Armadas que se encuentren interesadas en acceder a dicha información con fines de causar perjuicios a las mismas.

Extendida esta la afirmación relativa a la inexistencia de seguridad perfecta y, por más avanzados que se encuentren los sistemas telemáticos, siempre hay la posibilidad de vulnerar su protección y acceder a la información que contienen. Consecuentemente, las Instituciones Armadas constantemente están expuestas a que sus redes de datos puedan ser penetradas, interferidas o dañadas por entidades extrañas, es decir de actores que amenazan la seguridad digital.

También es preciso mencionar que de acuerdo con las estadísticas mundiales, el 70% de los ataques son de carácter interno por algún conflicto de intereses o desconocimiento natural del personal, situación que resulta más crítica debido a que desde dentro de la red de datos es mucho más fácil vulnerar los sistemas, dado que los medios de seguridad usualmente están destinados a proteger las bases de datos ante un ataque externo.

2 MEDIDAS DE SEGURIDAD

La información que se intercambia a través de los medios de comunicaciones debe ser protegida a fin de garantizar su confidencialidad, integridad y disponibilidad; por lo tanto las medidas de seguridad de las comunicaciones resultan de vital importancia para el éxito de las operaciones militares.

Asimismo, las medidas que deben adoptarse para proporcionar la seguridad de las comunicaciones consideran al personal, material, información e instalaciones, mediante el empleo de medios físicos, técnicos, tales como: equipamiento, programas (software) y procedimientos especiales.

Para tal efecto, las Fuerzas Armadas cuentan con un conjunto de medidas, como la implementación de Centros de Operaciones (SOC),[2] equipos de personas selectas, altamente capacitadas; así como, herramientas tecnológicas (Hardware y Software) especializadas en seguridad tales como: firewalls [3]correlacionador de eventos de seguridad (SIEM),[4] sistemas de prevención de fuga de Información, analizadores de vulnerabilidad, análisis forense, sistemas de detección y prevención de intrusos, etc.; a fin de realizar eficientemente las funciones y/o tareas de gestión, control y monitoreo de las incidencias de seguridad en la red de datos de las Instituciones Armadas.

Los indicados Controles de seguridad algunas veces son configurados con tres anillos de seguridad, como a continuación se describe:

- El primer anillo de seguridad perimetral establecido en la red de datos, es controlado y monitoreado a través del firewall “Checkpoint”; el mismo que tiene como función principal, brindar protección a la red de Servidores Institucionales (Base de Datos, Intranet, Servidor de Aplicaciones, Red Administrativa, Servidor de Proceso de Pagos).
- El segundo anillo de seguridad perimetral establecido en la red de datos, es controlado y monitoreado a través del firewall “SonicWall”; el mismo que se encarga de brindar protección y permisos para el acceso a las diversas VLAN’s.[5] Asimismo restringe el acceso a páginas WEB mediante su módulo de filtro de contenidos y a su vez permite

2 El Centro de Operaciones de Seguridad, SOC, se refiere al equipo responsable de garantizar la seguridad de la información. https://www.oracle.com/es/database/security/que-es-un-soc.html

3 Es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

4 Tiene como objetivo principal ayudar a las empresas a construir un centro de operaciones de seguridad, para centralizar información de múltiples fuentes y, además, brindar la posibilidad de identificar ataques complejos que afecten múltiples puntos a la vez. https://www.teamnet.com.mx/blog/qu%C3%A9-es-un-correlacionador-de-eventos-y-qu%C3%A9-puede-ayuda-a-mitigar

5 VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. https://soporte.syscom.mx/es/articles/2042744-networking-diferencias-en-configuraciones-de-vlans

realizar una inspección profunda de paquetes con la finalidad de prevenir y detectar posibles intrusiones a la red (IPS).[6]

- El tercer anillo de seguridad perimetral establecido en la red de datos, es controlado y monitoreado a través del firewall "Juniper"; el mismo que brinda protección a las amenazas que llegan directamente desde Internet tales como: gusanos, spyware, troyanos, y malware. Asimismo se encarga de natear[7] (mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles) las direcciones IP's privadas de los servicios que se encuentran publicados en Internet (servicio vpn,[8] correo, páginas web).

