TLC ASOCIADOS

TRADE LAW & CUSTOMS magazine

HAGAMOS UN TRUEQUE

TLC MAGAZINE MÉXICO

27 DE MAYO

27

Ciberseguridad

Dr. David Merino Téllez

Presidente de la Academia Mexicana de Derecho Digital y Tecnológico, A. C.

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

Ciberseguridad y las finanzas criminales como eje de investigación

Una perspectiva desde la banca, la tecnología y la investigación digital

Dr. David Merino

Coordinador General, Grupo de Inteligencia Artificial, GIAO
LXIV, F Cámara de Diputados de México

Definición de Ciberseguridad:

La **ciberseguridad** es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera, almacena, transmite y procesa a través de medios digitales y sistemas electrónicos.

es el conjunto de acciones tomadas por organizaciones e individuos para mitigar los riesgos que enfrentan en el ciberespacio, con el propósito de disminuir la probabilidad de sufrir un ciberataque.

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

Algunas definiciones

Ciberseguridad, es el conjunto de acciones tomadas por organizaciones e individuos para mitigar los riesgos que enfrentan en el ciberespacio, con el propósito de disminuir la probabilidad de sufrir un ciberataque.

Ciberataque, es un intento no autorizado por la vía digital de acceder a un sistema de control, dispositivo electrónico y/o red informática, con el propósito de sabotear su funcionamiento, extraer información y recursos, o extorsionar a usuarios y organizaciones. Estos ataques se dividen en dos, dirigidos y no dirigidos.

Ciberresiliencia, incluye la capacidad de grupos e individuos para mantenerse seguros de forma sostenida en el largo plazo. La ciberresiliencia integra la destreza de todos para tomar decisiones con información imparcial y veraz.

Algunas definiciones

El **Ciberespacio** es un concepto que se refiere al entorno digital creado por redes informáticas, dispositivos y sistemas en línea. En este espacio, la información fluye en forma de datos a través de redes interconectadas, permitiendo la comunicación, el intercambio de información y la ejecución de procesos en línea.

Se presenta como el nuevo dominio en seguridad nacional en varios países:

“Espacio Terrestre, Aéreo, Marítimo, Espacial y Ciber Espacio.”

“Agencia nacional de ciberseguridad”

Algunas definiciones

Seguridad de la Información: La seguridad de la información es un término más amplio que abarca la protección de toda la información, ya sea en formato digital o físico. Esto incluye no solo la información almacenada en sistemas informáticos, sino también en documentos impresos, conversaciones verbales y otros medios. La seguridad de la información se trata de asegurar que la información se maneje de manera adecuada, se proteja contra el acceso no autorizado y se mantenga disponible para las personas que la necesitan.

Seguridad Informática: La seguridad informática se refiere a la protección de los sistemas informáticos, incluyendo hardware, software y datos almacenados en ellos, contra amenazas físicas y cibernéticas. Esta área se centra en la implementación de medidas de seguridad técnicas y operativas para prevenir la explotación de vulnerabilidades y la protección de los activos digitales. La seguridad informática se encuentra dentro del ámbito más amplio de la seguridad de la información.

Ciberespacio

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

Seguridad de la Información Y Ciberseguridad.

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

ISO 27001

La **ISO 27001** es un Estándar Internacional de Sistemas de Gestión de Seguridad de la Información que permite a una organización evaluar su riesgo e Implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad del valor de la información.

El objetivo fundamental es proteger la información de su organización para que no caiga en manos Incorrectas o se pierda para siempre.

¿Qué es Información?

- La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada.

- La información puede estar:
  - Impresa o escrita en papel.
  - Almacenada electrónicamente.
  - Trasmitida por correo o medios electrónicos
  - Mostrada en fotos o videos.
  - Hablada/grabada en una conversación.

- Debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparte o almacena.

¿Qué es Seguridad?

