



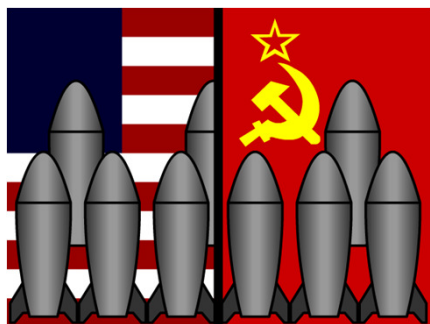
**"La Evolución de la Ciberguerra y Ciberdefensa"
¿Cómo defenderse de 3.000 Millones de atacantes potenciales?"**

www.gms.com.ec

Nombre del presentador

Fecha

Cold War to Cyberwar



Teoría de Juegos – Cybersecurity Game

Un juego es una descripción de la interacción estratégica entre los intereses opuestos o cooperantes, donde se toman en cuenta las limitaciones y las recompensas para las acciones. Por otro lado, un jugador es una entidad básica en un juego que tiene la tarea de hacer elecciones para las acciones. Un jugador puede representar a una persona, máquina o grupo de personas dentro de un juego.



*The enemy invariably attacks on two occasions:
when they're ready.
when you're not.*

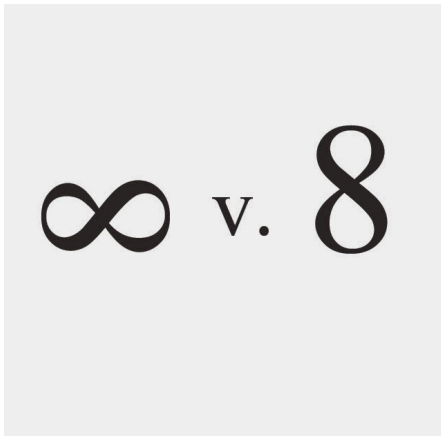
- Murphy's Laws of War

Cybersecurity Game - Actores

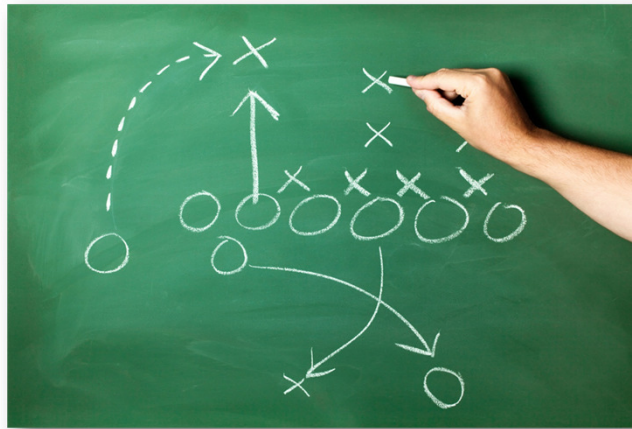


Cybersecurity Game – Tipo de Juego

Infinito vs. Finito



Juegos Estratégicos

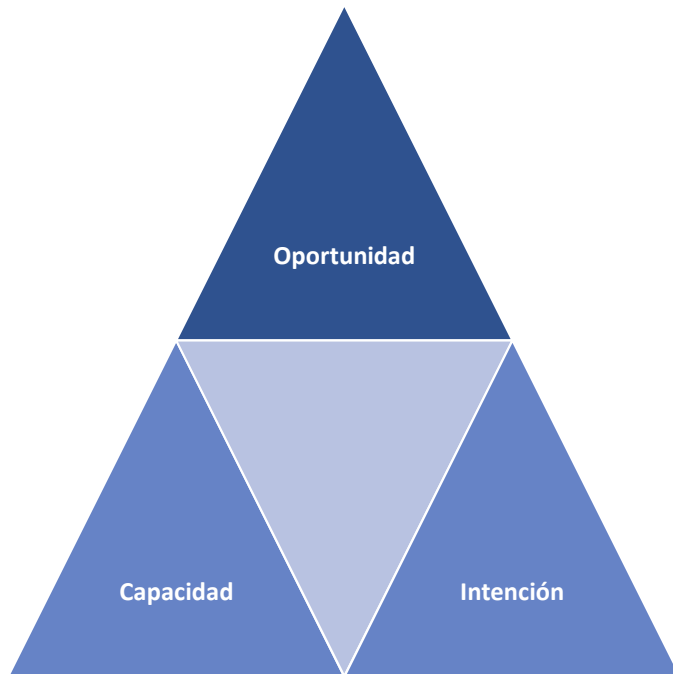


Información Perfecta vs. Imperfecta



Juego de Suma Zero: Unos ganan, otros pierden!!!