Asimismo, para la protección de los Correos Institucionales ubicado en la DMZ[9] (Zona Desmilitarizada), algunas veces se adquiere un equipo de seguridad de correo electrónico IRONPORT (antispam); el mismo que se encarga de brindar protección al Servidor de Correo contra el spam entrante (correo no deseado) y ataques de virus por mensajes. Al respecto, estos equipos cuentan con un módulo para la encriptación de correos y otro para la prevención de fuga de información de mayor clasificación de seguridad (pérdida de datos críticos).

En cuanto a las disponibilidad de medios es importante mencionar que las Instituciones cuenta con plataformas de comunicaciones alámbricas e inalámbricas. La topología algunas veces son empleadas del tipo estrella con un nodo central ubicada en un Cuartel General. Al encontrarse la misma centralizada y teniendo presencia en todo el territorio nacional, la interconexión de los nodos de red se da a través de servicios de proveedores de telecomunicaciones. Del mismo modo al no existir una red troncal de fibra administrada por el estado para servicios de banda ancha las Instituciones Armadas vienen empleando conexiones VPN, las mismas que requieren de servicios de internet dedicados o servicios de circuitos digitales para poder integrar las redes siempre dependiendo de los proveedores del servicio lo que reduce el nivel de control y seguridad en la misma.

Al respecto, un sistema de seguridad integral no puede ofrecerse ni mucho menos ser eficientes o cumplirse a cabalidad, si no existen normas claras y precisas así como una organización que lo dirija y controle. La seguridad de la información en las Instituciones Armadas requiere que se le brinde la atención requerida y la importancia necesaria para evitar posibles amenazas en el nuevo dominio del ciberespacio.

Después de haber descrito, brevemente, la normal infraestructura de seguridad que se implementa en las Instituciones Armadas, en contraposición se describirán las Capacidades de los Actores, las que a menudo se desconoce cuáles son o hasta donde afectan, ya que los Actores de esta Amenaza no necesitan tener calificaciones en centros académicos, ya que pueden ser empíricos, pero sí tener conocimientos de este submundo. Debido a esto veamos un poco a estos Actores como una Amenaza llamada "Afectación a la Seguridad Digital" de acuerdo como se describe a continuación:

- En el ámbito de las Ciberamenazas, los ciberataques muestran un frecuente activismo en el ciberespacio y sus impactos se dirigen contra los sistemas de información, la seguridad digital, las redes de comunicaciones y Ciberinfraestructuras. Son una amenaza latente y la coyuntura global da cuenta de su

6 Un Sistema de Prevención de Intrusos es un dispositivo de seguridad, fundamentalmente para redes, que se encarga de monitorear actividades a nivel de capa 3 (red) y/o a nivel de capa 7 (aplicación) del Modelo OSI. https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

7 Permite que se conecten a Internet las redes de IP privada que emplean direcciones IP no registradas. https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

8 Tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red controlada como Internet. https://www.usmp.edu.pe/publicaciones/boletin/fia/info41/redprivada.html

9 Una zona desmilitarizada (DMZ, por las siglas en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. https://www.pandasecurity.com/enterprise/downloads/docs/product/gatedefender-performa/help/v4.00.00/es/html/1508.htm

CUADRO N° 1

ACTOR	CAPACIDAD
Empresas transnacionales	Ejercer presión económica
Grupos de poder adversarios al Estado y Fuerzas del Orden (FFO)	Apoyar actividades de grupos cibercriminales
Agencias de inteligencia extranjeras	Obtienen información usando diversos medios ilegales
Activistas / Ciberactivistas	Promover consignas y lineamientos de manera masiva
	Articulan y difunden lineamientos y consignas
Hacktivistas	Ejecutan Ciberoperaciones
Cibercriminales	Atentar contra el ciberespacio
Países/Estados	Realizar acciones de ciberguerra, cibersabotaje y ciberespionaje
Organizaciones Internacionales	Controlan el ciberespacio

Cuadro modificado por el autor para fines didácticos.

alta probabilidad de ocurrencia y los efectos que pueden ocasionar en el Estado, el sector privado y la ciudadanía en general. Al respecto, dos incidentes registrados a escala mundial (12 de mayo y 28 de junio del 2017), revelan el efecto masivo que refieren los ciberataques que por ejemplo, en el primero caso, afectó a 150 países incluyendo al Perú.

