

CIPLA
CORAZÓN DE
SUDAMÉRICA

9^{no} CONGRESO INTERNACIONAL

DE PREVENCIÓN DE LAVADO DE ACTIVOS
LA PAZ, BOLIVIA 7 Y 8 DE OCTUBRE DE 2021

Tema: CIBERSEGURIDAD Y LA PREVENCIÓN
DE LAVADO DE DINERO

Expositor:
CPC SILVIA ROSA MATUS DE LA CRUZ

Contador Público por la Escuela Bancaria y Comercial en México .

- Socia en PLD y auditoría de Zepeda Consultores Asociados SC.

Certificado en 3 materias , Examen Único de Certificación, en fiscal y en Prevención de Lavado de Dinero por el Instituto Mexicano de Contadores Públicos AC.

Diplomada en Ciberseguridad y Protección de Datos Personales por la Universidad de las Americas en Puebla México . Egresada de Blockchain Academy México. Egresada del Bootcamp de Ciberseguridad en línea.

Perito en Compliance por la World Compliance México.

Estudiante de la licenciatura de Derecho en la Universidad Tecnológica Latinoamericana.

Catedrática en la Facultad de Contaduría y Administración de la UNAM, con las materias de Fintech y Prevención de Lavado de Dinero y en el INACIPE.

Ha impartido capacitación en México en diversos colegios del Instituto Mexicano de Contadores Públicos, así como en , USA, España, Centro y Sudamérica (Colombia, Guatemala, El Salvador , Nicaragua, Bolivia, Panama).

Ex vicepresidenta del Colegio de Contadores Públicos de México.

Ex vicepresidenta de la revista Contaduría Pública del IMCP.

Vicepresidenta electa de Práctica Externa del IMCP por el período 2021-2023



**SILVIA MATUS DE
LA CRUZ**
Email:
smatus@pldmex.com



¿QUÉ ES LA CIBERSEGURIDAD?

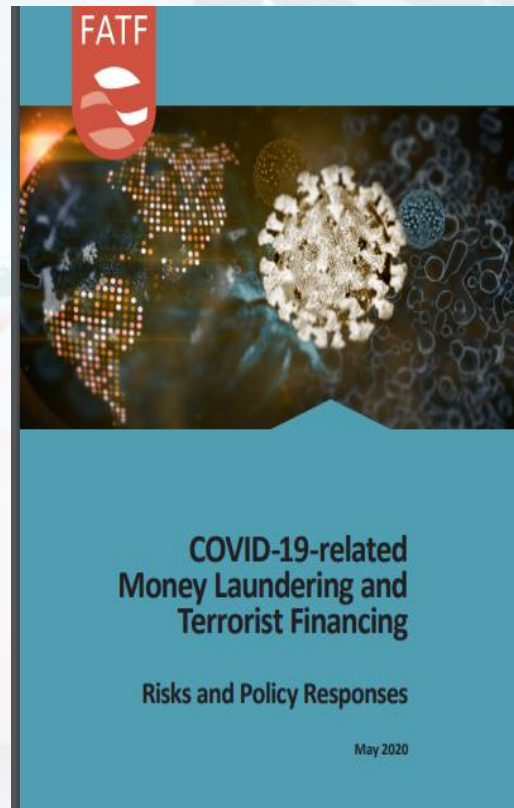
- Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.
- También se conoce como seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil y puede dividirse en algunas categorías comunes.