- ✓ Evitar el ingreso de personal no autorizado
- ✓ Sobrevivir aunque “algo” ocurra
- ✓ Cumplir con las leyes y reglamentaciones gubernamentales y de los entes de control del Estado
- ✓ Adherirse a los acuerdos de licenciamiento de software
- ✓ Prevención, Detección y Respuesta contra acciones no autorizadas

Seguridad de la Información

- La Seguridad de la Información se caracteriza como la preservación de los siguientes principios fundamentales:
  - su **confidencialidad**, asegurando que sólo quienes estén autorizados pueden acceder a la información;
  - su **integridad**, asegurando que la información y sus métodos de proceso son exactos y completos.
  - su **disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

Amenazas Informáticas

Password cracking

Escalamiento de privilegios

Fraudes informáticos

Exploits

Man in the middle

Violación de la privacidad de los empleados

Servicios de log inexistentes o que no son chequeados

Denegación de servicio

Backups inexistentes

Destrucción de

Últimos parches no instalados

Instalaciones default

Desactualización

Port scanning

Keylogging

Hacking de Centrales Telefónicas

Puertos vulnerables abiertos

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

Mas Amenazas Informáticas

Spamming

Intercepción y modificación y violación de e-mails

Violación de contraseñas

Captura de PC desde el exterior

Virus

Incumplimiento de leyes y regulaciones

Empleados deshonestos

Ingeniería social

Mails anónimos con agresiones

Programas “bomba, troyanos”