- El Perú es el segundo país más afectado con los ataques de suplantación de identidad de páginas web (phishing),[10] según el reporte de seguridad informática de la empresa ESET. La proyección es que esta modalidad se incremente en el presente año. Asimismo, se proyecta que aumenten los casos de secuestro de información (ransomware),[11] que fue la modalidad empleada en los ciberataques globales.
- Existen varios actores pero los más importantes se muestran en el Cuadro Nº 1.
- Algunas de sus formas de acción serían las siguientes:
  - Suplantación de identidad (phishing)
  - Secuestro de información (ransomware)
  - Virus que se esconden en documentos (malware)[12]

10 Es un método que los ciberdelincuentes utilizan para engañar y conseguir información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. https://www.avast.com/es-es/c-phishing

11 Es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados. https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/

12 Es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas. https://es.malwarebytes.com/malware/

- Daño informático (cracking)[13]
- Robo financiero
- Hacktivismo.[14]
- Denegación de servicios
- Utilización de Botnet[15]

3 ANÁLISIS DESCRIPTIVO:

A continuación pasaremos a ilustrar lo anterior, con el desarrollo de un evento hipotético. Supongamos que tenemos una dependencia de una Institución de las Fuerzas Armadas, que se encuentra ubicada en una ciudad capital.

Esta dependencia está protegida por los anillos de seguridad que le proporciona su Órgano de Telemática y el Cibercomando de esa Institución castrense. Acorde con lo descrito anteriormente, la infraestructura de la red es casi impenetrable, pero no existe una seguridad al 100%; siempre existe un eslabón débil en la cadena de seguridad. Debido a esto toda la información clasificada es transmitida a través de su planta externa o cableado de red (red interna), que en algunos casos por diseño del cableado estructurado no pueden interconectar físicamente a todos los dispositivos que requieren acceder a dicha red. Por tal motivo el Jefe de esa oficina o dependencia solicita al personal de informática que coloque un router para conectarse de forma inalámbrica (wifi) a su estación de trabajo (vulnerabilidad alta), sumándose a esto la falta de seguridad y conocimiento de la amenaza existente, colocando esta señal inalámbrica sin contraseña (acceso libre).

Debido a que los actores de esta amenaza están en permanente acecho, un agente de una Agencia de Inteligencia extranjera con grandes conocimientos en herramienta del ciberespacio, comienza un escaneo de redes inalámbricas de esa dependencia, llegando a detectar y aprovechar la vulnerabilidad de la red por esa señal que cuenta con acceso libre. Procede a ejecutar diversos códigos maliciosos que no son detectados por los anillos de seguridad de la Institución Armada, ni por el Cibercomando, ya que se ingresó a través de un usuario reconocido por el sistema pudiendo robar, destruir y neutralizar elementos críticos del Poder Militar desde el interior de la infraestructura digital (insite).

Analizando este ejemplo que podría ser muy común en las Instituciones Armadas procederemos a describir una experiencia. Para los efectos del presente tema no se mencionará nombres, institución, ni correo electrónico, con la finalidad de guardar la confidencialidad del caso.

El 26 ABR 11, se dio inicio a una investigación referente a un correo electrónico de nick “xxxxxx@gmail.com”, el mismo que fue recibido por diversos oficiales de las diferentes Instituciones Armadas y Policía Nacional, de los cuales solo un oficial dio a conocer lo ocurrido, quedando evidenciada la falta de conciencia de seguridad y del impacto de daño ocurrido a las infraestructuras informáticas de las Instituciones Armadas y Policía Nacional.

El indicado correo, era remitido por un seudónimo “5X”; el cual se anunciaba como supuesto ex agente de Purpura y que requería ayuda de parte de la Fuerzas Armadas Naranja y en compensación sería un colaborador efectivo de Naranja.