EL CRIMEN ESTA CAMBIANDO DEL MUNDO FÍSICO, AL MUNDO DEL CIBERESPACIO



GAFI: LAVADO DE DINERO Y FT DERIVADO DEL COVID 19



IFAC

INTERNATIONAL FEDERATION OF ACCOUNTANTS
STANDARD-SETTING BOARDS
NEWS
CONTACT
SELECCIONAR IDIOMA
LOGIN / REGISTER

WHO WE ARE | WHAT WE DO | KNOWLEDGE GATEWAY

Site Search

PREPARING FUTURE-READY PROFESSIONALS

Cybersecurity Is Critical for all Organizations – Large and Small

Steve Ursillo, Jr., Christopher Arnold | November 4, 2019 |

Introduction

In today's computerized world, new risks emerge every hour of every day. Connecting to the Internet opens up the

Issues and Insights

- Supporting International Standards
- Contributing to the Global Economy
- Building Trust & Ethics
- Developing the Accountancy Profession
- Preparing Future-Ready Professionals

Recent Articles

- Webinar Series: Practical Audit Quality

carretera de noche.jpg

Mostrar todo X

¿QUÉ ES EL CIBERCRIMEN?

- *El cibercrimen es toda aquella actividad que transgrede; en la que una computadora (o dispositivo de red) es atacada y / o utilizada directa o indirectamente.*
- **CIBERDELINCUENTES**
 - Gran parte de las fechorías cibernéticas son cometidas por ciberdelincuentes o piratas informáticos que ganan dinero con ellas. El cibercrimen es llevado a cabo por individuos u organizaciones.
 - Algunos ciberdelincuentes se reúnen en grupos organizados, utilizan métodos avanzados y tienen altas calificaciones técnicas, otros son hackers novatos.
 - Los cibercriminales rara vez piratean las computadoras por razones ajenas a las ganancias, por ejemplo, políticas o personales.

TIPOS DE CIBERCRÍMENES

- Algunos ejemplos de diferentes **tipos de cibercrímenes**:
- Fraude por correo electrónico y en Internet.
- Fraude de datos personales (robo y uso indebido de información personal).
- Robo de datos financieros o de tarjetas bancarias.
- Robo y venta de datos corporativos.
- Chantaje cibernético (exigiendo dinero para evitar los ciberataques).
- Ataques de programas de extorsión (tipo de chantaje cibernético).
- Criptología, o criptojacking (extracción de criptolitos utilizando los recursos de otras personas sin el conocimiento de sus dueños).
- Ciberespionaje (acceso no autorizado a datos de organizaciones estatales o comerciales).



- Se refiere al software malicioso. Ya que es una de las ciberamenazas más comunes, el malware es software que un cibercriminal o hacker ha creado para interrumpir o dañar el equipo de un usuario legítimo. Con frecuencia propagando a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima, el malware puede ser utilizado por los ciberdelincuentes para ganar dinero o para realizar ciberataques con fines políticos. Hay diferentes tipos entre los que se incluyen los siguientes:



RANSOMWARE

El ransomware es un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.

Este tipo de malware es un sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web.

El ransomware tiene la **capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña.**



PHISHING

Phishing es un término informático que denomina a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo revelar información confidencial o hacer click en un enlace).