Falsificación de información para terceros

Interrupción de los servicios

Destrucción de soportes documentales

Acceso clandestino a redes

Robo o extravío de notebooks, palms

Acceso indebido a documentos impresos

Robo de información

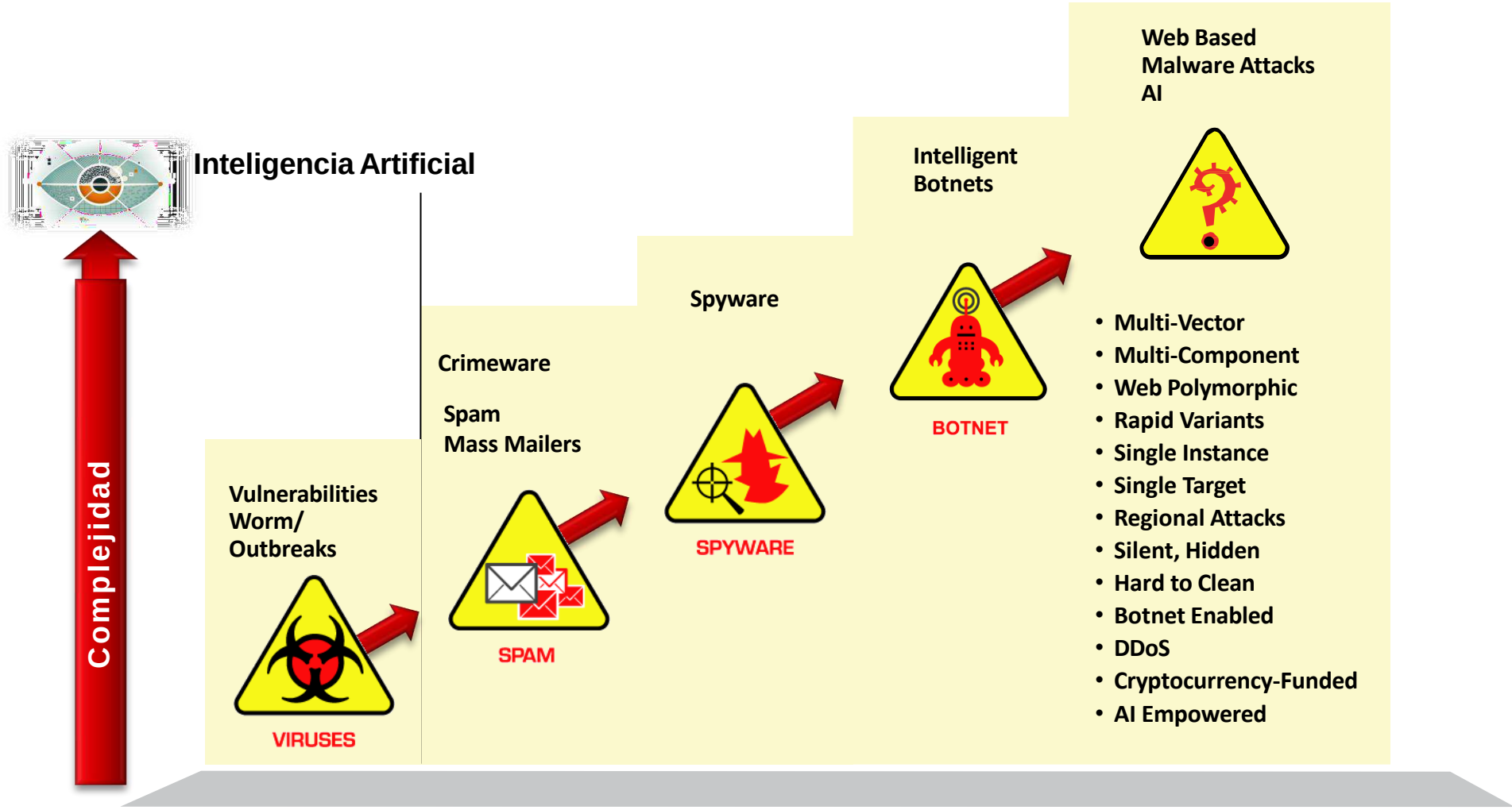
Indisponibilidad de información clave

Intercepción de comunicaciones voz y wireless

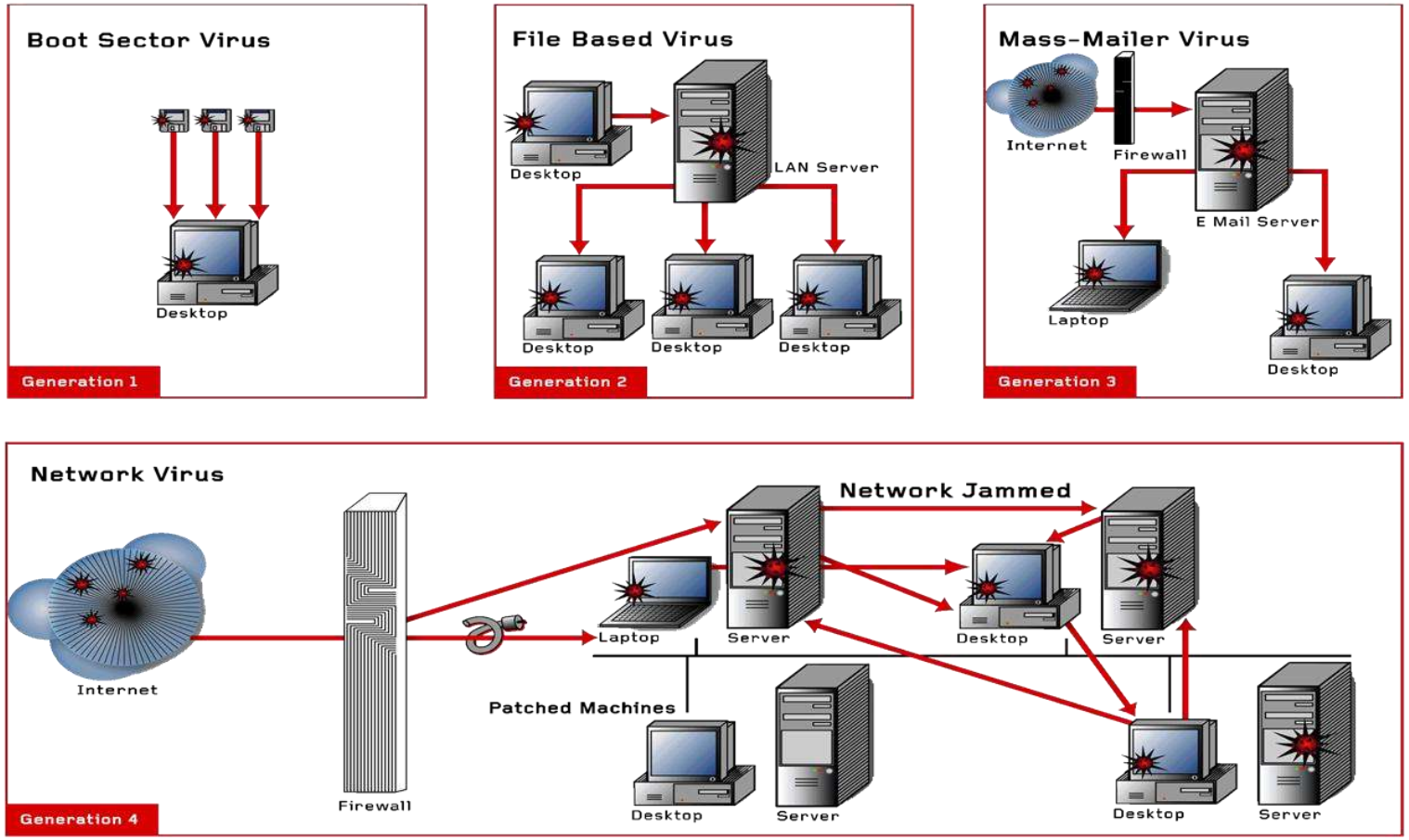
Agujeros de seguridad de redes conectadas

