

# infosecurity<sup>®</sup>

MEXICO



**info**security<sup>®</sup>  
MEXICO



# El Arte de la (Ciber) Guerra

Como aprovechar la ventaja del defensor

## Entorno actual de amenazas En números

- 21 días - Tiempo promedio para detectar la presencia de un atacante
- 74% de los ataques no son detectados por la tecnología
- 10% se incrementó el costo de un incidente de 2020 a 2021
- \$4.24M USD – Costo promedio de un incidente en 2020
- \$4.62M USD – Costo promedio de un incidente de ransomware
- \$180 USD – Costo de un registro con datos personales
- 91% del ciber crimen inicia con un correo electrónico
- 1% de los correos es malicioso
- 23% de las investigaciones de Mandiant en 2021 involucraron Ransomware
- Los sectores con los costos más elevados por incidente son el financiero, salud, farmacéutico, Gobierno, Manufactura, entre otros.



Fuentes:

- Mandiant M-Trends 2022
- FireEye Email Threat Report, 2018
- Radicati Group Email Statistics Report, 2017-2021
- Mandiant Security Effectiveness Report 2020
- Ponemon Institute / IBM Security - Cost of a Data Breach Report 2021



- *“Es un principio de la guerra no suponer que el enemigo no vendrá, sino más bien confiar en la propia preparación para enfrentarlo; no suponer que no atacará, sino más bien hacerse uno mismo invencible.”*

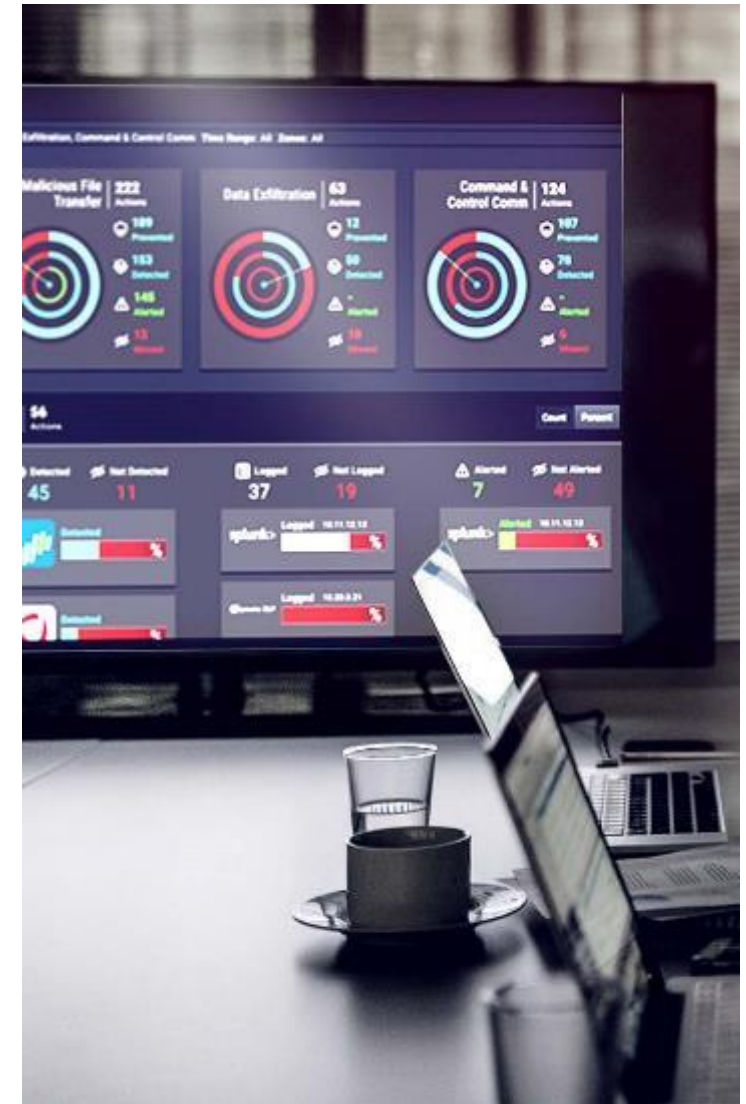
•  
- Sun Tzu

## Reglas del enfrentamiento

Considere las siguientes reglas que aplican a la mayoría de las organizaciones ante ataques cibernéticos:

- 1) “No suponer que el enemigo no vendrá”
- 2) La organización siempre tendrá una postura defensiva
- 3) Las batallas siempre se librarán en el entorno de la organización
- 4) Victorias se obtienen manteniendo a los atacantes fuera del entorno o mediante su expulsión antes de que el impacto a la organización sea relevante
- 5) El objetivo y victoria final consiste en mantener la operación, imagen y reputación de la organización a pesar de los embates de los atacantes

La organización tiene la **Ventaja del Defensor**



## Las cuatro funciones de la Seguridad de la Información



*“Si obtienes la ventaja del terreno, puedes vencer a los adversarios, incluso con tropas ligeras y débiles.”.  
(¿Cómo defender?)*

- **Gobierno de Seguridad.** “Generalmente, el manejo de muchos es igual al manejo de pocos. Es una cuestión de organización. Y el control de muchos es lo mismo que el control de pocos. Es cuestión de formaciones y señales.” (¿Qué?)
- **Gestión de Riesgos de Seguridad.** “Por eso, la capacidad de evaluar la situación del enemigo y calcular las distancias, así como el grado de dificultad del terreno para controlar la victoria, son virtudes del general superior. El que lucha con pleno conocimiento de esos factores está seguro de ganar.” (¿Por qué?)
- **Arquitectura de Seguridad.** “Así, un ejército victorioso obtiene sus triunfos antes de recurrir al combate; un ejército destinado a triunfar pelea con la esperanza de ganar.” (¿Cómo proteger?)
- **Ciber Defensa.** “La ventaja en una operación militar consiste en aprovecharse de todos los factores beneficiosos del terreno.”



*“Generalmente, el manejo de muchos es igual al manejo de pocos. Es una cuestión de organización. Y el control de muchos es lo mismo que el control de pocos. Es cuestión de formaciones y señales.”*

*- Sun Tzu*



## El Arte de la (Ciber) Guerra

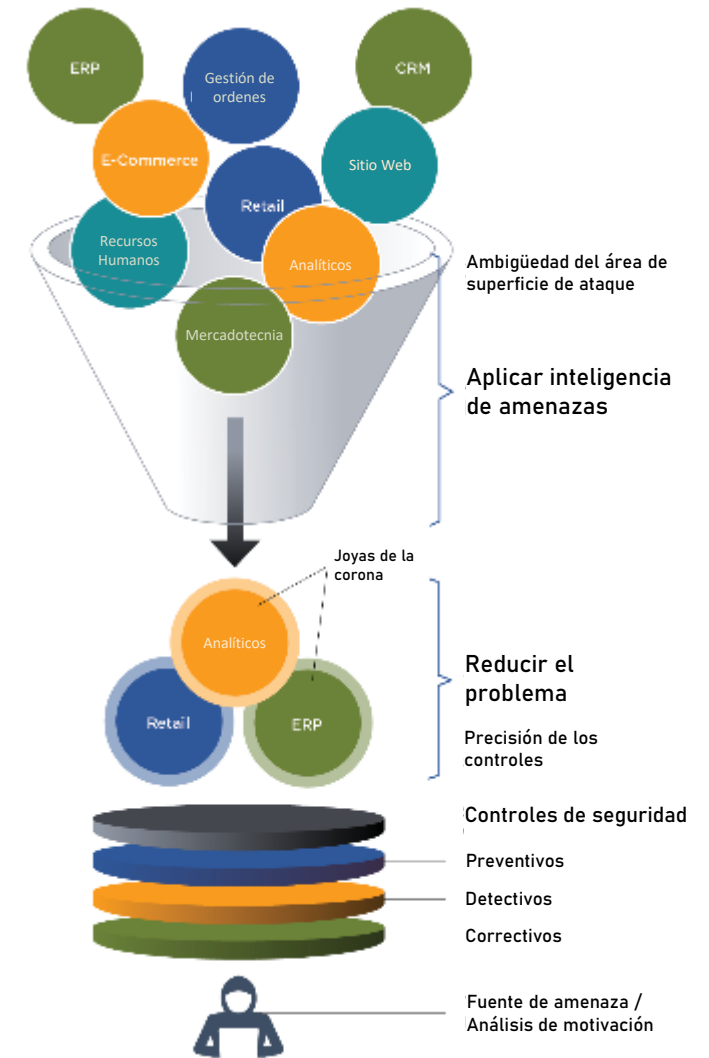
*“Por eso, la capacidad de evaluar la situación del enemigo y calcular las distancias, así como el grado de dificultad del terreno para controlar la victoria, son virtudes del general superior. El que lucha con pleno conocimiento de esos factores está seguro de ganar.”*

