Foundstone
STRATEGIC SECURITY

Un modelo abierto de ciberseguridad ¿Puede ayudar en Latinoamérica?

Mateo Martinez, CISSP, PCI QSA

Foundstone Professional Services Consultant

Introducción

Noticias y contexto de Ciberseguridad

McAfee
An Intel Company

Algunas noticias de Ciberseguridad

REUTERS

TOP NEWS

Ukraine hit by cyberattacks: head

Tue, Mar 04 06:08 AM EST

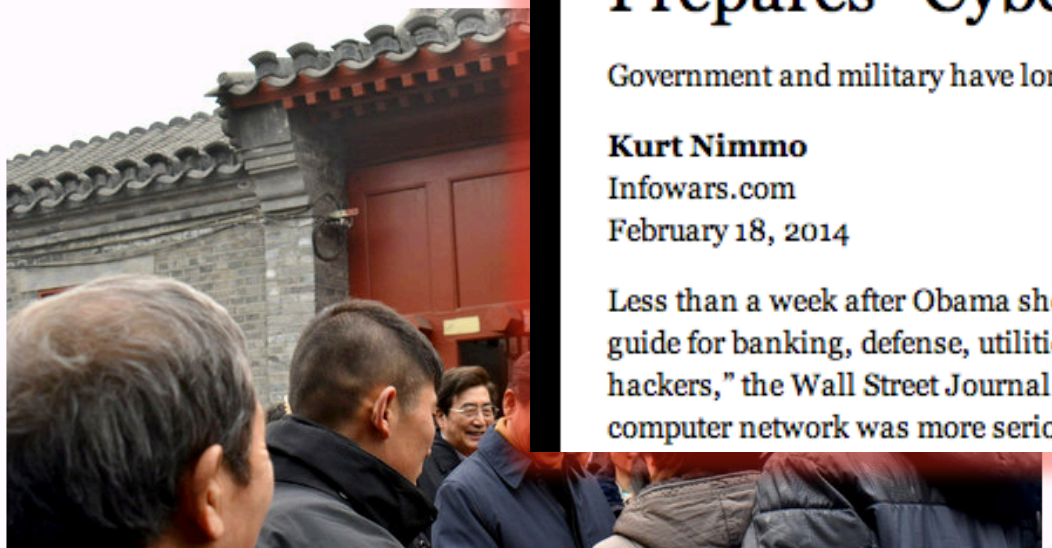
(Reuters) - Ukraine's telecommunica

SECTIONS HOME SEARCH

ASIA PACIFIC

China's President Will L

By DAVID BARBOZA FEB. 27, 2014



ALEX JONES' INFOWARS.COM BECAUSE THERE IS A WAR ON

Home Alex Jones Radio Show News Multimedia Forum Store Contact Top Stories Breaking

Navy Describes Iran Hack Attack As Obama Prepares "Cybersecurity Framework"

Government and military have long a history of deception and lies

Kurt Nimmo
Infowars.com
February 18, 2014

Less than a week after Obama showed off the government's "cybersecurity framework" and "best practices guide for banking, defense, utilities and other industries to help protect themselves against attacks by hackers," the Wall Street Journal reports the supposed Iranian hack of the Navy's largest unclassified computer network was more serious than originally reported.

Algunas noticias de Ciberseguridad regional

Colombia, primer país latino
ciberdefensa

La inicia
el Grupo
Fuer

Bog

méx

Uruguay: Realizarán un simulacro regional de ataque
cibernético masivo

LA NACI
Indispensable para decidir

COBERTURA ESPECIAL - CYBERWAR - PENSAMENTO

05 de Fevereiro, 2014 - 09:25 (Brasília)

EXECUTIVOS BRASILEIROS NÃO TÊM IDEIA DO QUE É CIBE
SEGURANÇA

Compartilhe Curtir 16 Tweet 7

SUPERTEL
SUPERINTENDENCIA DE TELECOMUNICACIONES

República del Ecuador

INICIO | ORGANIZACIÓN | MARCO JURÍDICO | RESOLUCIONES | ENLACES | INFORMACIÓ

CNT EP reportó un corte en la interconexión del servicio de voz hacia las operadoras SETEL y Global Crossing

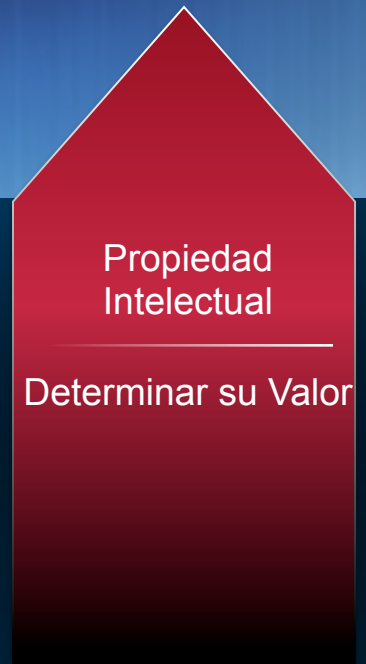
Like 0 Tweet 0

Thursday, 06 March 2014 09:26

Contexto de la Ciberseguridad

Perdidas en propiedad intelectual e información confidencial

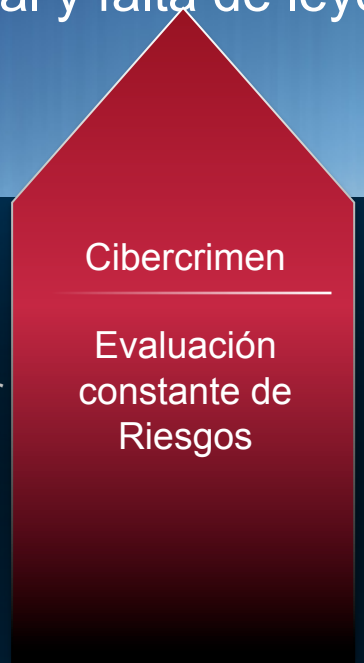
- Espionaje económico
- El Ciberespionaje no es un juego nuevo
- La información robada no se pierde realmente
- Espionaje personalizado
- La organización no se entera (perdió el control de su información)



Contexto de la Ciberseguridad *(cont.)*

Cibercrimen, cientos de millones de dólares en perdidas cada año.

- Robo de identidad
- Interrupción de servicios
- No tratados directamente como seguridad nacional
- Las pérdidas directas de los consumidores puede ser el componente más pequeño de esta actividad
- Costo Social y falta de leyes



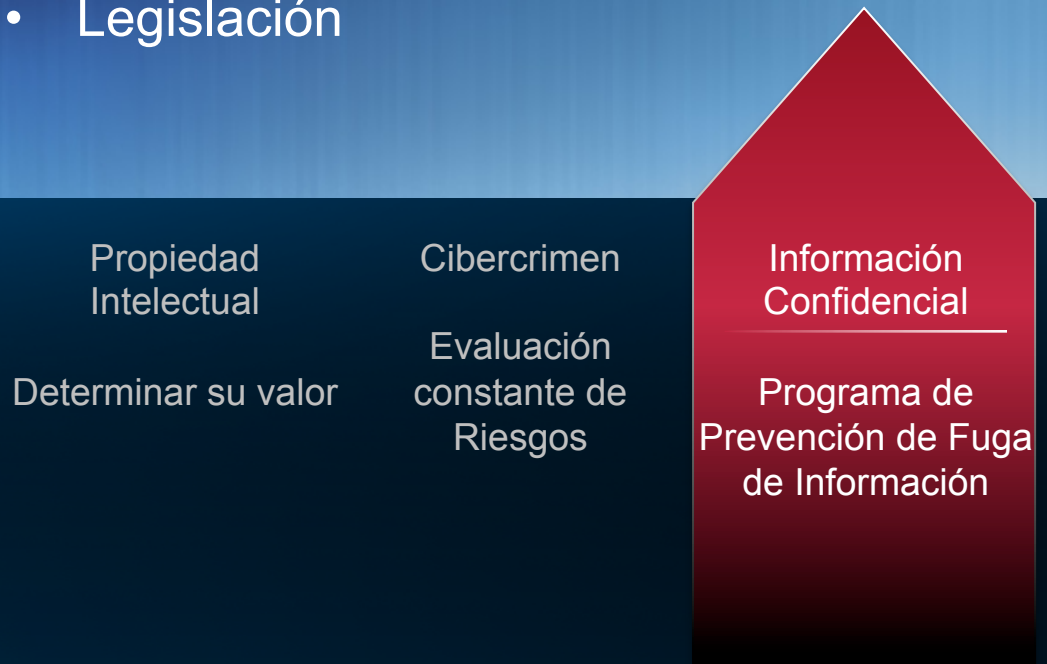
Propiedad Intelectual

Determinar su valor

Contexto de la Ciberseguridad *(cont.)*

Perdida de Información organizacional sensible, incluyendo posible manipulación de mercado de valores