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

Amenazas recientes



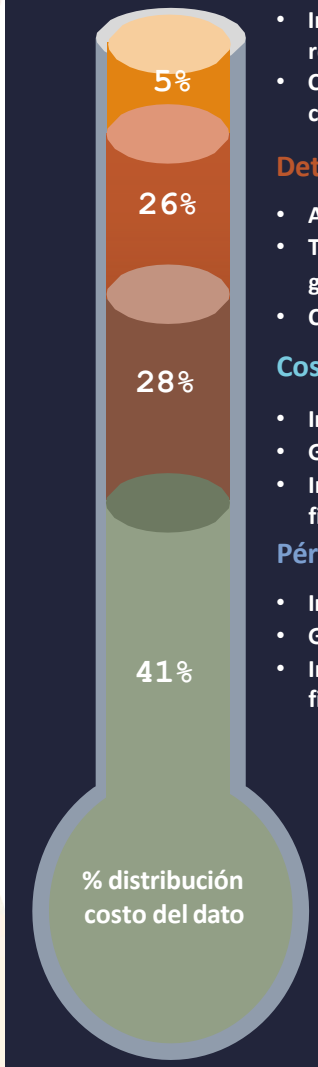
Amenazas recientes



Amenazas recientes

Costo de una filtración de seguridad

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial



Notificaciones

- Investigaciones sobre requisitos regulatorios
- Costos de comunicaciones y correspondencia

Detección y escalado

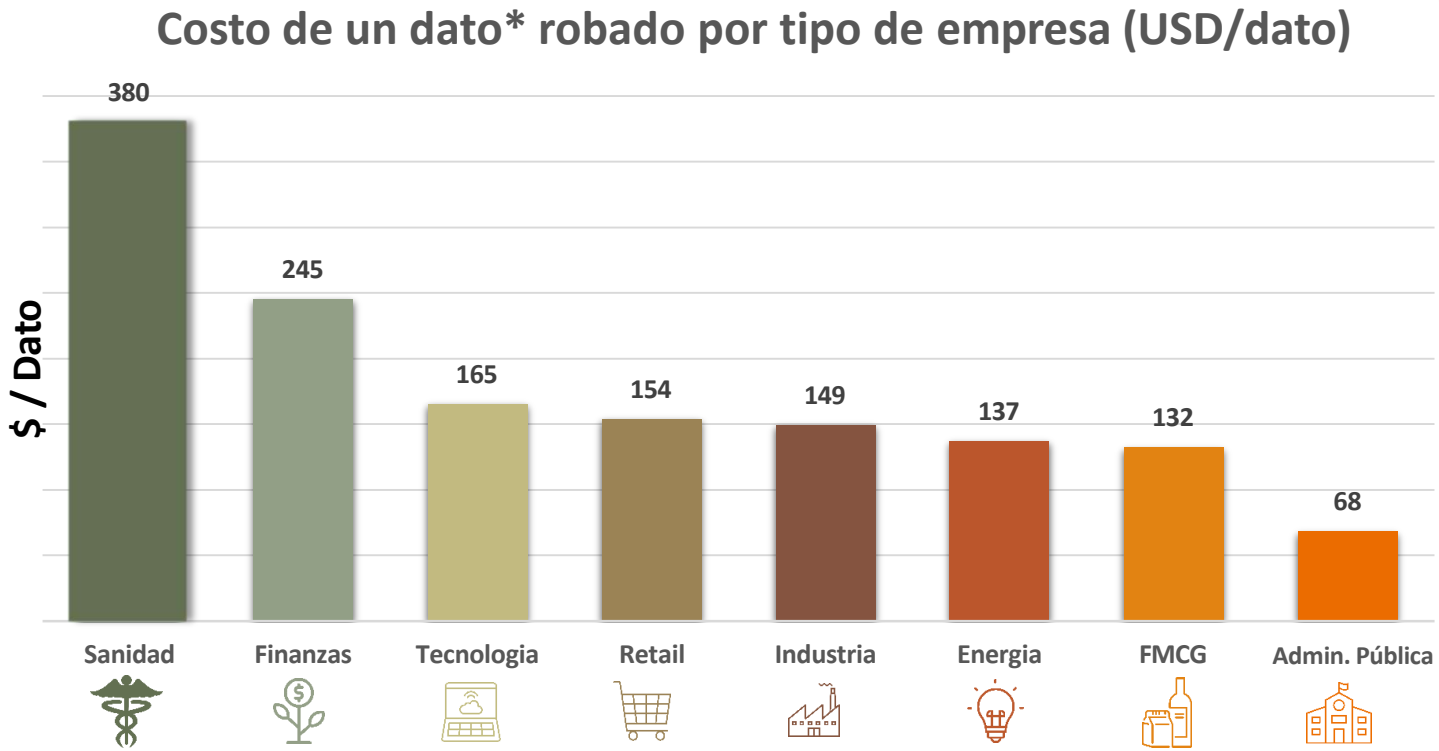
- Análisis forense y auditoría
- Tiempo del equipo directivo en gestión de crisis
- Comunicaciones internas.

