



Transformación Digital y los Riesgos

Manuel Acosta Abeyta



MEXICO



Situación Actual

- Ciudadano Digital
- Trabajo Híbrido: Remoto y en Oficina
 - Demasiados Datos
 - Aplicaciones en Sitio y en la Nube
 - Dispositivos móviles
 - Poca Cultura de Seguridad – usuarios descuidados
- Ciber crimen como negocio
 - (Malware, Ransomware, Criptomining, Ciber-Extorsión, etc)
 - Activos valiosos para el cibercrimen



Ciber crimen

Un **activo** es un bien que se posee ilegítimamente y que puede convertirse en dinero **electrónico** u otros medios líquidos equivalentes.

Web Server

Phishing Site
Malware Download Site
Warez / Piracy Server
Child Pornography Server
Spam Site

Bot Activity

Spam Zombie
DDoS Extortion Zombie
Click Fraud Zombie
Anonymization Proxy
CAPTCHA Solving Zombie

Account Credentials

eBay/Paypal Fake Auctions
Online Gaming Credentials
Web Site FTP Credentials
Skype/VoIP Credentials
Client Side Encryption Certificates

Lateral Movement

More Hacked PC
Advanced Persistent Threat (APT)
Data exfiltration
Industrial/Corporate Espionage



THE VALUE
OF A
HACKED
PC

E-Mail Attacks

Webmail Spam
Stranded Abroad Advance Scams
Harvesting E-mail Contacts
Harvesting E-mail Contacts
Access to Corporate E-mail

Virtual Goods

Online Gaming Characters
Online Gaming Goods/Currency
PC Game License Keys
Operating System License Key

Financial Credentials

Bank Account Data
Credit Card Data
Stock Trading Account
Mutual Fund / 401k Account

Reputation Hijacking

Facebook
Twitter
LinkedIn
Google +

Hostage Attacks

Fake Antivirus
Ransomware
Email Account Ransom
Webcam Image Extortion

Importancia de la Tecnología



Estrategia de Ciber Seguridad
para el Sector Público debe
ser clave en el proceso de
Transformación Digital

Bienestar

Productividad

Reducción de Costos



Inteligencia de Amenazas

Agilidad para identificar y clasificar activos
Mayor visibilidad para mayor protección.



Arquitecturas de Seguridad

Establecimiento de un comportamiento de referencia
Detección de intrusiones, intentos de comunicación con
atacantes



Detección de Amenazas/Brechas

Visibilidad en los flujos de información y rastreo de
comunicaciones entre dispositivos y aplicaciones



Automatización

Reportes detallados sobre hallazgos y un plan de ruta para
alcanzar el estado deseado de seguridad, basado en guías y
estándares de industria (Playbooks)



Respuesta a incidentes

Acelera la investigación ante incidentes críticos de seguridad



Sugerencias

- Metodologías - Mejores prácticas de seguridad
- Modelo de ciber seguridad para el sector público
 1. Arquitectura de Seguridad Integral
 2. Capacitación Continua para crear cultura de seguridad
 3. Evaluaciones continuas de terceros
 4. Automatización de arquitecturas de referencia
 5. Manejo de Crisis e Incidentes
- Colaboración con diferentes entidades para compartir inteligencia.
- Normatividad que ayude de manera explícita a crear los marco de seguridad / arquitectura de referencia escalable en todo tipo de gobierno.
- Todas las crisis son oportunidades de cambio y esta sin duda acelerará la madurez digital

Cisco México, 27 años siendo el aliado tecnológico y estratégico del país, impulsando su desarrollo y su plena inserción en la transformación digital



MEXICO



cisco.com/go/security