Cybersecurity Game – Aspectos del Cibercimen



Un control/defensa que amenaza aborda?

Cómo responderá?

El defensor proporcionará una buena relación entre la inversión y la reducción de la capacidad del atacante?

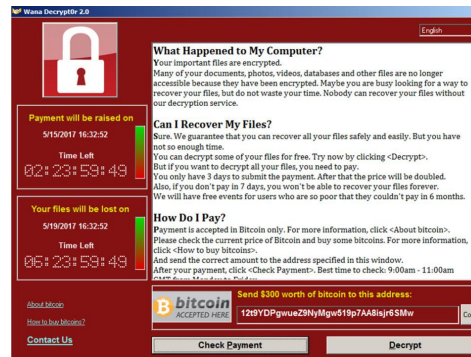
Actores de Amenaza

Los atacantes tienen restricciones de recursos!!



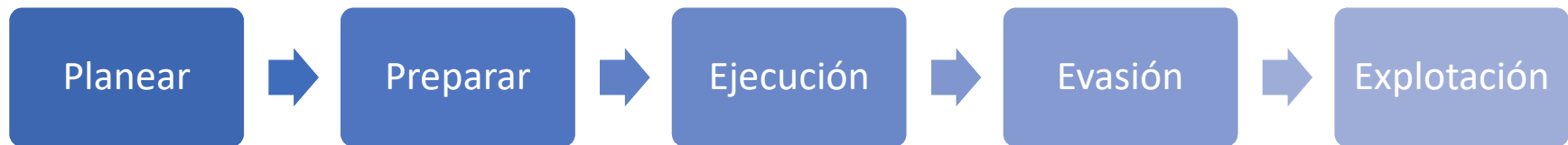
EQUIFAX

Tienen sus motivos!!!



SONY

Ciberataques: Ciberoperaciones



¿Cómo Defenderse?



¡¡Es inevitable ser atacado!!



¿Cómo Defenderse?



Oportunidad

Reducir los vectores de ataques.

Tarea ardua, casi imposible.

Implementación de Procesos.

Todo se puede hackear!

*If you make it impossible for the enemy to get in
then you can't get out*

- Murphy's Laws of War

¿Cómo Defenderse?



Capacidad

Inversión en tecnología.

Los defensores deben cubrir todo. Los atacantes descubrir solo una.

Implementar controles de las mejores prácticas según el riesgo.

*The important things are always simple; the simple things are always hard .
The easy way is always mined.*

- Murphy's Laws of War

¿Cómo Defenderse?



Intención

Reduzca lo “sexy” de su información.

Los atacantes temen ser descubiertos:

- Implementar trampas.
- Monitoree sus acciones.
- Primeras etapas de detección

The key insight then, is that we shouldn't deploy boxes that look vulnerable on the network, we should deploy boxes that look valuable instead! - Haroon Meer

Construya un “Patio de Juegos”