- Información Confidencial
- Información Personal
- Propiedad Intelectual
- Privacidad
- Legislación



Contexto de la Ciberseguridad *(cont.)*

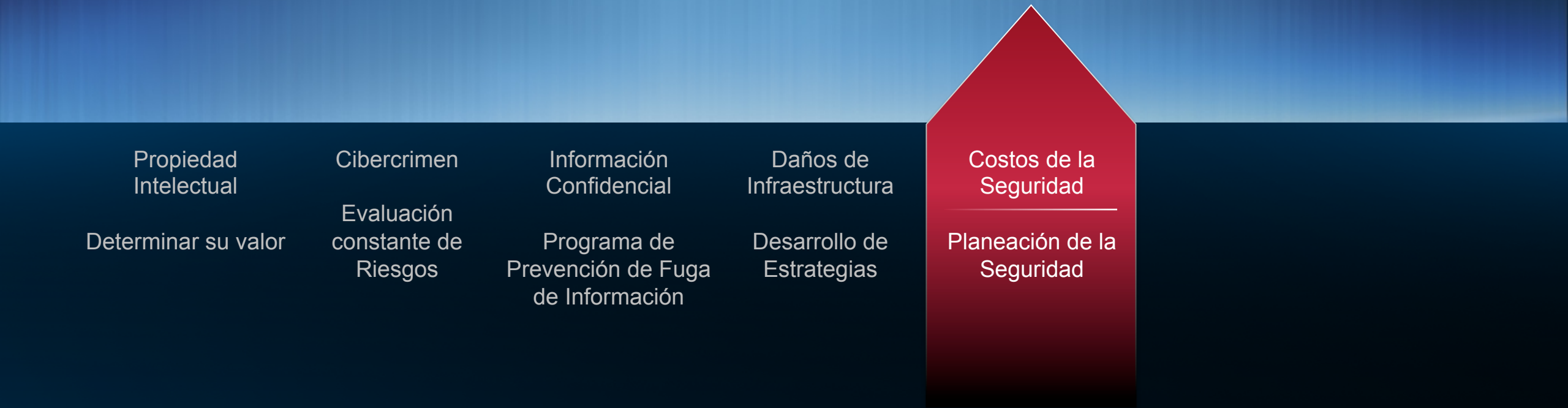
Daños de Infraestructura crítica, incluyendo interrupción de servicios, fallas totales y fatalidades

- Falta de servicios básicos
- Impacto en Personas
- Impacto ecológico
- Impacto económico
- Daños físicos directos y colaterales

Contexto de la Ciberseguridad *(cont.)*

Costo adicional en aseguramiento de redes, polizas y recuperación de ataques cibernéticos

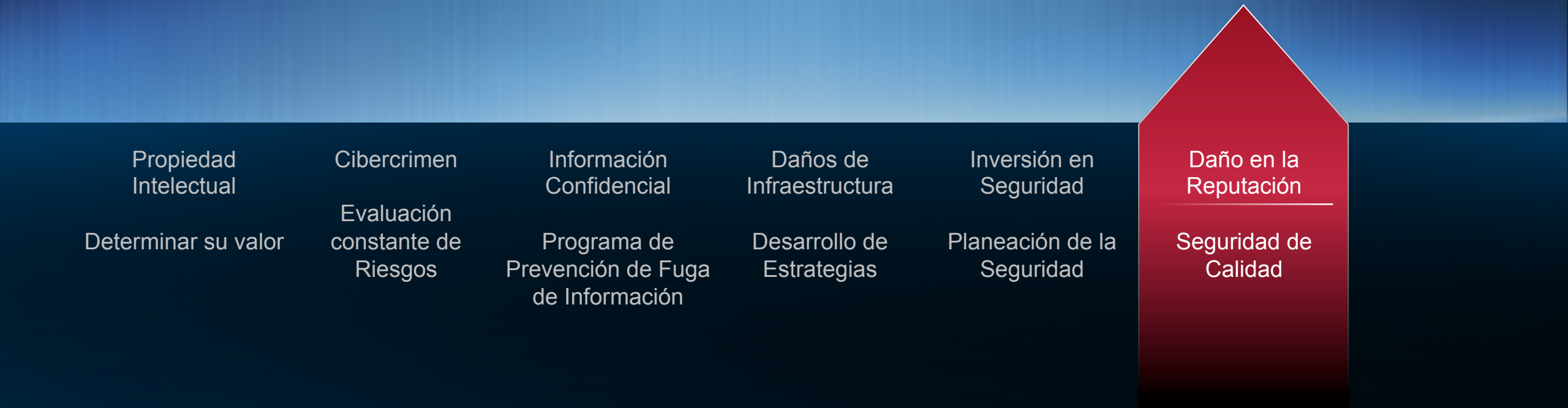
- Inversiones no presupuestadas
- Costos asociados a sanitización posterior al ataque
- Pago de pólizas por incumplimiento
- Re asignación de presupuestos



Contexto de la Ciberseguridad *(cont.)*

Daño de la reputación para la organización victima del ciberataque

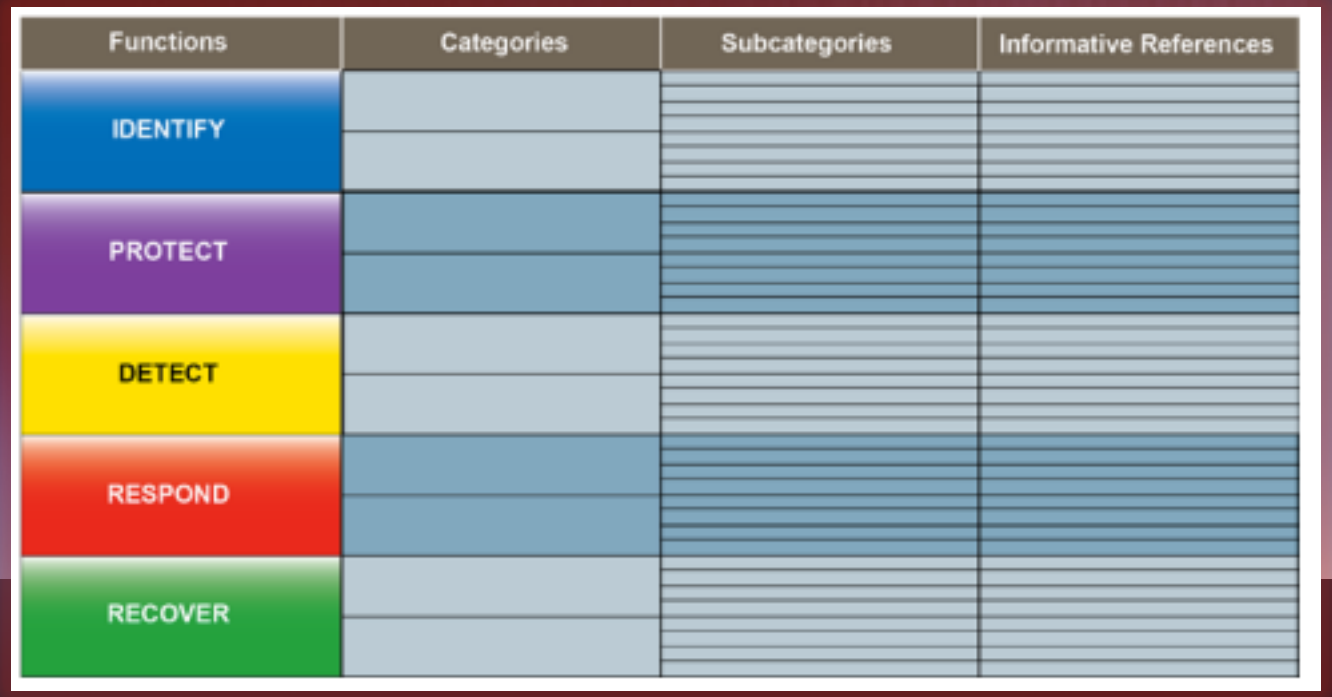
- Temor ante la perdida de reputación
- Caída de las acciones
- Incumplimiento ante terceros
- Daño de imagen



