Ciberseguridad para redes de comunicación e infraestructura crítica en organismos estatales

Ciberseguridad para redes de comunicaciones e infraestructura critica

Juan Ignacio Munté

Licenciatura en tecnología de la información.

UP
Universidad de Palermo

Agenda

II Introducción.

III Antecedentes y problemática actual.

IV Enumeración de las tecnologías y tipos de ciber ataques.

V Riesgos, vulnerabilidades y amenazas.

VI Soluciones Propuestas.

VII Conclusiones.

VII Futuras líneas de investigación.

UP
Universidad de Palermo

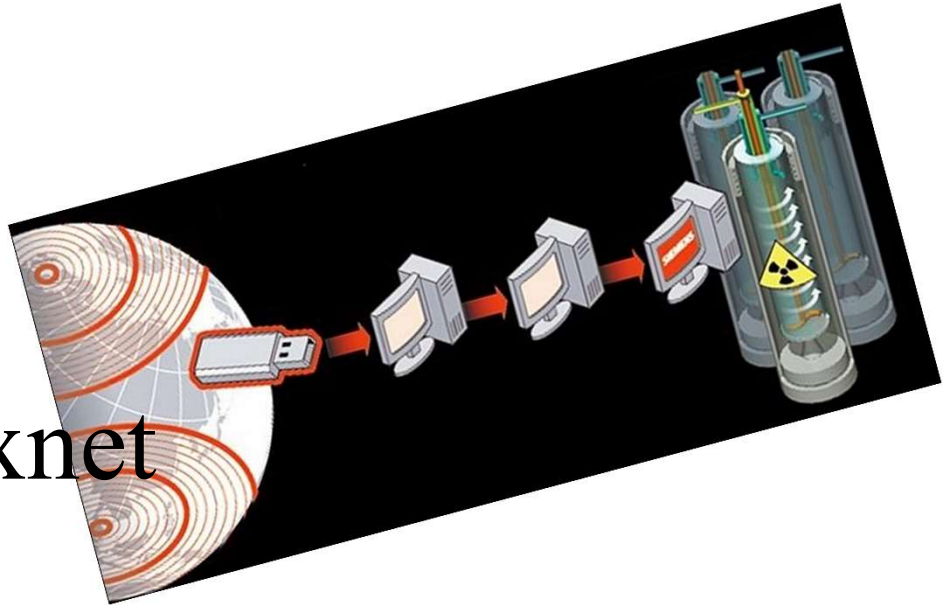
Introducción

- Era digital
  - Guerra cibernética entre países
- Ciberataques
  - Origen y evolución
- Ciberarmas
  - Stuxnet
  - Flame
  - WannaCry

UP
Universidad de Palermo

Introducción





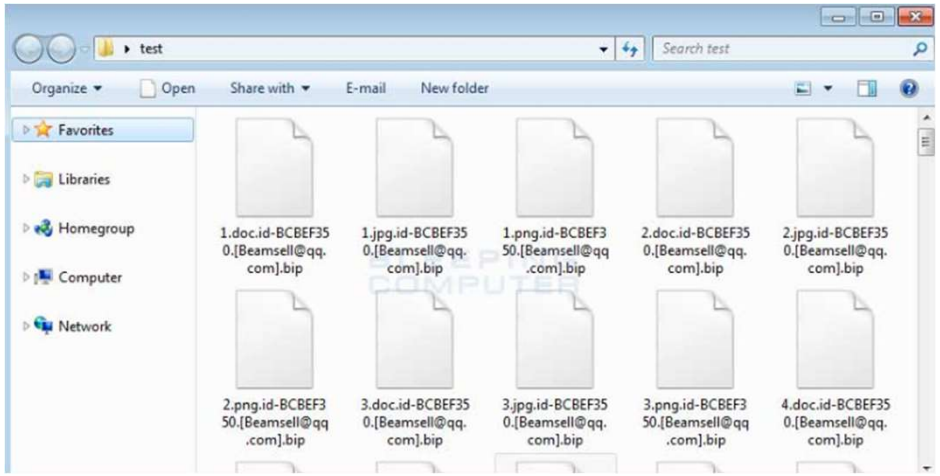
Stuxnet



Flame

Introducción





WannaCry

UP Universidad de Palermo

Antecedentes y problemática actual







UP
Universidad
de Palermo

Enumeración de las tecnologías y tipos de ciber ataques

- Tecnologías actuales en uso
  - Firewalls
  - Webservers
  - IPS /IDP
  - DLP
- Ciberataques
  - Phishing
  - DDOS
  - SQLi
  - Fuerza Bruta
  - Explotación de vulnerabilidades
  - Pharming

UP Universidad de Palermo

Riesgos, vulnerabilidades y amenazas.

- Activos estratégicos de las organizaciones.
- Ciber riesgos para los sistemas estratégicos.
- Organismos de Control de ciberseguridad en Argentina.

UP
Universidad de Palermo

Soluciones Propuestas.