- Sun Tzu



## Enfoque de “joyas de la corona” para la gestión de riesgos

- Ayuda a encontrar el balance entre innovación y seguridad
- Enfoque en proteger los activos más críticos para el negocio (y más atractivos para los atacantes)
- La gestión proactiva de los activos considerados “joyas de la corona” le permite a la organización moverse más rápido y adaptarse a las ciber amenazas
- Aplicar inteligencia de amenazas para reducir el problema y emplear los controles de seguridad más adecuados





## El Arte de la (Ciber) Guerra

*“Así, un ejército victorioso obtiene sus triunfos antes de recurrir al combate; un ejército destinado a triunfar pelea con la esperanza de ganar.”*

- Sun Tzu

# Herramientas de seguridad

The image displays a comprehensive grid of security tool logos, organized into several key categories:

- Network & Infrastructure Security:** Includes logos for Advanced Threat Protection (e.g., Palo Alto, Cisco, Fortinet), NAC (e.g., Duo, Cisco), SDN (e.g., Cisco, VMware), DDoS Protection (e.g., Cloudflare, Akamai), DNS Security (e.g., Cisco, Fortinet), Network Firewall (e.g., Palo Alto, Cisco), and Deception (e.g., Splunk, Tenable).
- Web Security:** Features logos for Web Application Security (e.g., Check Point, Cisco, Imperva), Network Analysis & Forensics (e.g., Snort, Suricata), and various security services.
- Endpoint Security:** Shows logos for Endpoint Prevention (e.g., Symantec, McAfee, Trend Micro), Endpoint Detection & Response (e.g., Snovvisor, Palo Alto), and other endpoint protection solutions.
- Application Security:** Includes WAF & Application Security (e.g., Akamai, Cloudflare, Imperva), Application Security Testing (e.g., Burp Suite, Acunetix), and various security services.
- MSSP:** Lists logos for Traditional MSSP (e.g., AT&T, ATOS) and Advanced MSS & MDR (e.g., ATOS, IBM).
- Data Security:** Covers Encryption (e.g., McAfee, Symantec), DLP (e.g., Symantec, McAfee), Data Privacy (e.g., OneTrust, TrustArc), and Data Centric Security (e.g., Datto, Veritas).
- Mobile Security:** Features logos for mobile device management and security solutions (e.g., VMware, SOTI, Zimperium).
- Risk & Compliance:** Includes Risk Assessment & Visibility (e.g., Delve, Kenna), Risk Quantification (e.g., RiskIQ, Cofense), Pen Testing & Breach Simulation (e.g., Cobalt, Rapid7), and Security Awareness & Training (e.g., KnowBe4, SANS).
- Security Ops & Incident Response:** Shows logos for SIEM (e.g., Splunk, IBM), Security Incident Response (e.g., IBM, LogRhythm), and other security operations tools.
- Threat Intelligence:** Lists logos for threat intelligence platforms and services (e.g., Anomali, Blueliv, Intel 4i).
- IoT:** Features logos for IoT device security and management solutions (e.g., BlackBerry, IBM, Cisco).
- Messaging Security:** Includes logos for secure messaging and communication tools (e.g., AGARI, AREA 1, Cisco).
- Identity & Access Management:** Shows logos for authentication and access management solutions (e.g., Okta, One Identity, Saviynt).
- Digital Risk Management:** Lists logos for digital risk management and reputation management tools (e.g., OGD, Reliclic).
- Security Consulting & Services:** Features logos for various security consulting firms (e.g., Accenture, IBM, Deloitte).
- Blockchain:** Includes logos for blockchain security and solutions (e.g., Guardtime, Idee).
- Fraud & Transaction Security:** Shows logos for fraud prevention and transaction security tools (e.g., Biatch, DataVisor).
- Cloud Security:** Lists logos for cloud security solutions (e.g., AWS, Azure, Google Cloud, Palo Alto).