Marcos de referencia de Ciberseguridad a nivel internacional

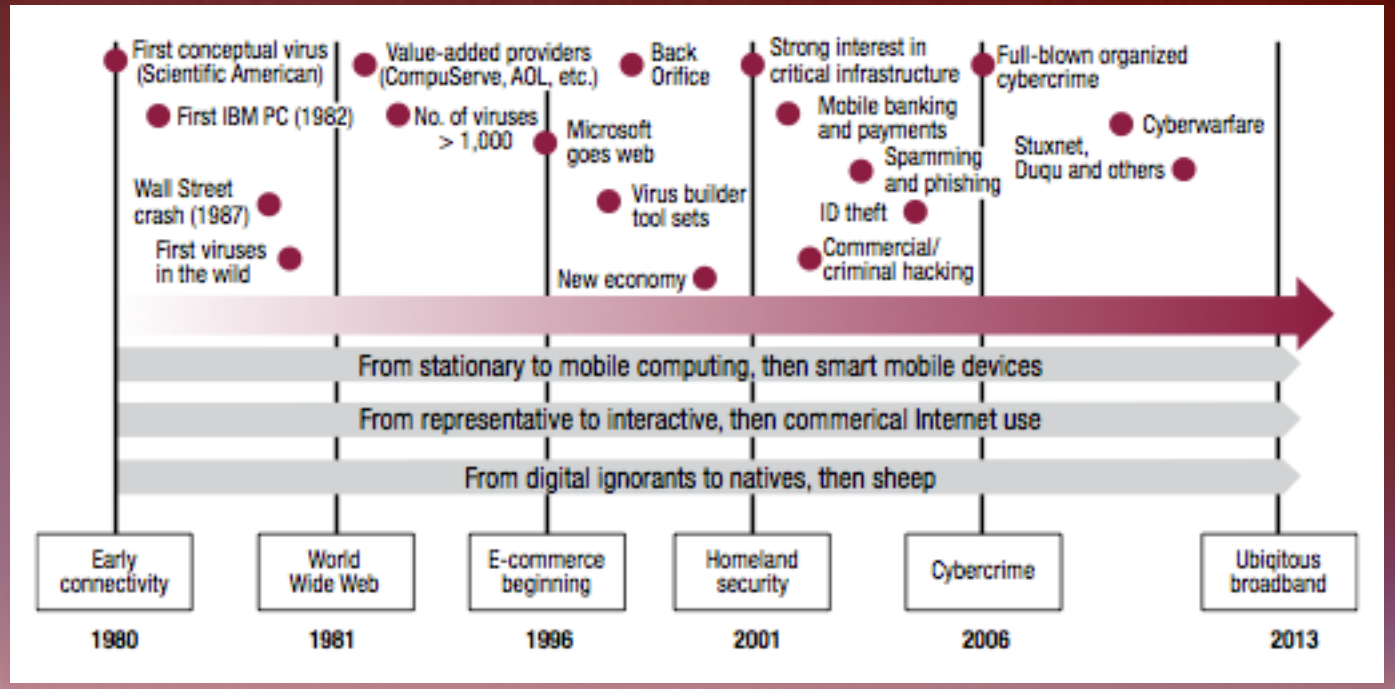
McAfee
An Intel Company

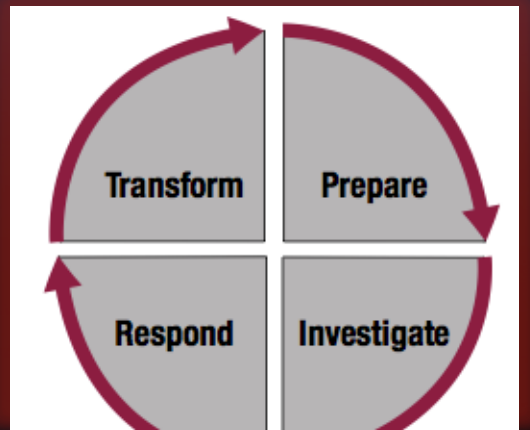
Estado Actual *"Tendencia Internacional" sobre modelos #1 – NIST Cybersecurity Framework*



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Estado Actual *"Tendencia Internacional" sobre modelos*
#2 – Transforming Cybersecurity using COBIT5





Estado Actual *"Tendencia Internacional" sobre modelos #3 – Council on CyberSecurity*