Higiene de
Credenciales

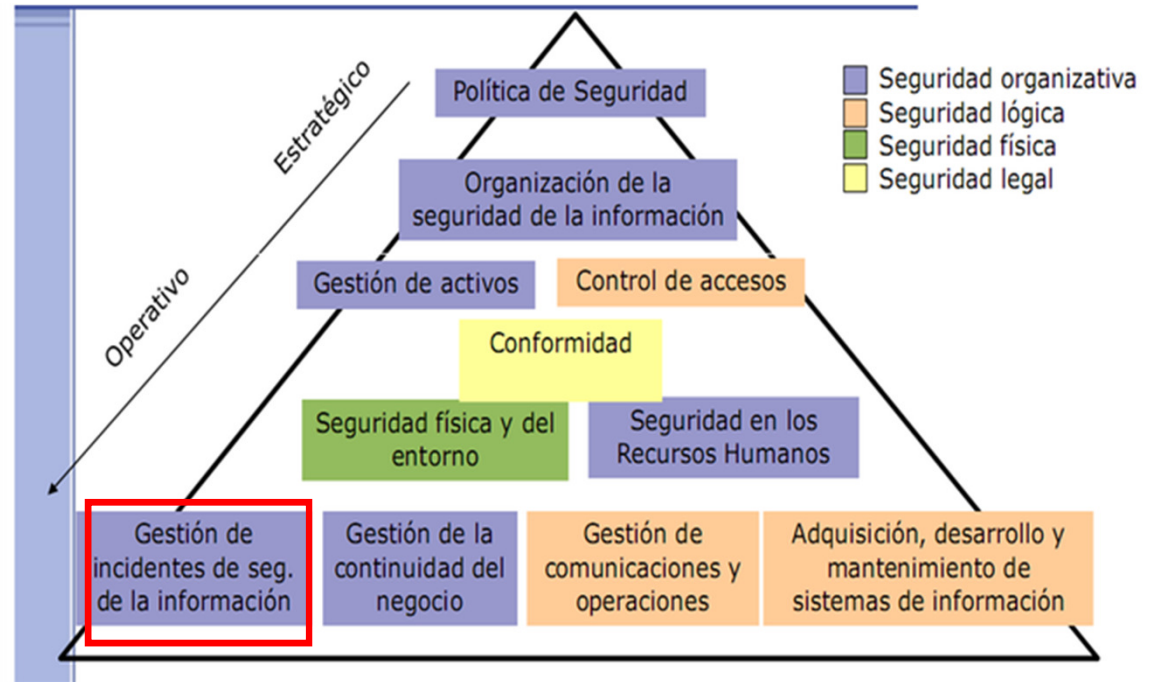
Segmentación
de Red



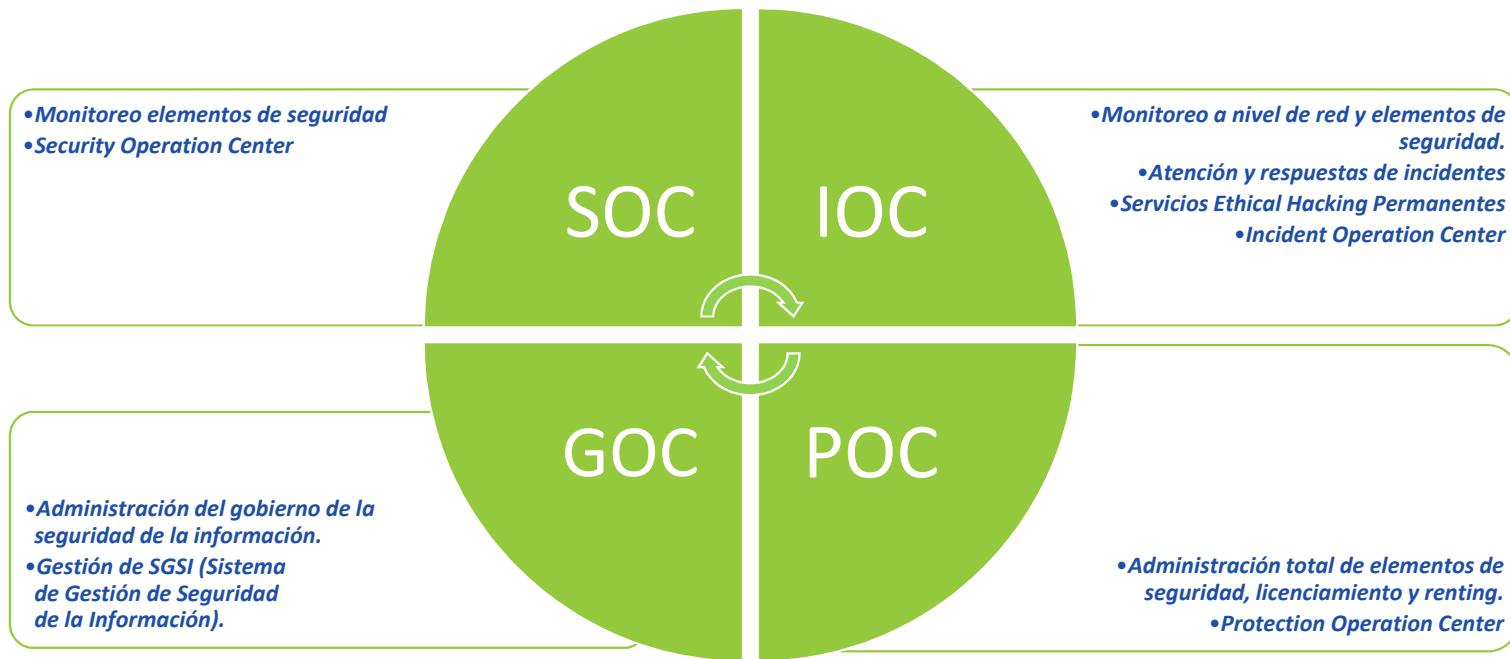
Menor
Privilegio

Monitoreo
Orientado

Cambio de Enfoque




¿Cómo te ayuda GMS?






www.gms.com.ec

 [GMS Seguridad de la Información](#)

 [@GMSseguridad](#)

 [GMS Seguridad de la Información](#)