*“La ventaja en una operación militar consiste en aprovecharse de todos los factores beneficiosos del terreno.”*  
*“Si obtienes la ventaja del terreno, puedes vencer a los adversarios, incluso con tropas ligeras y débiles.”*

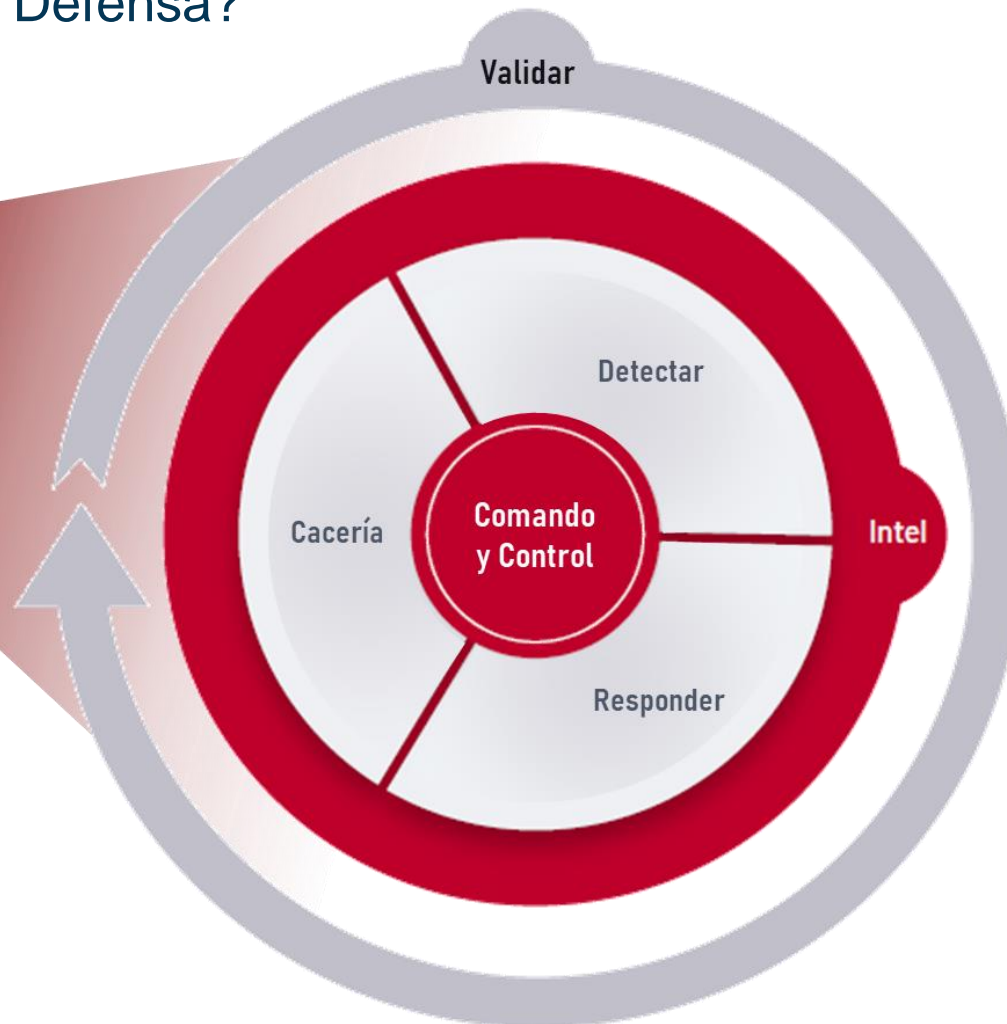
- Sun Tzu

***La Ventaja del Defensor es el concepto de que las organizaciones se defienden de ataques en su propio entorno. Esto proporciona una ventaja fundamental derivada del hecho de que tienen el control del entorno cuando enfrentan a sus adversarios.\****