The Critical Security Controls

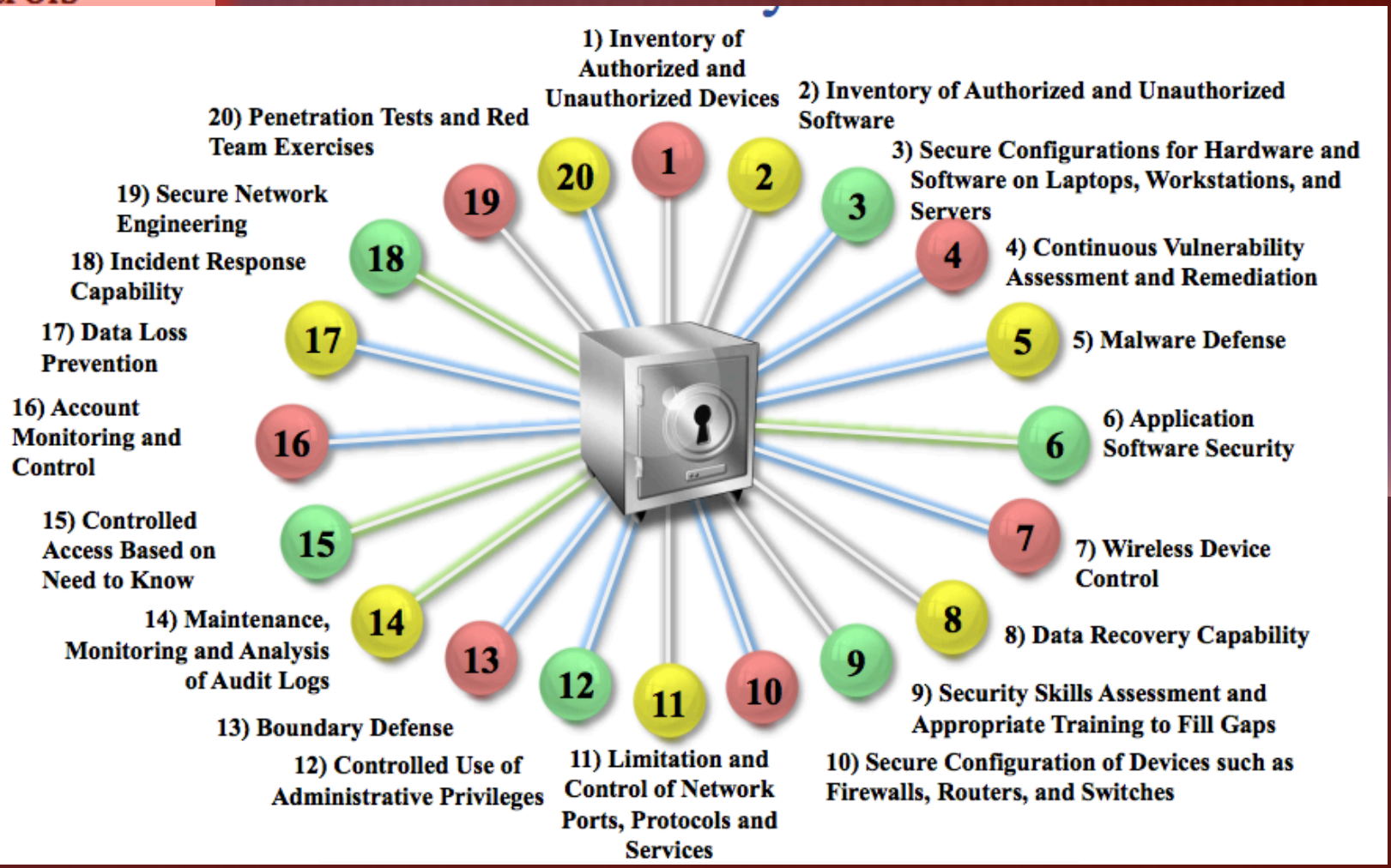
for

Effective Cyber Defen

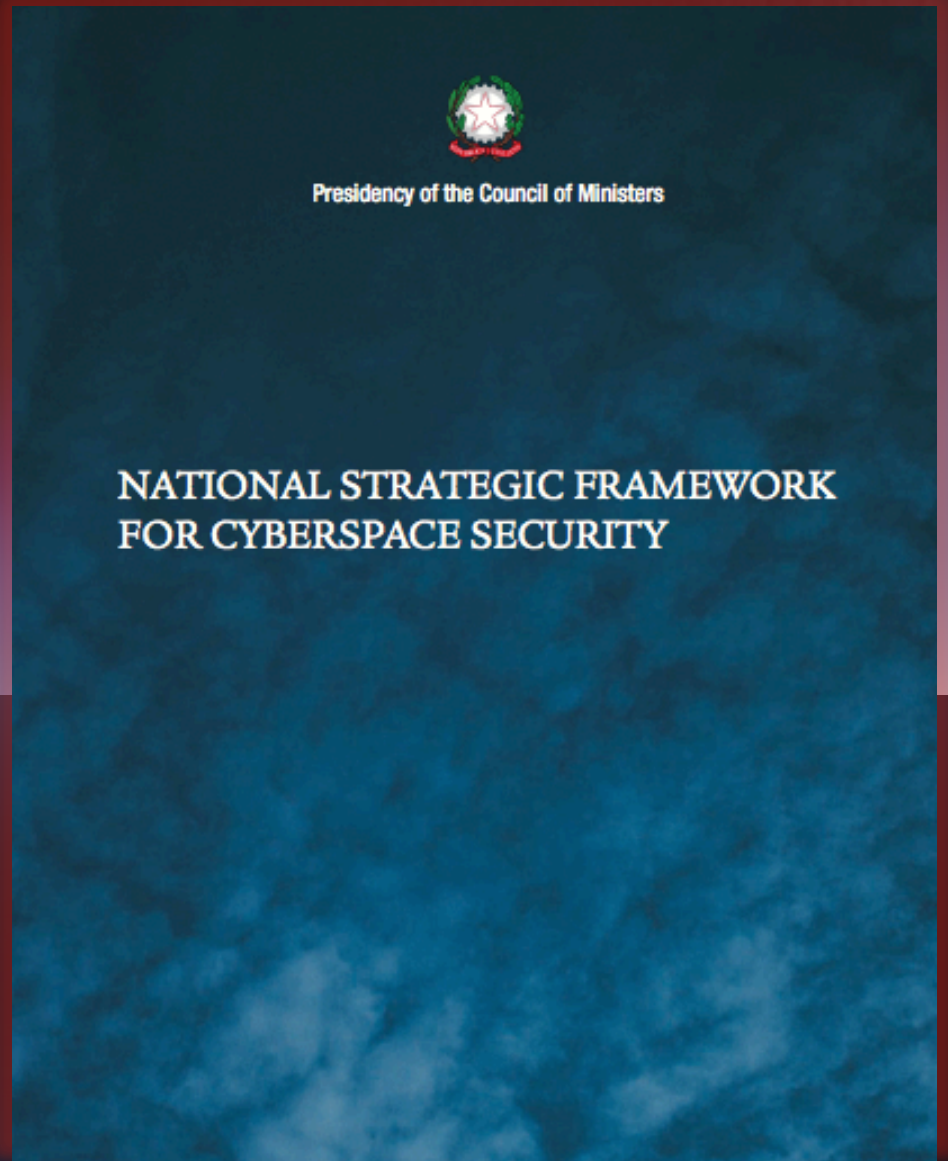
Version 5.0

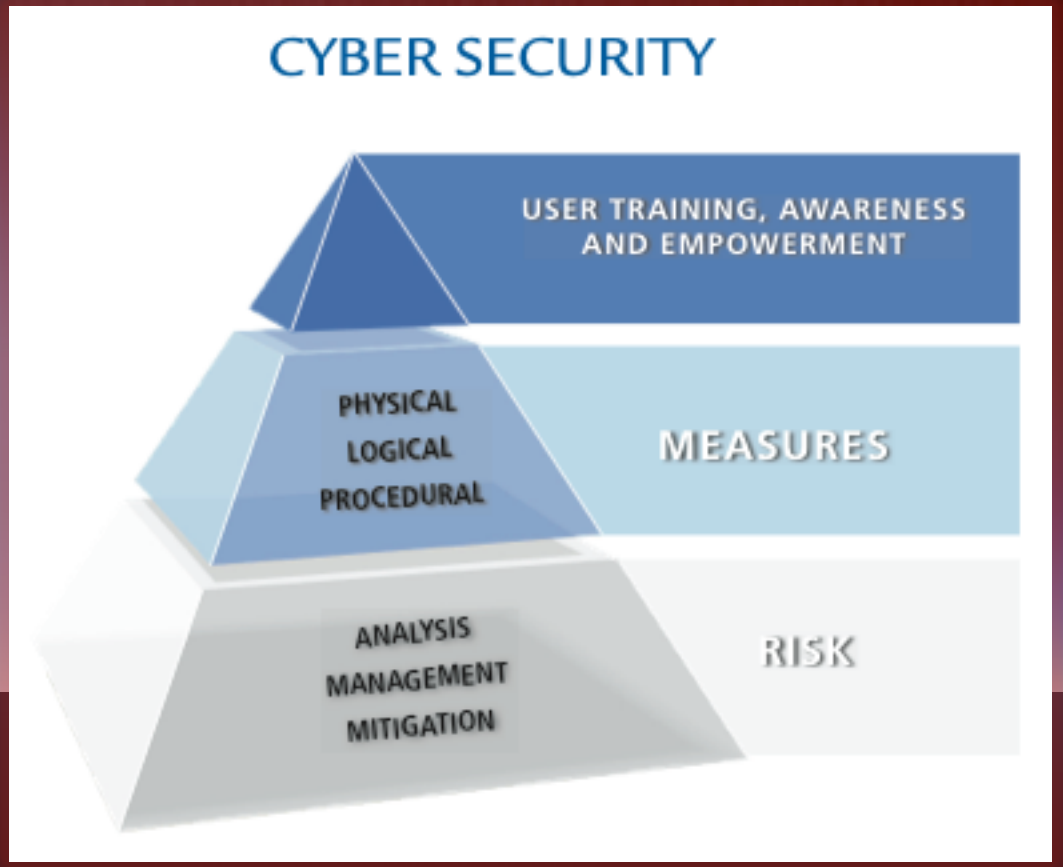
COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

1



Estado Actual *"Tendencia Internacional" sobre modelos*
#4 – National Strategic Framework (Italia)