Costos derivados de la filtración

- Investigación
- Gastos legales
- Incentivos a clientes para fidelizar

Pérdida de negocio

- Investigación
- Gastos legales
- Incentivos a clientes para fidelizar



* Dato que contenga un dato sensible (nombre, apellido, ficha medica, # tarjeta de crédito, etc.)

Amenazas recientes

¿Cómo afecta la inteligencia artificial a la ciberseguridad?

En el campo de la ciberseguridad, la Inteligencia Artificial puede ser utilizada como una herramienta poderosa para mejorar la protección de la información, y, por otro lado, también plantea desafíos y riesgos en términos de ataques y vulnerabilidades.

¿Qué son los delitos digitales?

- Los delitos informáticos, llamados también delitos cibernéticos, delitos electrónicos, delitos relacionados con las computadoras, delincuencia relacionada con el ordenador, computer related crimes, etc. se han definido por la Organización para la Cooperación Económica y el Desarrollo, como: "Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos".

- El concepto de abuso informático incluye una diversidad de ofensas, tanto penales como administrativas; algunas de éstas constituyen delitos que ya se castigan en diversas legislaciones; sin embargo, quedan conductas que aún no encuentran tipificadas en legislaciones penales.

Documentos Internacionales:

- Convenio Internacional sobre la Ciberdelincuencia
https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

- Protocolo Adicional a la Convención sobre el Delito Cibernético
https://www.boe.es/eli/es/ai/2003/01/28/(1)