***Sin embargo, las organizaciones tienen problemas en capitalizar esta ventaja.***

\* Para más información puede consultar el siguiente enlace: [The Defender's Advantage](#)

## ¿En qué consiste la Ciber Defensa?



**Inteligencia**  
Luz Guía



**Cacería**  
Cacería de Amenazas y  
Análisis de Compromiso



**Comando y Control**  
Mantener la Misión



**Detectar**  
Monitoreo de Alertas  
e Investigación

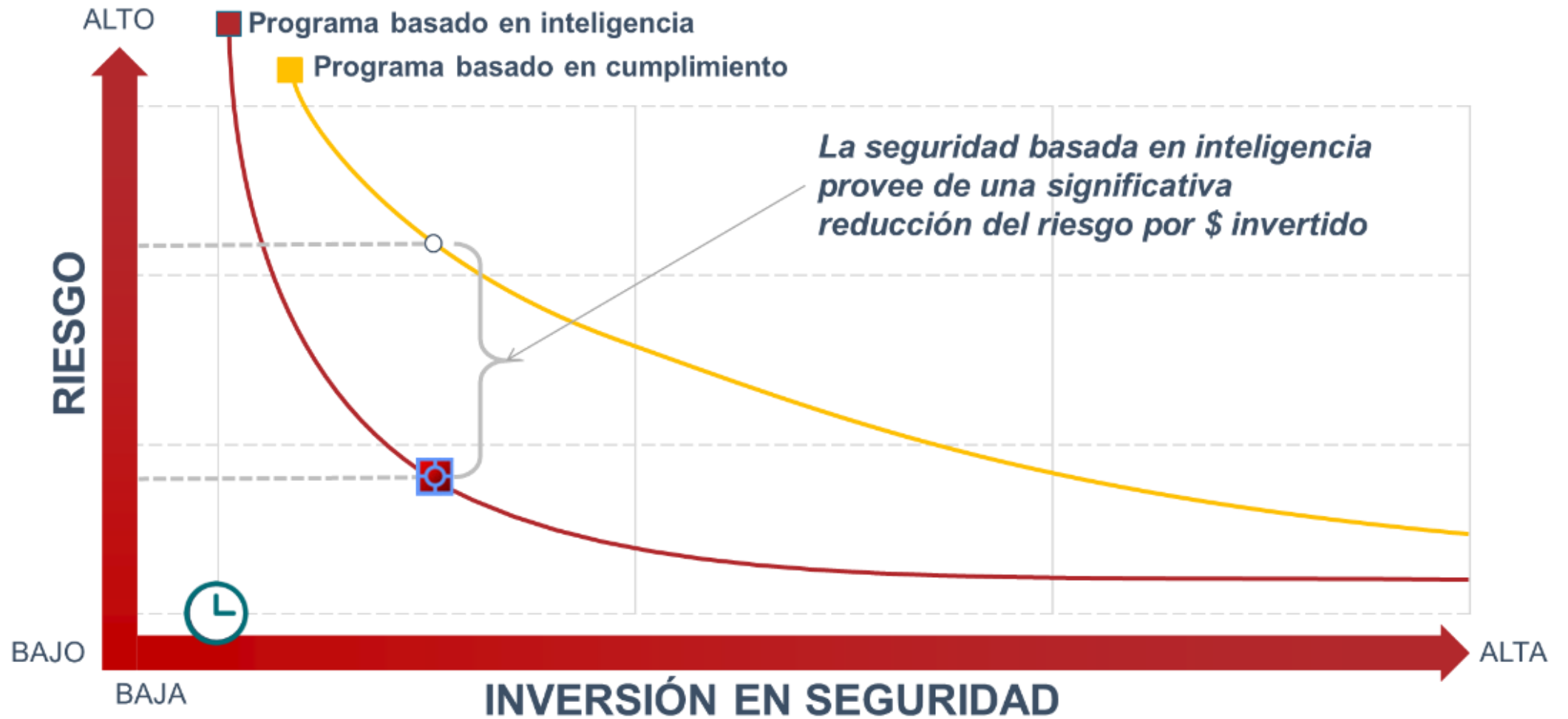


**Responder**  
Respuesta a Incidentes  
y Recuperación



**Validar**  
Pruebas Dirigidas y  
Validación de Controles

## Enfoque basado en Inteligencia



## Inteligencia es la luz guía

Las organizaciones se suscriben a un promedio de

**7.5**

Feeds de Inteligencia de Amenazas\*

**66.5%**

aún diseminan CTI a través de correo electrónico, PPT, y hojas de cálculo\*\*

Sólo

**43%**

ha documentado requisitos de CTI\*\*

- ¿Qué es lo que se quiere lograr con inteligencia?
- ¿Quién va a consumir la inteligencia?
- ¿Cómo se comunicará la inteligencia?
- ¿Cómo se obtendrá retroalimentación y se medirá el consumo?
- ¿Qué fuentes de información se necesitan?

Muchas organizaciones se suscriben a feeds de inteligencia de amenazas, pero tienen problemas para hacer operativa la inteligencia y emplearla para proteger al negocio.

*Se enfocan en la cantidad de IOCs proporcionados en lugar de la calidad y relevancia de los mismos.*