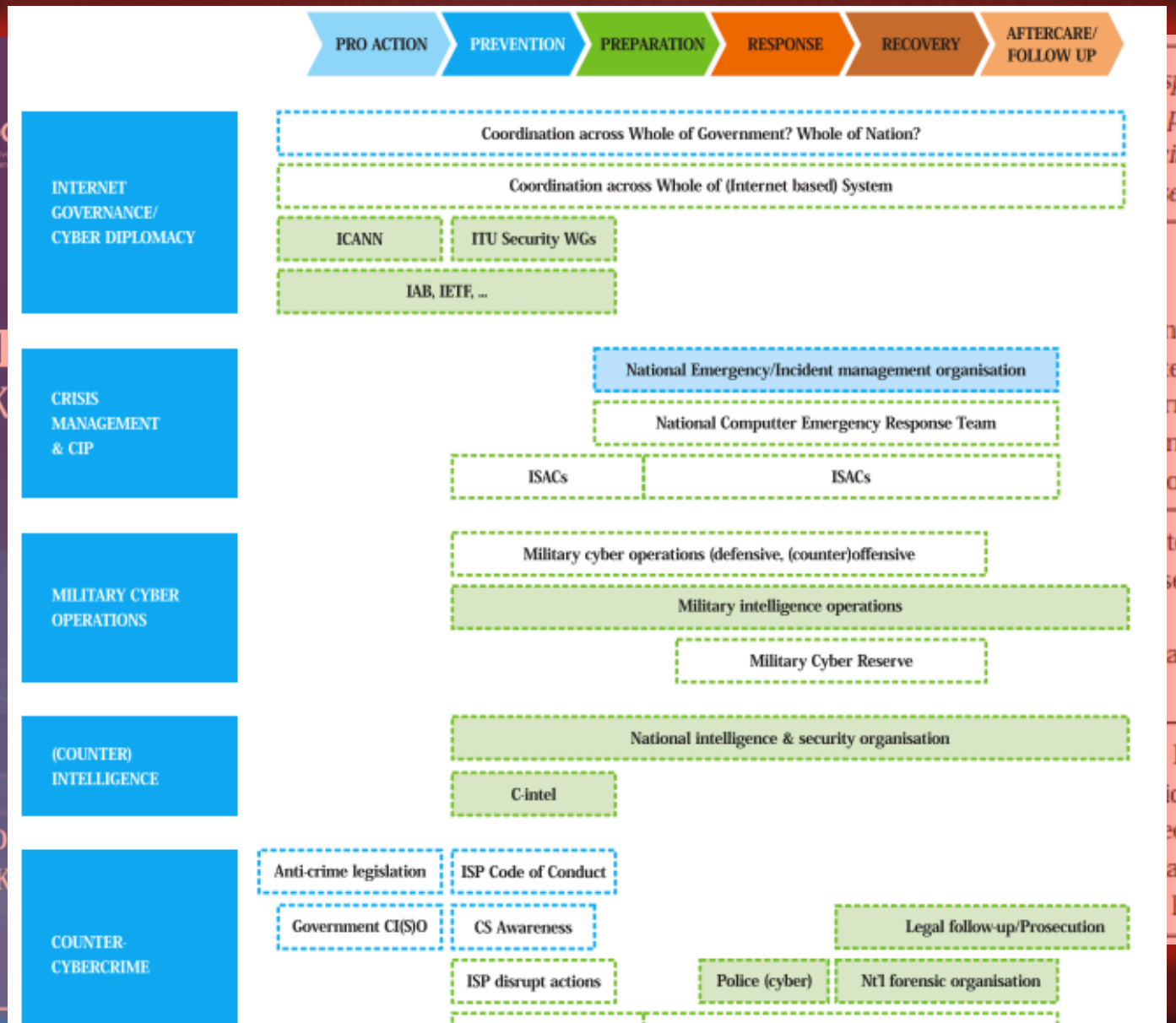




Estado Actual *"Tendencia Internacional" sobre modelos*
#5 – National Cyber Security Framework (Estonia)

NATIONAL CYB
FRAMEWORK

EDITED
ALEXANDER K



specific governmental levers and informa-
public, private and relevant international
iated content, where these systems
ecurity.'

ntelligence
ection and National Crisis Management
rnet Governance
nation, information exchange and data
opment and education

te, local) – 'coordination'
security companies, civil society) – 'co-

al and industry frameworks) – 'collabora-

Improve National Security
ion vs. Critical Infrastructure Protection
ector
ation Sharing
Political Stability

Estado Actual *"Tendencia Internacional" sobre modelos #6 – Seguranca Cibernética no Brasil (2010)*

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Secretaria Executiva
Departamento de Segurança da Informação e Comunicações

LIVRO VERDE
SEGURANÇA CIBERNÉTICA NO BRASIL

Raphael Mandarino Junior e Claudia Canongia
(Organizadores)

SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS

OPORTUNIDADES

- ✓ No Brasil, a criação do Plano Nacional de Segurança das Infraestruturas Críticas (PNSIEC) prevê o estabelecimento de um processo integrado, por meio da criação de cultura de segurança e proteção, em todas as esferas de poder, de recursos humanos qualificados, equipamentos, instalações, conhecimentos, serviços, rotinas, dados, informações e processos estratégicos, e busca estender o esforço das iniciativas ao setor privado;
- ✓ Os Grupos Técnicos de Segurança das Infraestruturas Críticas

DESAFIOS

- ✓ Falta de clareza e de identificação das interdependências nas infraestruturas críticas e entre infraestruturas críticas, e seus respectivos graus de criticidade e impactos;
- ✓ Ausência de integração das várias políticas setoriais, iniciativas e investimentos de segurança das infraestruturas críticas;
- ✓ Movimentos tardios de definição de prioridades estratégicas da Nação e harmonização das estratégias, com foco na prevenção;
- ✓ Limitado leque das infraestruturas críticas nacionais já priorizadas;
- ✓ Crescentes riscos de ataques cibernéticos a Sistemas SCADA[14];
- ✓ Insuficiente número de equipes de resposta e tratamento de incidentes em rede computacionais nos vários segmentos da sociedade, bem como insuficiente número de especialistas com competência para desempenhar tais atividades.

Estado Actual *"Tendencia Internacional" sobre modelos*

Richard Clarke (former spook and cybersecurity advisor to presidents, author of "Cyberwar: The Next Threat to National Security and What To Do About It").

International Civil Aviation Organization

AN-Conf/12-WP/122
9/10/12
English only

AIAA

The Connectivity Challenge: Protecting Critical Assets in a

A **DRAFT Outline - Preliminary Framework to Reduce Cyber Risks to Critical Infrastructure, July 1, 2013**

htt
AN

NOTES TO REVIEWERS:
This draft is produced for discussion purposes at the upcoming workshops and to further encourage private sector input before NIST publishes a preliminary Draft *Framework to Reduce Cyber Risks to Critical Infrastructure*, ("the Framework") for public comment in October.