CYBER EXPERTOS MARIBEL POYATO

El cibercrimen ya mueve más dinero que el narcotráfico



Vicente Ramírez
4 octubre, 2019

21 Compartido ⚡ 4,056 Visualizaciones 1

f Compartir artículo

🐦 Compartido en twitter



RECIBE NUESTRA NEWSLETTER

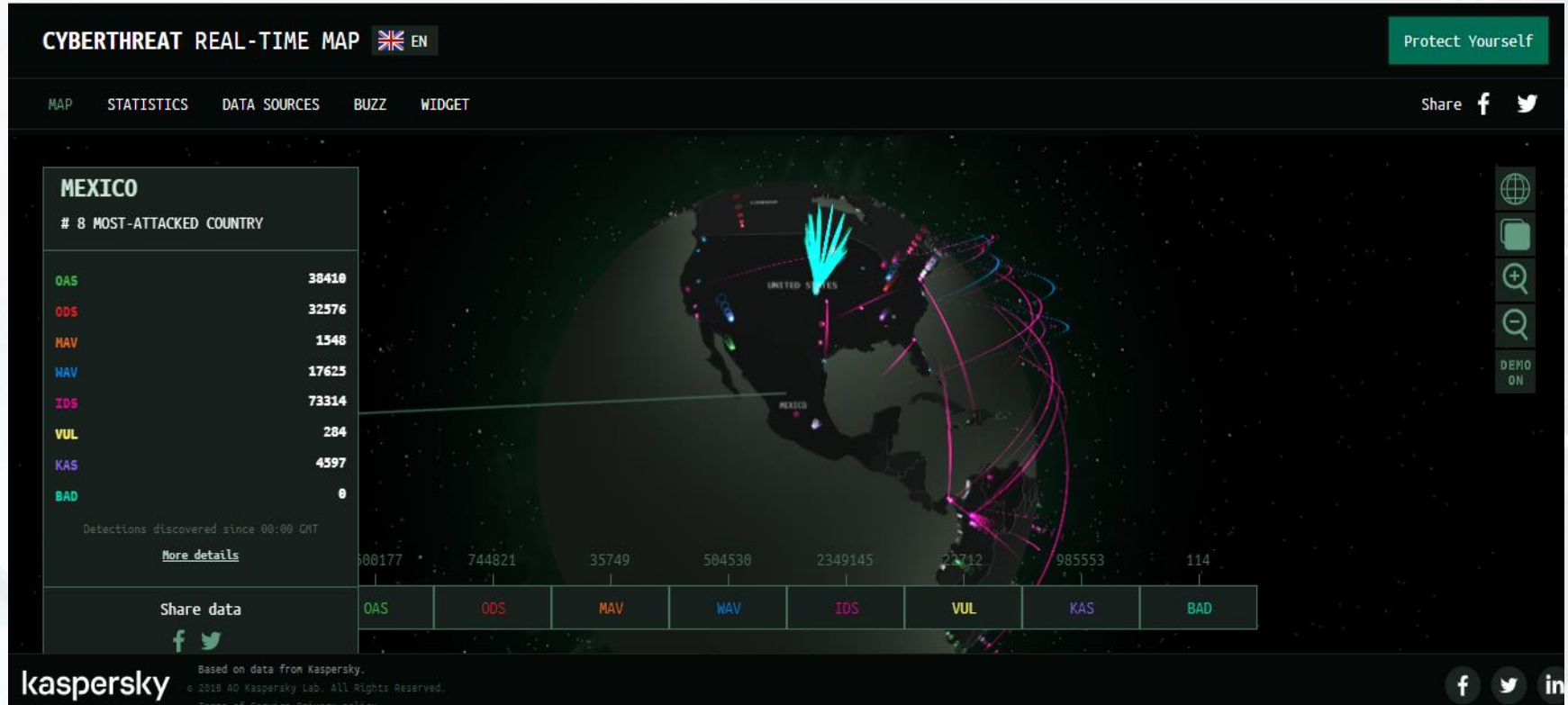
*Email:

*Nombre apellidos:

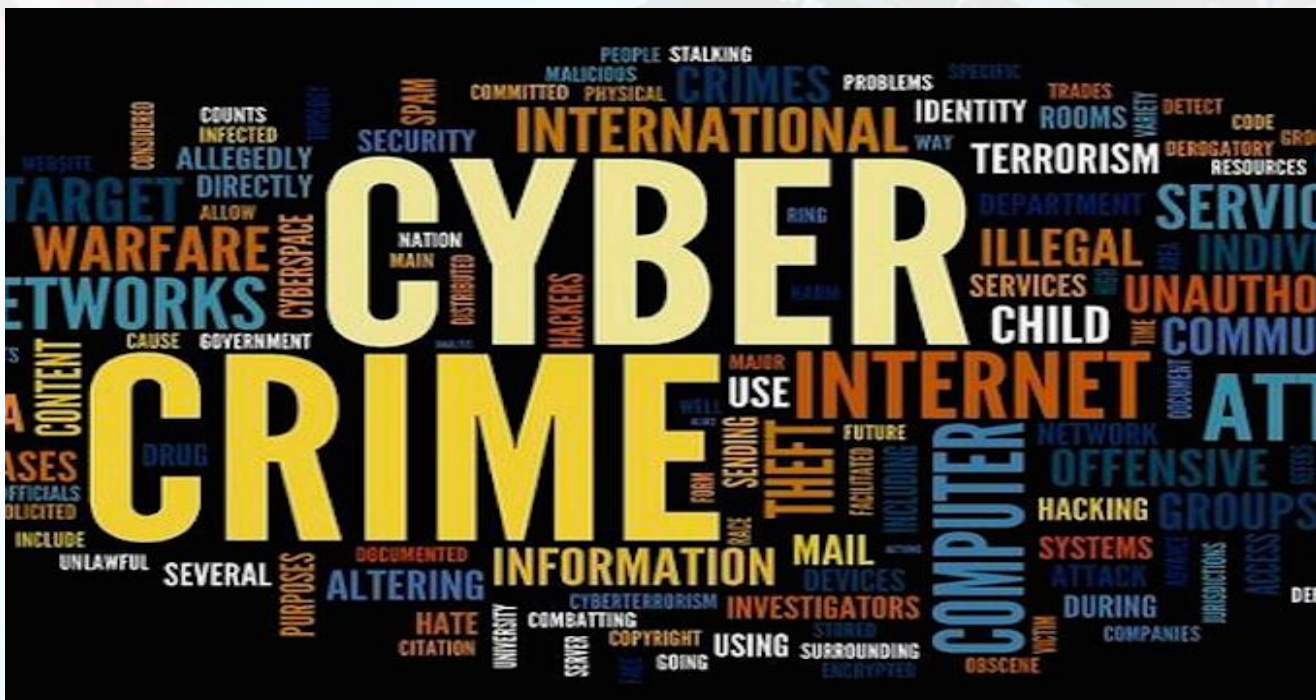
*Empresa:

Por Maribel Poyato, Country Manager de Tixeo España.

Los avances tecnológicos y las nuevas formas de comunicación han abocado al planeta al mundo digital. Un cambio que, en su cara menos agradable, cuenta con efectos indeseados. Y es que se han abierto las puertas a unos ciberdelincuentes cada vez más sofisticados. El nacimiento y la rápida difusión de las redes informáticas, están propiciando que la cibercriminalidad sea uno



“EL CIBERCRIMEN NO ES REPORTADO”



“Cybercrime is the greatest threat to every
company in the world.”

Ginni Rommety
Actual presidenta y CEO de la compañía IBM.

UDLAP.

JENKINS GRADUATE SCHOOL

“El Cibercrimen es la más grande amenaza a las compañías en el
mundo.”

CIPLA
CORAZÓN DE
SUDAMÉRICA

9^{no} CONGRESO INTERNACIONAL

DE PREVENCIÓN DE LAVADO DE ACTIVOS
LA PAZ, BOLIVIA 7 Y 8 DE OCTUBRE DE 2021

www.cipla.grupoamlc.org



Apoyan: **CIPLA** **AML**C
Anti Money Laundering Consultants

Organizan:



EL ECONOMISTA



REPORTES 2T

● CORONAVIRUS

SUSCRÍBETE

El Economista > Sector Financiero

Publicidad

CIBERSEGURIDAD

Ciberdelincuentes nigerianos modernizan sus estructuras

El Buisness Email Compromise es una modalidad de fraude cibernético donde se comprometen los correos electrónicos de personas o empresas, con el fin de enviar órdenes de pago a instituciones financieras o proveedores.



Fernando Gutiérrez

27 de julio de 2020, 16:30



CIPLA
CORAZÓN DE
SUDAMÉRICA

9^{no} CONGRESO INTERNACIONAL

DE PREVENCIÓN DE LAVADO DE ACTIVOS
LA PAZ, BOLIVIA 7 Y 8 DE OCTUBRE DE 2021

www.cipla.grupoamlc.org



Apoyan: **CIPLA** **AML**C
Anti Money Laundering Consultants

Organizan:





THE ANATOMY OF BUSINESS EMAIL COMPROMISE 3 TOXIC INGREDIENTS

Low cost!
Low risk!
High rate
of return!