\*Forrester Wave ETIS Q1, 2021

\*\*SANS CTI Survey 2021





**Perfil de Amenazas**



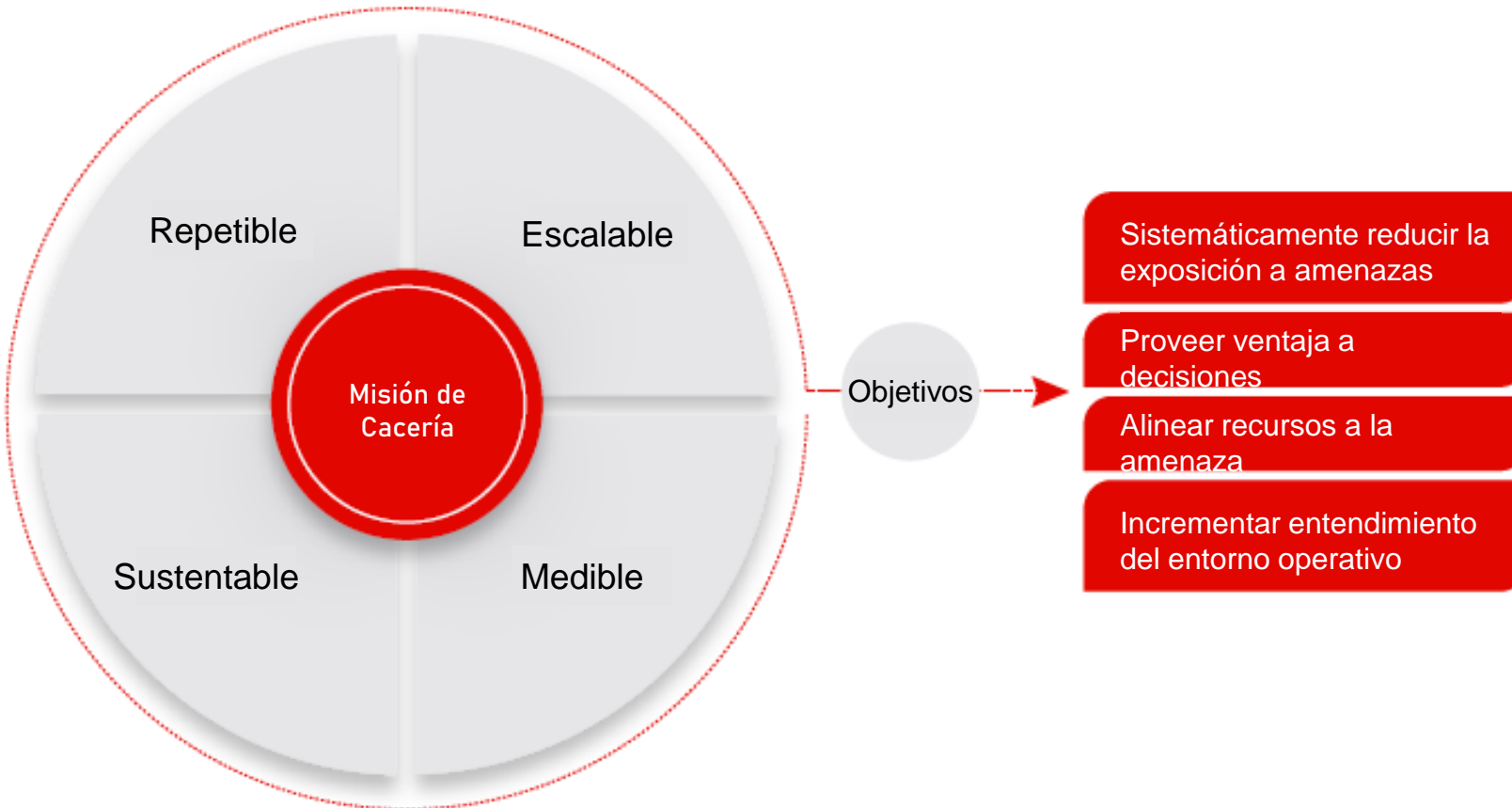
**Perfil de Amenazas**

*“Conoce a tu enemigo y conócete a ti mismo; en cien batallas, nunca estarás en peligro.”*

- Sun Tzu



## Cacería de amenazas



## El Arte de la (Ciber) Guerra

*“Para mantener una defensa infaliblemente segura, defiende donde no haya ataque.”*

- Sun Tzu

Emplear inteligencia sobre un adversario y sus operaciones para buscar en el entorno de la organización por compromisos previos o activos.



**Detectar**

Realidades

- 1 Las brechas de seguridad inevitables
- 2 Las vulnerabilidades
- 3 ¿Dónde los sistemas están cada vez más conectados?