http://www.nist.gov/itl/cyberframework.cfm

Algunas estrategias a considerar: Colombia

Documento

Conpes

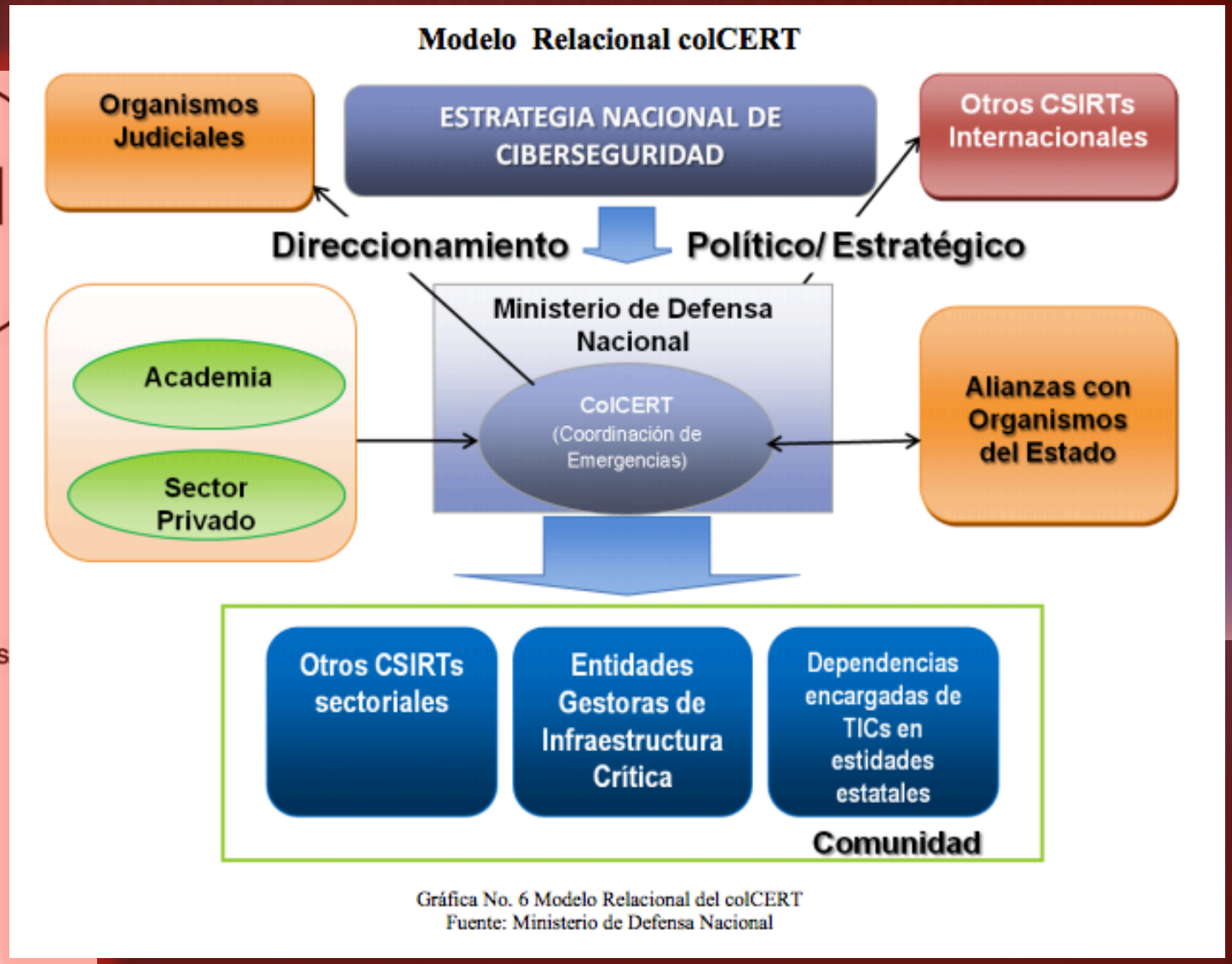
3701

Consejo Nacional de Política Económica y Social
República de Colombia
Departamento Nacional de Planeación

LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENS

Ministerio de Interior y de Justicia
Ministerio de Relaciones Exteriores
Ministerio de Defensa Nacional
Ministerio de Tecnologías de la Información y las Comunicaciones
Departamento Administrativo de Seguridad
Departamento Nacional de Planeación-DJSG-DIFP-DIES-OI
Fiscalía General

Versión aprobada



Gráfica No. 6 Modelo Relacional del colCERT
Fuente: Ministerio de Defensa Nacional

Algunas estrategias considerar: España

EL PAÍS

PORTADA | INTERNACIONAL | POLÍ

MONCLOA | FERRAZ | GÉNOVA | + PARTIDOS | CONGRESO | OPINIÓN | SUCESOS

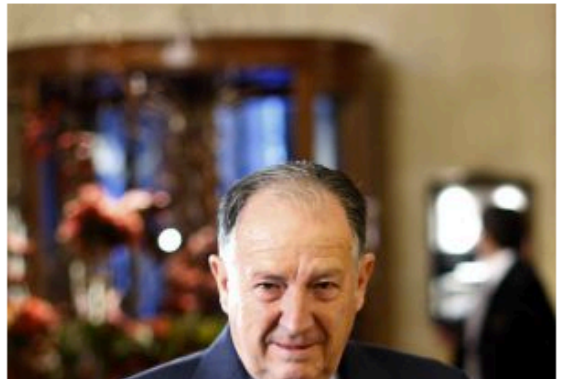
ESTÁ PASANDO: Aniversario 11-M | Congreso del PP vasco | Inmigración irregular | Con

El Gobierno constituye el Consejo de Ciberseguridad Nacional

- El órgano tiene el objetivo de garantizar el uso seguro de las redes y sistemas de información
- Félix Sanz, director del CNI, será el primer presidente del consejo

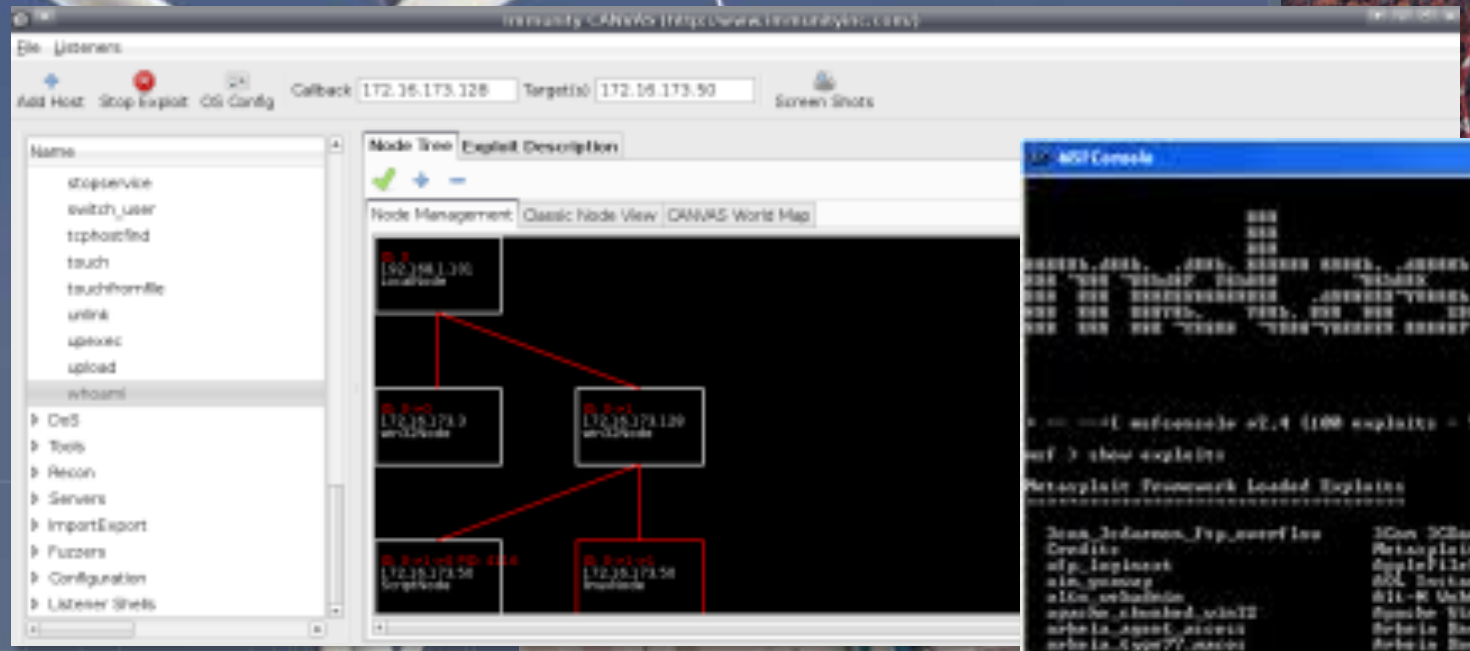
EP | Madrid | 14 FEB 2014 - 09:51 CET 14

Archivado en: Mariano Rajoy | Félix Sanz Roldan | CNI | Ciberespionaje | Gobierno de España | Delitos informáticos | Privacidad internet | Servicios inteligencia | Seguridad nacional | Espionaje