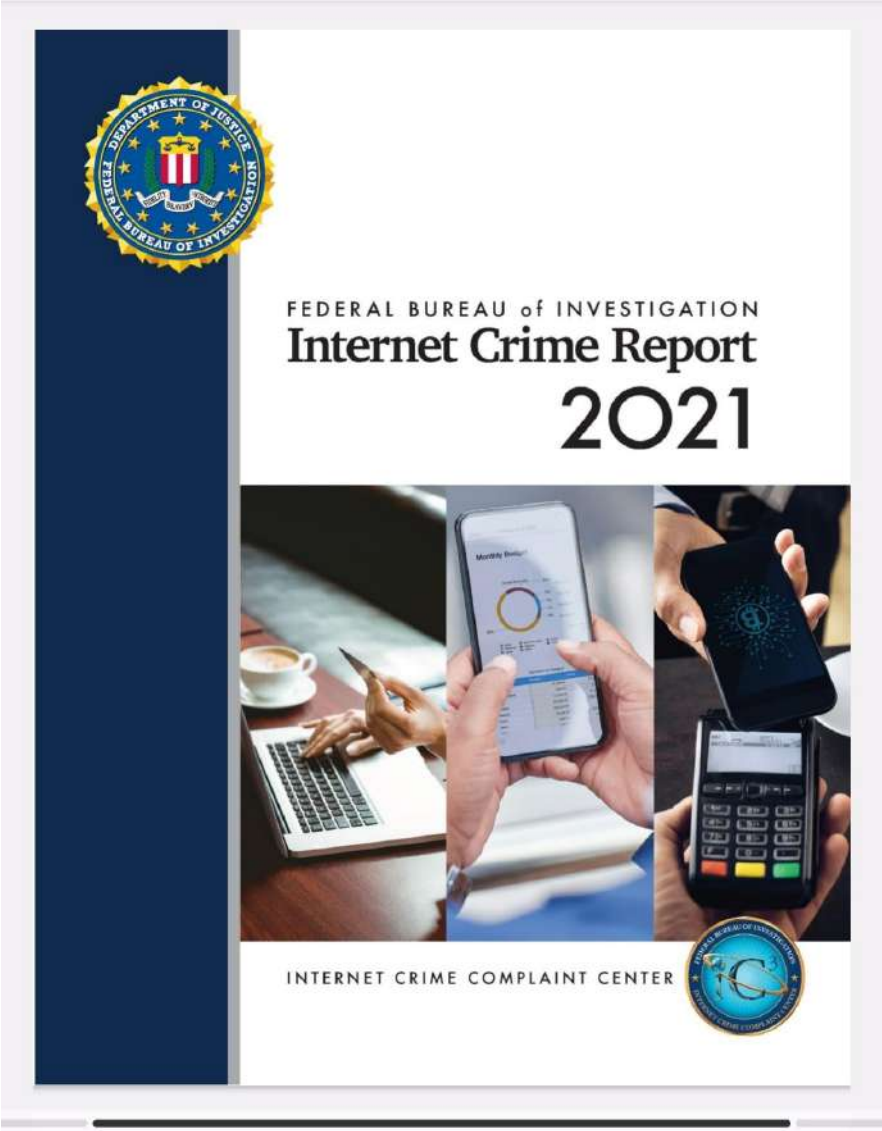
- Proposición con punto de acuerdo que exhorta al Ejecutivo Federal a iniciar a través de un proceso de múltiples partes interesadas, los trabajos necesarios para la adhesión de México al Convenio sobre la Ciberdelincuencia o Convenio de Budapest
http://sil.gobernacion.gob.mx/Archivos/Documentos/2019/03/asun_3825185_20190307_1551805094.pdf

- Guía de Identidad Digital del Grupo de Acción Financiera Internacional (GAFI) de marzo de 2020.

http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

- Indicadores de Riesgo (señales de alerta) en Activos Virtuales en materia de Lavado de Dinero y Financiamiento al Terrorismo del Grupo de Acción Financiera Internacional (GAFI) de septiembre de 2020.

https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf


FEDERAL BUREAU of INVESTIGATION
Internet Crime Report
2021
INTERNET CRIME COMPLAINT CENTER


UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito
COMPENDIO DE CIBERDELINCUENCIA ORGANIZADA

Vulnerabilidades Comunes

- Inadecuado compromiso de la dirección.
- Personal inadecuadamente capacitado y concientizado.
- Inadecuada asignación de responsabilidades.
- Ausencia de políticas/ procedimientos.
- Ausencia de controles
  - Físicos/lógicos Disuasivos/preventivos/detectivos/correctivos
- Ausencia de reportes de incidentes y vulnerabilidades.
- Inadecuado seguimiento y monitoreo de los controles.

¿De quién nos defendemos?

- **Ataques internos**: Empleados, proveedores o personas allegadas.
- Un **Hacker** que busca algo en específico.
- Un grupo de **Hackers** que busca monetizar o reconocimiento
- La **competencia**: Espionaje, Saboteo
- Desastres naturales, otros.

¿De qué nos defendemos?

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

- Fraude
- Extorsión
- Robo de Información
- Robo de servicios
- Actos terroristas
- Reto de penetrar un sistema
- Deterioro

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

¿De qué nos defendemos?

- Desastres Naturales
- Terremotos.
- Inundaciones.
- Huracanes.
- Incendios.
- Pandemias.

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

¿De qué nos defendemos?