Visión

**DETECTAR**

Red equipada con tecnología de seguridad y monitoreada por personal de seguridad

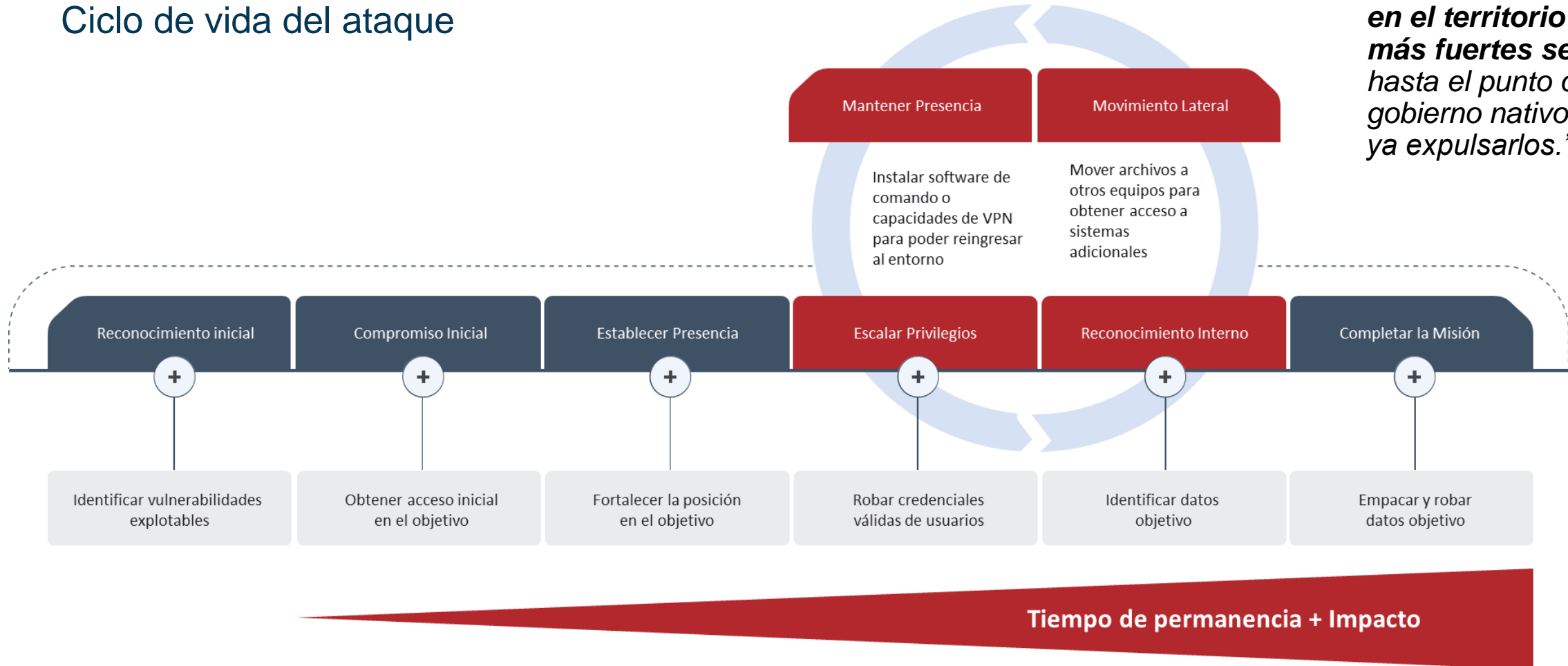
**RESPONDER**

Proceso eficaz de respuesta a incidentes y gestión de crisis de ciberseguridad

**CONTENER**

El BCP y el DRP consideran el compromiso de los activos críticos

## Ciclo de vida del ataque



*“En una invasión, por regla general, **cuanto más se adentran los invasores en el territorio ajeno, más fuertes se hacen, hasta el punto de que el gobierno nativo no puede ya expulsarlos.**”*

- Sun Tzu



## Validación y pruebas dirigidas

- Ponga a prueba los controles en:
  - Tecnología
  - Procesos
  - Gente

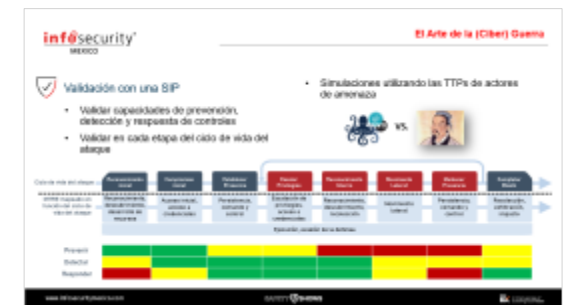
### Tipos de prueba:

- Pentest
- Red Team
- Purple Team
- Table Top Exercise (TTX)
- Security Instrumentation Platform (SIP)

## El Arte de la (Ciber) Guerra

*“Conoce al enemigo, conócete a ti mismo; tu victoria no correrá nunca peligro. Conoce el terreno, conoce las condiciones meteorológicas; tu victoria será entonces total.”*

- Sun Tzu





## Comando y Control

- Un reto común que enfrentan las organizaciones es que cada equipo de trabajo actúa de forma independiente con poca o nula comunicación
- La función de Comando y Control se encarga de:
  - Establecer procesos para la gestión de recursos, comunicaciones, métricas y gestión de crisis
  - Transferir información entre los distintos equipos de trabajo
  - Gestión de incidentes mayores
  - Toma de decisiones con autoridad para actuar

*“Por eso el gobernante esclarecido es prudente y el buen general está prevenido contra la acción precipitada. De ese modo, el Estado se mantiene en seguridad y se preserva el ejército.”*

- Sun Tzu

**info**security<sup>®</sup>  
MEXICO



**El Arte de la (Ciber) Guerra**  
Como aprovechar la ventaja del defensor

# Conclusiones

## Conclusiones

- “No suponer que el enemigo no vendrá”
- Protección ≠ Defensa
- Prestar más atención a la función de Ciber Defensa
- El principal objetivo es mantener la operación, imagen y reputación de la organización a pesar de posibles ataques exitosos
- El impacto será mayor entre más tiempo pase un atacante en el entorno y es más difícil expulsarlo
- La organización debe tomar control de su terreno y aprovechar la ventaja que le ofrece para defenderse

*“Generalmente, aquel que primero ocupa el campo de batalla y espera a su enemigo, está descansado.”*

*- Sun Tzu*



**M**ANDIANT

YOUR CYBERSECURITY ADVANTAGE

# infosecurity<sup>®</sup>

MEXICO