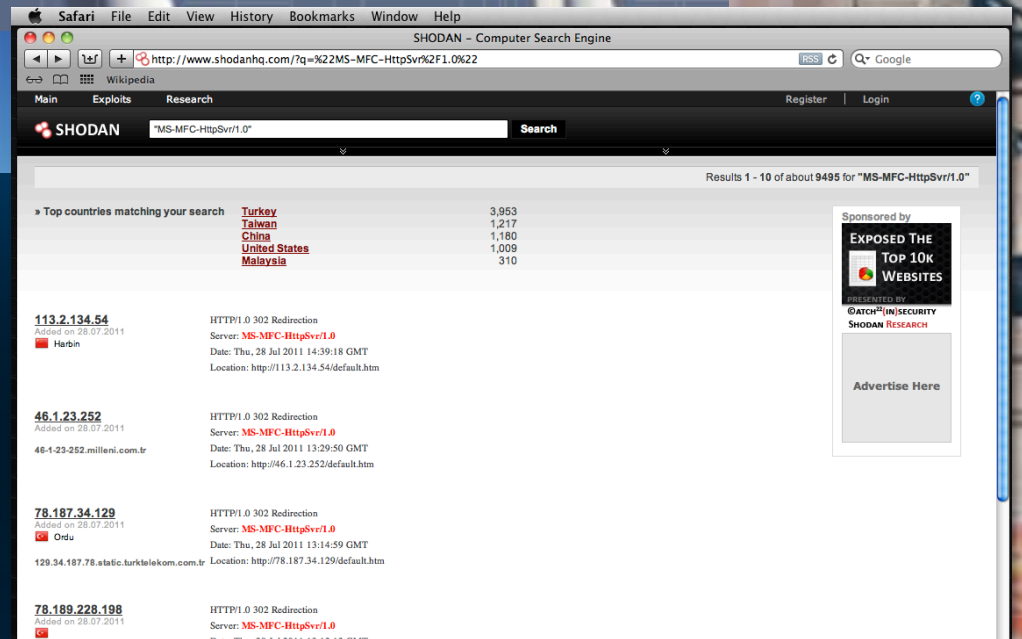


El presidente del Gobierno, Mariano Rajoy, presidirá este viernes la cuarta reunión del Consejo de Seguridad Nacional, que servirá para constituir a su vez el Consejo de Ciberseguridad Nacional, cuyo objetivo es garantizar el uso seguro de las redes y sistemas de información mediante el fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques

Tools


File Listeners
Add Host
Stop Exploit
OS Config
Callback 172.16.173.128
Target(s) 172.16.173.50
Screen Shots
Name
stopservice
switch_user
tcphostfind
touch
touchfromfile
unlink
upexec
upload
whoami
Ctrl
Tools
Recon
Servers
ImportExport
Fuzzers
Configuration
Listener Shells
Node Tree
Exploit Description
Node Management
Classic Node View
CANVAS World Map

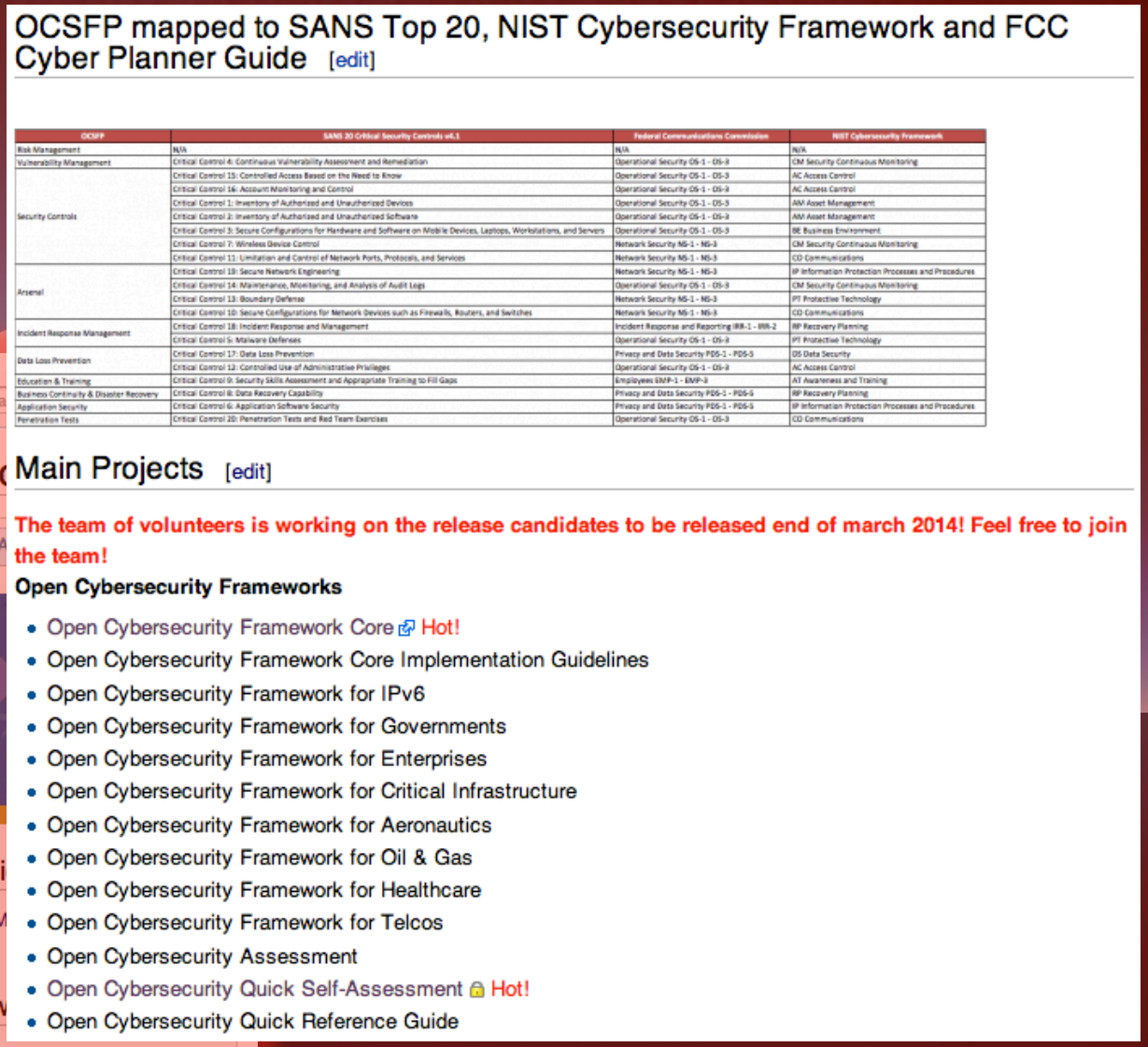

msf > show exploits
Metasploit Framework Loaded Exploits


Safari File Edit View History Bookmarks Window Help
SHODAN - Computer Search Engine
http://www.shodanhq.com/?q=%22MS-MFC-HttpSvr%2F1.0%22
Wikipedia
Main Exploits Research
Register Login
SHODAN
"MS-MFC-HttpSvr/1.0"
Search
Results 1 - 10 of about 9495 for "MS-MFC-HttpSvr/1.0"
» Top countries matching your search
Turkey 3,953
Taiwan 1,217
China 1,180
United States 1,009
Malaysia 310
113.2.134.54
Added on 28.07.2011
Harbin
HTTP/1.0 302 Redirection
Server: MS-MFC-HttpSvr/1.0
Date: Thu, 28 Jul 2011 14:39:18 GMT
Location: http://113.2.134.54/default.htm
46.1.23.252
Added on 28.07.2011
46-1-23-252.milleni.com.tr
HTTP/1.0 302 Redirection
Server: MS-MFC-HttpSvr/1.0
Date: Thu, 28 Jul 2011 13:29:50 GMT
Location: http://46.1.23.252/default.htm
78.187.34.129
Added on 28.07.2011
Ordu
129.34.187.78.static.turktelekom.com.tr
HTTP/1.0 302 Redirection
Server: MS-MFC-HttpSvr/1.0
Date: Thu, 28 Jul 2011 13:14:59 GMT
Location: http://78.187.34.129/default.htm
78.189.228.198
Added on 28.07.2011
HTTP/1.0 302 Redirection
Server: MS-MFC-HttpSvr/1.0
Sponsored by
Exposed The Top 10k Websites
Advertise Here

Un marco de referencia abierto de ciberseguridad

McAfee
An Intel Company

Open Cyber Security Framework Project (www.ocsfp.org)



OCSFP mapped to SANS Top 20, NIST Cybersecurity Framework and FCC Cyber Planner Guide [edit]