- Tecnología
- Fallas en procedimientos
- Fallas en el software aplicativo
- Fallas en el software Operativo
- Fallas en el hardware
- Fallas en los equipos de soporte
- Paros, huelgas

Efectos de las Amenazas y los Ataques

- Interrupción de actividades
- Dificultades para toma de decisiones
- Sanciones
- Costos excesivos
- Pérdida o destrucción de activos
- Desventaja competitiva
- Insatisfacción del usuario

Protección en el Mundo Digital

El eslabón más frágil en seguridad: El usuario

- ✓ Contraseñas seguras y autenticación de dos factores.
- ✓ Uso de VPN para proteger la conexión en redes públicas.
- ✓ Actualizaciones de software y sistemas operativos.
- ✓ Educación en la identificación de correos electrónicos y sitios web falsos.
- ✓ Uso de tecnologías como Escritorios Virtuales y centralización del EndPoint

Protección en el Mundo Digital

El eslabón más frágil en seguridad: El usuario

Contraseñas Seguras:
Las contraseñas son la primera línea de defensa contra amenazas cibernéticas. Optar por contraseñas fuertes es crucial para evitar accesos no autorizados. Se recomienda:

Usar combinaciones de letras (mayúsculas y minúsculas), números y caracteres especiales.*

- Evitar información personal como nombres o fechas de nacimiento.
- No reutilizar contraseñas en múltiples cuentas.
- Utilizar frases secretas en lugar de palabras comunes.

Protección en el Mundo Digital

El eslabón más frágil en seguridad: El usuario

Autenticación de Dos Factores (2FA):

La autenticación de dos factores añade una capa adicional de seguridad. Además de la contraseña, se requiere una segunda forma de autenticación, como un código enviado un APP o por SMS al teléfono móvil. Esto dificulta enormemente el acceso no autorizado, incluso si la contraseña se ve comprometida.

- "Algo que se y Algo que tengo"

Protección en el Mundo Digital

El eslabón más frágil en seguridad: El usuario

Uso de VPN para proteger la conexión en redes públicas:

Virtual Private Network (VPN): Las redes públicas, como las de cafeterías y aeropuertos, son vulnerables a ataques. Una VPN cifra la conexión entre tu dispositivo y el servidor VPN, protegiendo tus datos de posibles interceptaciones.
Beneficios:

- ✓ Privacidad mejorada al ocultar tu dirección IP real.
- ✓ Encriptación de tráfico para evitar escuchas no deseadas.
- ✓ Acceso seguro a redes corporativas desde ubicaciones remotas.

Protección en el Mundo Digital

El eslabón más frágil en seguridad: El usuario

Actualizaciones de Software y Sistemas Operativos:

Importancia de las Actualizaciones: Las actualizaciones de software y sistemas operativos no solo brindan nuevas características, sino que también corrigen vulnerabilidades de seguridad conocidas. Ignorar estas actualizaciones deja los sistemas expuestos a ataques. Razones para mantenerse actualizado:

- ✓ Parcheo de brechas de seguridad conocidas.
- ✓ Mejora de la estabilidad y rendimiento.
- ✓ Adaptación a nuevos desafíos de seguridad.

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

Protección en el Mundo Digital

El eslabón más frágil en seguridad: El usuario

Educación en la Identificación de Correos Electrónicos y Sitios Web Falsos:

“Ingeniería Social” → ***La ingeniería social es el engaño psicológico para obtener información o acceso no autorizado.***

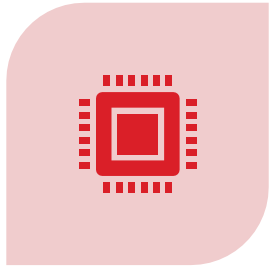
Phishing y Sitios Web Falsos: Los ciberdelincuentes a menudo utilizan correos electrónicos falsos y sitios web fraudulentos para engañar a las personas y robar información confidencial. Consejos para identificarlos:

- ✓ Verificar la dirección de correo del remitente y la URL del sitio web.
- ✓ Desconfiar de solicitudes urgentes de información personal o financiera.
- ✓ Evitar hacer clic en enlaces de correos no solicitados.
- ✓ Utilizar extensiones de navegadores que verifiquen la autenticidad de los sitios web.

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

Ciberseguridad Organizacional: Pasos Clave

EVALUACIÓN DE VULNERABILIDADES Y RIESGOS.



