

---

# **Tendencias en Inseguridad Informática**

*Algunos referentes internacionales para revisar*

Jeimy J. Cano, Ph.D, CFE

SEGURINFO

-ACIS-

# Agenda

---

- Introducción
- Antecedentes de terrorismo online
- Motivaciones para hablar de Seguridad Informática
- Avances en vulnerabilidades y ataques
- Evaluaciones y auditorías de seguridad informática
- Reflexiones sobre el futuro de la inseguridad informática

# Introducción

---

- La criminalidad informática organizada viene creciendo de manera exponencial.
- Los intrusos cada vez más conocen en profundidad los detalles de las tecnologías y sus limitaciones
- Las vulnerabilidades cada vez son más especializadas y técnicas
- El perfil del intruso cambia con el tiempo y su formación: más información, más herramientas, más interés.
- Los atentados terroristas del 11-S y el 11-M cambiaron la manera de entender la seguridad.

# Terrorismo Online

---

- Envenenamiento de caché de DNS
- Negación de servicios de 10 de los 13 DNS Root
- Ataques masivos con Nimda, código rojo, slammer
- Vulnerabilidades en BGP – Border Gateway Protocol
- ¿Apagón de New York?

¿Internet Infraestructura Crítica?

# Motivaciones – Seguridad Informática

---

- Recuperación de desastres y continuidad de negocio
- Respaldos de datos – Backups
- Concientización de usuarios
- Auditorías periódicas de seguridad
- Admon centralizada de la gestión de la seguridad
- Monitoreo permanente de infraestructura y empleados
- Protección de la propiedad intelectual
- Certificación y acreditación de aplicaciones de misión crítica
- Designación de oficiales de seguridad

¿Gobierno de la Seg. Inf.?

# Vulnerabilidades y ataques

---

- Se advierte una combinación explosiva, que mezcla la técnica, la experiencia y la propagación
  - WEB + Motivación Técnica + Fallas de Procedimientos



Vectores de ataques masivos

¿Gobierno de la Inseguridad?

# Evaluaciones y Auditorías

---

- ¿Nuestra seguridad hoy es mejor que hace un año?
- ¿Qué nivel de fraude ocupacional y fallas de seguridad puedo tener?
- ¿Mi póliza de riesgos, incluye el tema de tecnologías de información?

¿Qué hacer?

Validación de controles +  
Administración de riesgos +  
Pruebas+Monitoreo +  
Pólizas de *hacking*

---

> *Nivel de Gestión en Seguridad Informática*

# Futuro de la Inseguridad Informática

---

## ○ Características de la Inseguridad

- *Objetiva*
- *Es viable definirle cuota superior*
- *Tangible*
- *Es una propiedad **inherente** de un sistema*
- *No se requiere modelarla para que el resultado se presente.*



- Investigación y Desarrollo
- Sistemas de inteligencia en Seguridad informática
- Compartir la experiencia positiva y negativa
- Centros de prevención y atención de incidentes
- Análisis de tendencias multidimensionales de ataques
- Ganas de aportar y crecer en el tema.
- Iniciativas!



# Futuro de la Inseguridad Informática

---

## Más predicciones fruto de la experiencia

Aquí no pasada nada!

¿Qué es lo peor que nos puede pasar?

¿No nos ha pasado nada antes, porqué si ahora?

¿Si hemos vivido sin seguridad antes, porqué ahora no?

Deje así!

# Reflexiones

---

**Comentarios?**

---

# **Tendencias en Inseguridad Informática**

*Algunos referentes internacionales para revisar*

Jeimy J. Cano, Ph.D, CFE

SEGURINFO

-ACIS-