Hacking

An email account is compromised through malware, employee intrusion, etc.

1

+

2

+

3

=

Millions in
illegal profits

Social engineering fraud

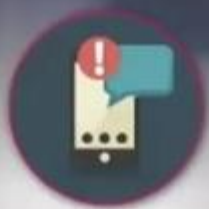
The victim is manipulated into providing information or funds.

Money laundering

Multiple transfers are made involving foreign banks/institutions

#BECareful

COVID-19 SCAMS INCLUDE:



TELEPHONE FRAUD

Calls from
'hospital
officials'

Requests
for payment
to help
relatives



PHISHING

Emails from
national or
global health
authorities

Attachments
or links which
contain
malware

Payment
requests

Requests
for personal
information

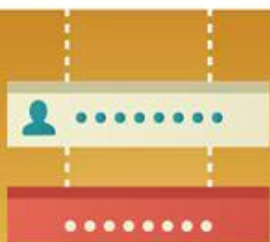


INTERPOL

BE VIGILANT . BE SKEPTICAL . BE SAFE

#WashYourCyberHands

WHAT IS **BUSINESS EMAIL COMPROMISE?**



ILLEGAL ACCESS

Criminals gain entry to a victim's devices or systems – through hacking, phishing websites, malware – then deceive the victim into transferring money into their bank account.



SOCIAL ENGINEERING

Criminals can target their victims based on information they share on social media platforms.



