Intendencia de Montevideo

Security Operation Center

Segurinfo 2017

María Eugenia Corti

maria.corti@imm.gub.uy

Intendencia de Montevideo

Las cuatro funciones claves de un CISO moderno

* Software Engineering Institute | Carnegie Mellon University

Intendencia de Montevideo

Función de seguridad tradicional

* Software Engineering Institute | Carnegie Mellon University

Intendencia de Montevideo

Funciones de seguridad de la información modernas

Protect / Shield / Defend / Prevent	Monitor / Detect / Hunt	Respond/ Recover / Sustain
		

Management,
Governance,
Compliance,
Education,
Risk Management.

* Software Engineering Institute | Carnegie Mellon University

Intendencia de Montevideo

¿Qué es un SOC?

Un SOC es un equipo, formado principalmente por analistas de seguridad, organizado para detectar, analizar, responder, informar y prevenir incidentes de ciberseguridad.

* MITRE – “Ten Strategies of a World-Class SOC”

Intendencia de Montevideo

¿Por qué un SOC?

- **Porque proteger, defender no es suficiente (firewall, IPS, WAF)**
- **Es necesario centralizar la información de las operaciones de seguridad.**
- **Permite prevenir, detectar y responder en forma temprana**
- **Permite realizar análisis posteriores**

Intendencia de Montevideo

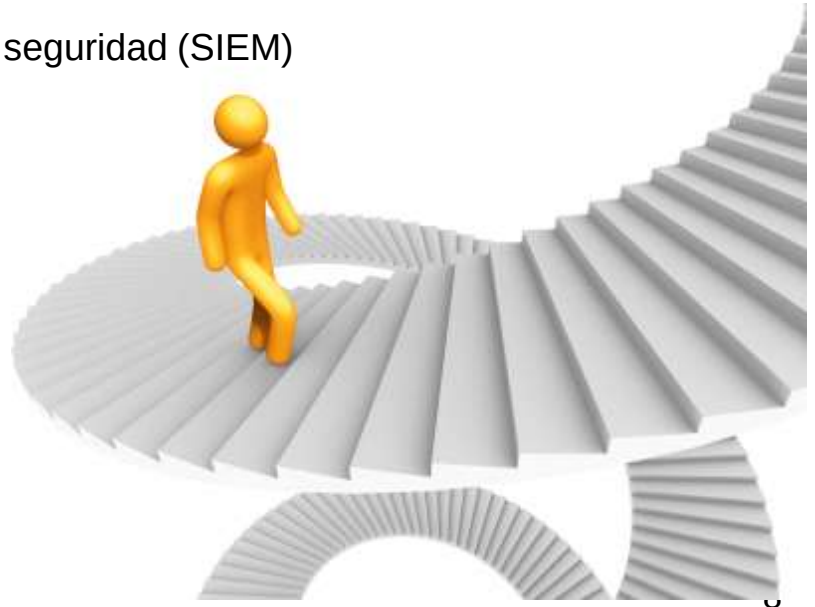
Tríada de operaciones de seguridad

* SANS Institute

Intendencia de Montevideo

Nuestro camino

- Contar con el apoyo de la dirección
- Asignar personal con perfil adecuado
- Diseñar estrategia de recolección y análisis de información
- Adquirir y configurar herramientas de monitoreo de seguridad (SIEM)
- Definir procesos de análisis, respuesta y reporte
- Convencer de la necesidad de contar con un SOC
- Revisión y mejora continua



Intendencia de Montevideo

Gracias