Normativas y Directrices de ciberseguridad

Framework de Nist

CSF Core

CFS Tiers

CSF Profile

UP
Universidad
de Palermo

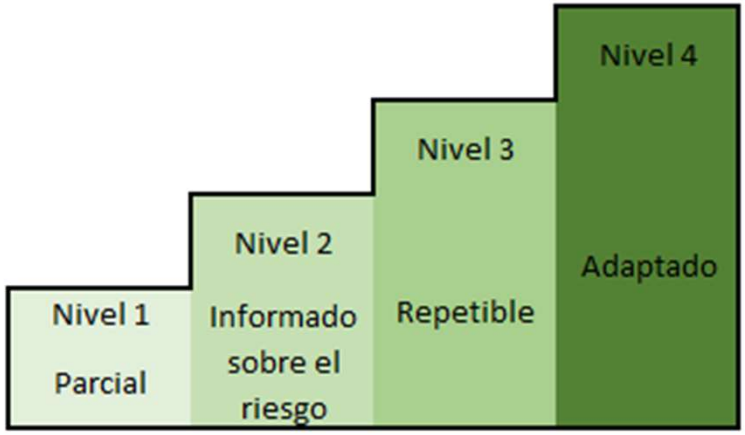
CSF Core

Nombres e identificadores de funciones y categorías principales de CSF 2.0

Función	Categoría	Identificador de Categoría
Gobernar (GV)	Contexto organizacional	GV.OC
	Estrategia de Gestión de riesgo	GV.RM
	Funciones, responsabilidades y autoridades	GV.RR
	Politica	GV.PO
	Vigilancia	GV.OV
	Gestión de riesgos de la cadena de suministro de ciberseguridad	GV.SC
Identificar (ID)	Gestion de Archivos	ID.AM
	Evaluacion de riesgos	ID.RA
	Mejora	ID.IM
Proteger (PR)	Gestión de identidades, Autenticación y control de acceso	PR.AA
	Concientización y capacitación	PR.AT
	Seguridad de datos	PR.DS
	Seguridad de la plataforma	PR.PS
	Resiliencia de la infraestructura tecnológica	PR.IR
Detectar (DE)	Monitoreo continuo	DE.CM
	Análisis de eventos adversos	DE.AE
Responder (RS)	Administración de Incidentes	RS.MA
	Análisis de incidentes	RS.AN
	Informes y comunicación de respuesta a incidentes	RS.CO
	Mitigación de Incidente	RS.IR
Recuperar (RC)	Ejecución de un plan de recuperación de incidentes	RC.RP
	Comunicación de recuepración de incidentes	RC.CO

UP Universidad de Palermo

CFS Tiers



Niveles del CSF para la gobernanza y gestión de riesgo de ciberseguridad

UP
Universidad de Palermo

CFS Profile



Pasos para crear y utilizar un perfil organizacional

UP Universidad de Palermo

Zero trust



UP
Universidad
de Palermo

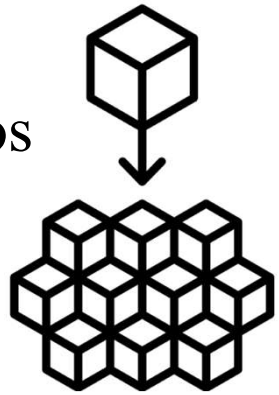
Conclusiones.

- Importancia de la coordinación y colaboración Multilateral
- Vulnerabilidad de las Infraestructuras Críticas
- Evolución y Sofisticación de los Ataques Cibernéticos

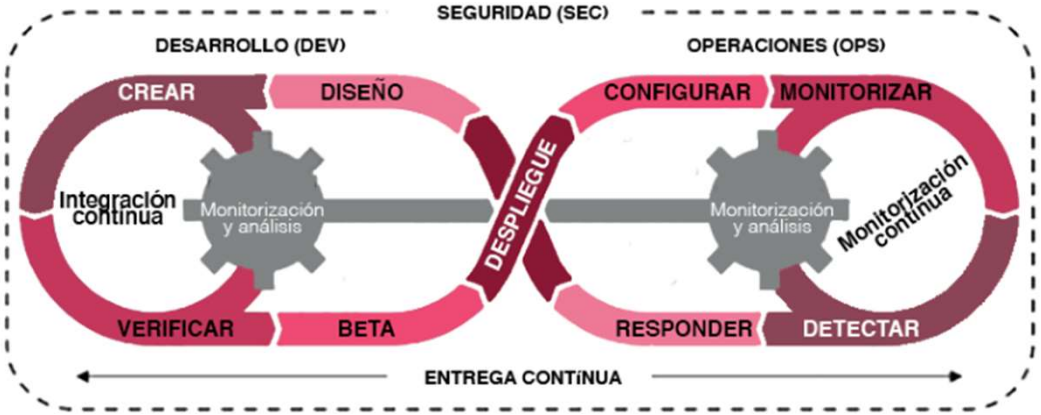
UP Universidad de Palermo

FUTURAS LÍNEAS DE INVESTIGACIÓN

Microservicios



Desarrollo de Software Seguro



UP Universidad de Palermo

Muchas gracias!

UP
Universidad
de Palermo

¿ Preguntas ?

UP
Universidad
de Palermo