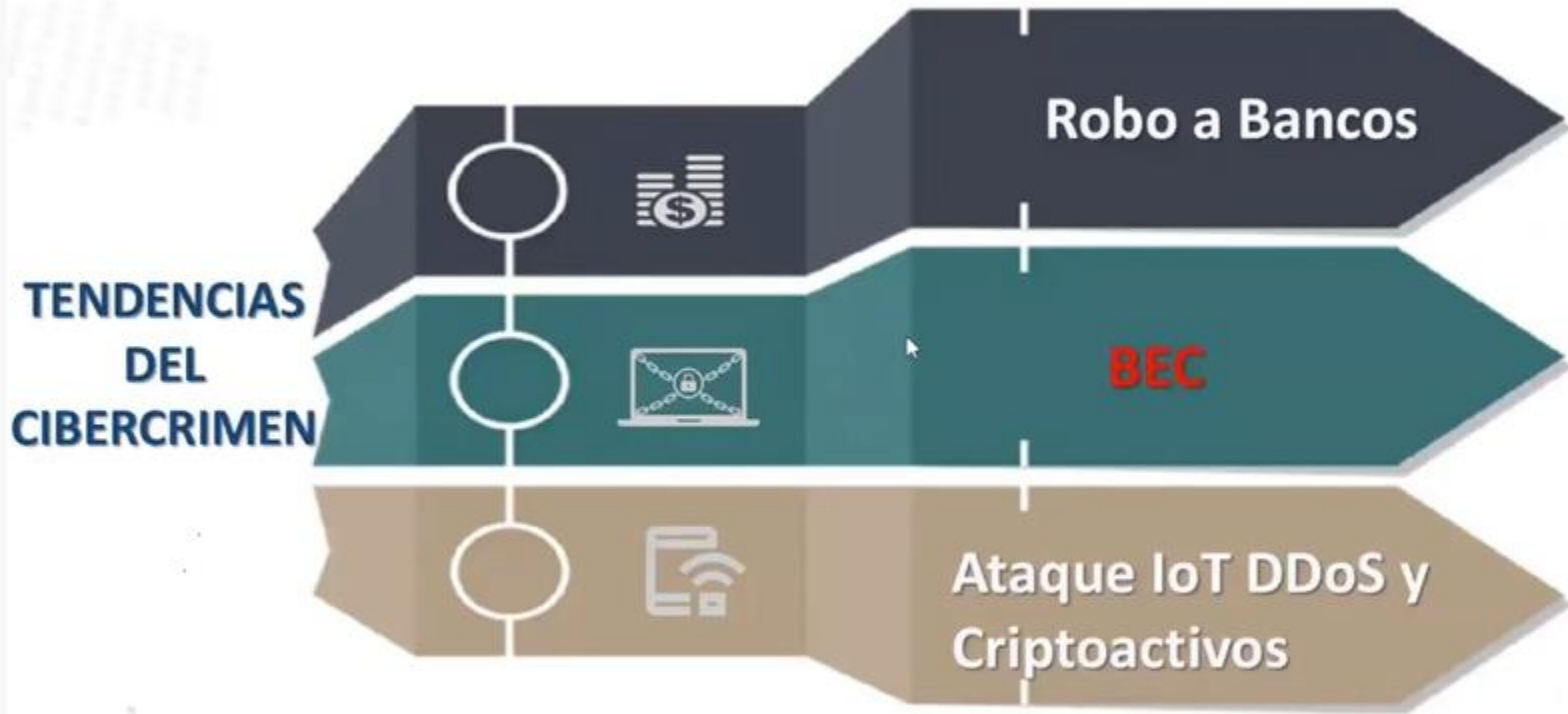
URGENT REQUEST

The criminal impersonates a supplier requesting an urgent payment or change to banking details, or a senior employee in the company with authority to authorize payments.

#BECareful



INTERPOL



Smart Car



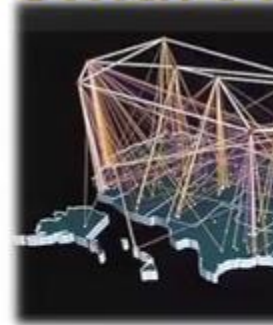
Smart Home



Smart City



Smart M



Futuro brillante

La tecnología va
más rápido

¿Qué se puede
Hacer?





Necesitamos Saber

CÓMO EVITAR SER VÍCTIMA DEL DELITO CIBERNÉTICO

Aquí algunos consejos:

- **Actualizar regularmente el software y el sistema operativo.**

Las continuas actualizaciones de software y del sistema operativo garantizan que se utilicen los últimos parches de seguridad para proteger el ordenador.

- **Instalar un software antivirus y actualizarlo regularmente.**

El uso de un antivirus o de una solución de seguridad integral para Internet es la forma correcta de proteger el sistema de los ataques. Si se utiliza un software antivirus, es necesario actualizarlo regularmente para garantizar el mejor nivel de protección.

- **Use contraseñas seguras**

Usar contraseñas seguras que sean difíciles de aprender y no las escriba en ningún lado. Se puede hacer uso del servicio de un administrador de contraseñas confiable, que facilite la tarea de sugerir una contraseña segura generada por este.

- **No abrir archivos adjuntos en mensajes electrónicos de spam**

La forma clásica de infectar computadoras con ataques maliciosos y otros tipos de delitos informáticos es adjuntarlos a mensajes electrónicos de spam. Por ello es mejor nunca abrir un archivo adjunto de un remitente que no se conozca.

Conocer los riesgos en la Red

Nos permite estar preparados

De esta forma disminuir el número de víctimas

Prevención

Indicadores de compromiso

Modus Operandi

Buenas practicas

Medidas de detección y protección

Necesitamos **Compartir**

← → × 🏠 incibe.es/que-es-incibe

Aplicaciones Google ScotiaWeb IDC IDC

Otros marcadores

SUSCRIPCIÓN
BOLETINES

English Contacto Ayuda en ciberseguridad Agenda Sala de prensa Encuestas Mapa web

PORTALES
INCIBE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Protege tu empresa ▾ Eventos ▾ Otras actividades ▾ Qué es INCIBE ▾ 🔍

Inicio / Qué es INCIBE

Qué es INCIBE



Conoce INCIBE

INSTITUTO NACIONAL DE CIBERSEGURIDAD

PREGUNTAS

MUCHAS GRACIAS!!!

smatus@pldmex.com



www.grupoamlc.org