IMPLEMENTACIÓN DE FIREWALLS, SOLUCIONES ANTIVIRUS Y CLOUD.

CONTROL DE ACCESO Y POLÍTICAS DE AUTENTICACIÓN EN LA EMPRESA.

RESPALDO DE DATOS Y RECUPERACIÓN ANTE DESASTRES.

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

Desarrollo y Mantenimiento de Políticas de Ciberseguridad

Creación de manuales de ciberseguridad y políticas internas.

Capacitación constante de empleados en buenas prácticas y actualización de ataques.

Monitoreo y revisión regular de las políticas para adaptarse a nuevas amenazas.

MATRIZ DE RIESGOS DIGITALES Y TECNOLÓGICOS - Guardado

fx Escribe aquí el texto o la fórmula

RIESGO	Probabilidad (Ocurrencia)	Gravedad (Impacto)	Valor del Riesgo	Nivel de Riesgo
PHISING	3	5	15	Muy grave
PASSWORD CRACKING	4	5	20	Muy grave
FRAUDE INFORMATICO	3	5	15	Muy grave
SERVICIO DE LOG INEXISTENTE	3	4	12	Importante
BACKUP INEXISTENTE	3	4	12	Importante
DESACTUALIZACION	4	4	16	Muy grave
INSTALACIONES DEFICIENTES	4	5	20	Muy grave
FALTA DE POLITICAS ADMINISTRATIVAS	4	5	20	Muy grave
HACKING	4	5	20	Muy grave
PUERTOS ABIERTOS	2	3	6	Apreciable
KEYLOGGING	4	4	16	Muy grave
SPAMMING	3			
INTERCEPCION DE E-MAILS	3	5	15	Muy grave
TERMINALES ABIERTAS	4	5	20	Muy grave
CAPTURA DE PANTALLAS	4	3	12	Importante
VIRUS	3	5	15	Muy grave
INCUMPLIMIENTO DE LEYES Y REGULACIONES	4	5	20	Muy grave
DESTRUCCION DE SOPORTES	3	4	12	Importante
INGENERIA SOCIAL	4	4	16	Muy grave
ACTUALIZACION DE CRIPTOACTIVOS	3	4	12	Importante
CARENCIA DE CIBERSEGURIDAD	4	5	20	Muy grave
DEFICIENCIAS EN ON BOARDING DIGITAL	4	5	20	Muy grave
FALTA DE CONVENIO DE TRANFERENCIA DE DATOS	4	5	20	Muy grave
NO UTILIZAN VPN	4	5	20	Muy grave
NO UTILIZAN IP DINAMICA	4	5	20	Muy grave
ABANDONO DE EQUIPOS	4	5		
EQUIPOS COMPARTIDOS	4	5	20	Muy grave
TOTAL:	90	123	366	Importante
TOTAL DE SUPUESTOS DE RIESGO: 27				
TOTAL MÁXIMO: 675				
TOTAL DE PROBABILIDAD / TOTAL MÁXIMO PROBABILIDAD	90/675= 1.3			
TOTAL GRAVEDAD / TOTAL MÁXIMO PROBABILIDAD		123/675=18.22		
DIFERENCIAS TOTALES		213/675=31.5	366/675= 54.2	Muy grave
RESULTADO FINAL				

Esta versión de Excel no admite la ejecución de los controles de

			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar
	Riesgo apreciable. Estudiar económicamente ai es posible introducir medidas
	Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

+ DATOS

DR. DAVID MERINO®
Consultor Empresarial y Atelier Patrimonial

LinkedIn
David E Merino Téllez

YouTube
Doc Merino

Chat IBLATAM Digital

IBLATAM Digital
Grupo Iberoamericano de Especialistas en Regulación Digital, Inteligencia Artificial y Ciberseguridad

Chat OC

Chat PLD

Chat Fiscal

TOP COMPLIANCE
AND RISK MANAGEMENT COMMUNITY ®

TLC MAGAZINE MÉXICO

HAGAMOS UN TRUEQUE

PODCAST DE TLC MAGAZINE MÉXICO

TRADE LAW & CUSTOMS magazine

Escúchanos en:

Spotify® Apple Podcasts

www.tlcmagazinemexico.com.mx

contacto@tlcmagazinemexico.com.mx