El 26 ABR 11, se comenzó a entablar la conversación con “5X”, mediante un correo facilitado por el referido oficial (xxxxxx@hotmail.com), quien fue uno de los que recibió la solicitud antes indicada.

El 29 ABR 11, 5X envió un correo electrónico con 44 archivos adjunto, entre los cuales se destaca el “Plan Anual de Inteligencia (PAI) 2008”, una conversación de un supuesto espía (presumible de una Institución Armada, por los temas tratados) a Purpura, observando entre otros; cabe resaltar que los archivos contenían códigos maliciosos (virus o troyanos) que permitían la manipulación remota de la

13 Consiste en burlar los sistemas de seguridad para obtener acceso a los equipos informáticos. https://www.avast.com/es-es/c-cracking

14 Acrónimo de hacker y activismo, también denominado ciberactivismo. https://core.ac.uk/download/pdf/44311132.pdf

15 Botnet es el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota. https://www.kaspersky.es/blog/que-es-un-botnet/755/

computadora infectada (control total de la maquina victima).

En el intercambio de los mail se le indicó a "5X" que cambiemos de correo electrónico, debido a que otra dirección electrónica sería más segura. Se creó una dirección electrónica falsa de Nick "xxxxxx@gmail.com" para el intercambio de información y poder obtener la real intención del atacante.

El 30 ABR 11, se inició la conversación induciéndolo a que explique las verdaderas intenciones, dándonos respuestas esquivas.

El 03 MAY 11, nos invita a ingresar a un link que se descargaban varios códigos maliciosos, del cual permitía al sujeto tener el control total de nuestra máquina y penetrar a las redes existentes.

El 05 MAY 11, enviamos un código malicioso, para obtener información referente al adversario con quien conversábamos.

El 10 MAY 11, "5X" nos comunica que ha cambiado de dirección electrónica y de seudónimo (6X "xxxxx@gmail.com"); enviando 11 archivos adjuntos (algunos con códigos maliciosos), en los que resalta una Orden de Operaciones.

El 16 MAY 11, se enlazó vía chat, llegándose a realizar una conversación por un lapso de dos (02) horas; y fue gracias a esa conversación que se pudo obtener la verdadera identidad de "5X", debido a que en registros pasados se tenía una identificación del Actor con el nombre de 10X, el indicado sujeto sería un perito en las artes del hacking de sombrero negro o black hat,[16] quien prestaba servicio en la dirección de Inteligencia de la Fuerza Aérea de Plateado.

La intención del indicado sujeto fue ofrecer información, con la finalidad de poder ingresar a las redes de los sistemas de información de las Instituciones Armadas y Policía Nacional de Naranja, y así poder obtener información sensible y tener control de las indicadas infraestructuras tecnológicas.

4 CONCLUSIONES

a) Toda infraestructura es vulnerable a ataques informáticos.
b) El personal en general y en especial el de las FF.AA requieren reforzar su conciencia situacional sobre las medidas de ciberseguridad y de seguridad digital.
c) Agentes de otros Estados o de actores particulares, pueden contar con capacidades en manejo de ciberguerra y ciberespionaje, ante los cuales debemos desarrollar continuamente nuestras propias capacidades.
d) Los procedimientos vigentes para canalizar un tipo de ataque al personal de las FF.AA requieren siempre de actualización y mejora permanente
e) Existe la tendencia a priorizar la infraestructura digital en detrimento del desarrollo de las capacidades humanas del personal.

5 LECCIONES APRENDIDAS

a) Contar con un protocolo adecuado para realizar este tipo de operaciones.
b) Implementar y desarrollar cursos y conferencias sobre la cultura de seguridad digital.
c) Contar con protocolo para proporcionar información, dar parte, de algún ataque a través del ciberespacio.
d) Necesidad de diseñar mecanismos para proteger el activo más vulnerable de las infraestructuras informáticas, que son los usuarios.
e) Profundizar el análisis de cada capacidad de los actores de la amenaza (conocer al actor, como piensa, como trabaja y cuál es su objetivo).

16 Es un hacker que viola la seguridad informática por razones más allá de la malicia o para beneficio personal. (https://www.avira.com/es/blog/hackers-y-sombreros-neglo-blanco-gris)