OCSFP	SANS 20 Critical Security Controls v4.1	Federal Communications Commission	NIST Cybersecurity Framework
Risk Management	N/A	N/A	N/A
Vulnerability Management	Critical Control 4: Continuous Vulnerability Assessment and Remediation	Operational Security OS-1 - OS-3	CM Security Continuous Monitoring
Security Controls	Critical Control 15: Controlled Access Based on the Need to Know	Operational Security OS-1 - OS-3	AC Access Control
	Critical Control 16: Account Monitoring and Control	Operational Security OS-1 - OS-3	AC Access Control
	Critical Control 1: Inventory of Authorized and Unauthorized Devices	Operational Security OS-1 - OS-3	AM Asset Management
	Critical Control 2: Inventory of Authorized and Unauthorized Software	Operational Security OS-1 - OS-3	AM Asset Management
	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Operational Security OS-1 - OS-3	BE Business Environment
	Critical Control 7: Wireless Device Control	Network Security NS-1 - NS-3	CM Security Continuous Monitoring
	Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	Network Security NS-1 - NS-3	CO Communications
Arsenal	Critical Control 19: Secure Network Engineering	Network Security NS-1 - NS-3	IP Information Protection Processes and Procedures
	Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	Operational Security OS-1 - OS-3	CM Security Continuous Monitoring
	Critical Control 13: Boundary Defense	Network Security NS-1 - NS-3	PT Protective Technology
	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Network Security NS-1 - NS-3	CO Communications
Incident Response Management	Critical Control 18: Incident Response and Management	Incident Response and Reporting IRR-1 - IRR-2	RP Recovery Planning
	Critical Control 5: Malware Defenses	Operational Security OS-1 - OS-3	PT Protective Technology
Data Loss Prevention	Critical Control 17: Data Loss Prevention	Privacy and Data Security PDS-1 - PDS-5	DS Data Security
	Critical Control 12: Controlled Use of Administrative Privileges	Operational Security OS-1 - OS-3	AC Access Control
Education & Training	Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	Employees EMP-1 - EMP-3	AT Awareness and Training
Business Continuity & Disaster Recovery	Critical Control 8: Data Recovery Capability	Privacy and Data Security PDS-1 - PDS-5	RP Recovery Planning
Application Security	Critical Control 6: Application Software Security	Privacy and Data Security PDS-1 - PDS-5	IP Information Protection Processes and Procedures
Penetration Tests	Critical Control 20: Penetration Tests and Red Team Exercises	Operational Security OS-1 - OS-3	CO Communications

Main Projects [edit]

The team of volunteers is working on the release candidates to be released end of march 2014! Feel free to join the team!

Open Cybersecurity Frameworks

- Open Cybersecurity Framework Core Hot!
- Open Cybersecurity Framework Core Implementation Guidelines
- Open Cybersecurity Framework for IPv6
- Open Cybersecurity Framework for Governments
- Open Cybersecurity Framework for Enterprises
- Open Cybersecurity Framework for Critical Infrastructure
- Open Cybersecurity Framework for Aeronautics
- Open Cybersecurity Framework for Oil & Gas
- Open Cybersecurity Framework for Healthcare
- Open Cybersecurity Framework for Telcos
- Open Cybersecurity Assessment
- Open Cybersecurity Quick Self-Assessment Hot!
- Open Cybersecurity Quick Reference Guide

Open Cyber Security Framework Project (www.ocsfp.org)

- **Open Cybersecurity Framework Core**
- Open Cybersecurity Framework Core Implementation
- Open Cybersecurity Framework for IPv6
- Open Cybersecurity Framework for Governments
- Open Cybersecurity Framework for Enterprises
- Open Cybersecurity Framework for Critical Infrastructure
- Open Cybersecurity Framework for Aeronautics
- Open Cybersecurity Framework for Oil & Gas
- Open Cybersecurity Framework for Healthcare
- Open Cybersecurity Framework for Telcos
- Open Cybersecurity Framework for Military
- Open Cybersecurity Assessment
- Open Cybersecurity Quick Self-Assessment

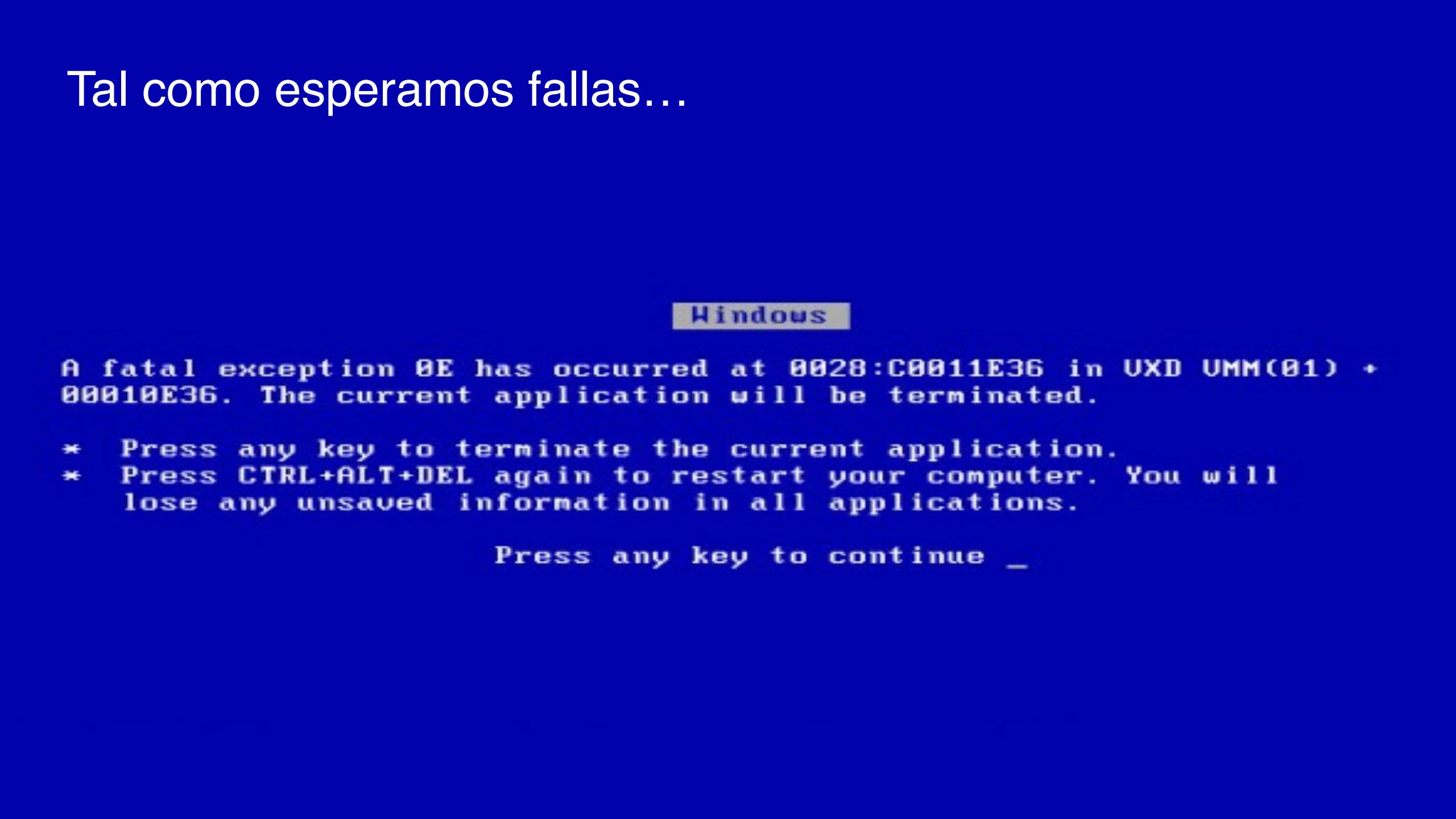
Open Cyber Security Framework Project (www.ocsfp.org)

1. Security Strategy Roadmap
2. Gestión de Riesgos
3. Gestión de Vulnerabilidades
4. Controles de Seguridad
5. Arsenal / Armamento / Herramientas
6. Respuesta ante Incidentes
7. Prevención de Fuga de Datos
8. Educación y Entrenamientos
9. BCP y DRP
10. Seguridad en el Desarrollo de Software
11. Pruebas de Seguridad

Hay que recordar que los adversarios…

- x Transforman nuestros bugs en exploits
- x Se adaptan a nuestras defensas
- x Esperan a que se cometa un error
- x Atacan tecnología y personas

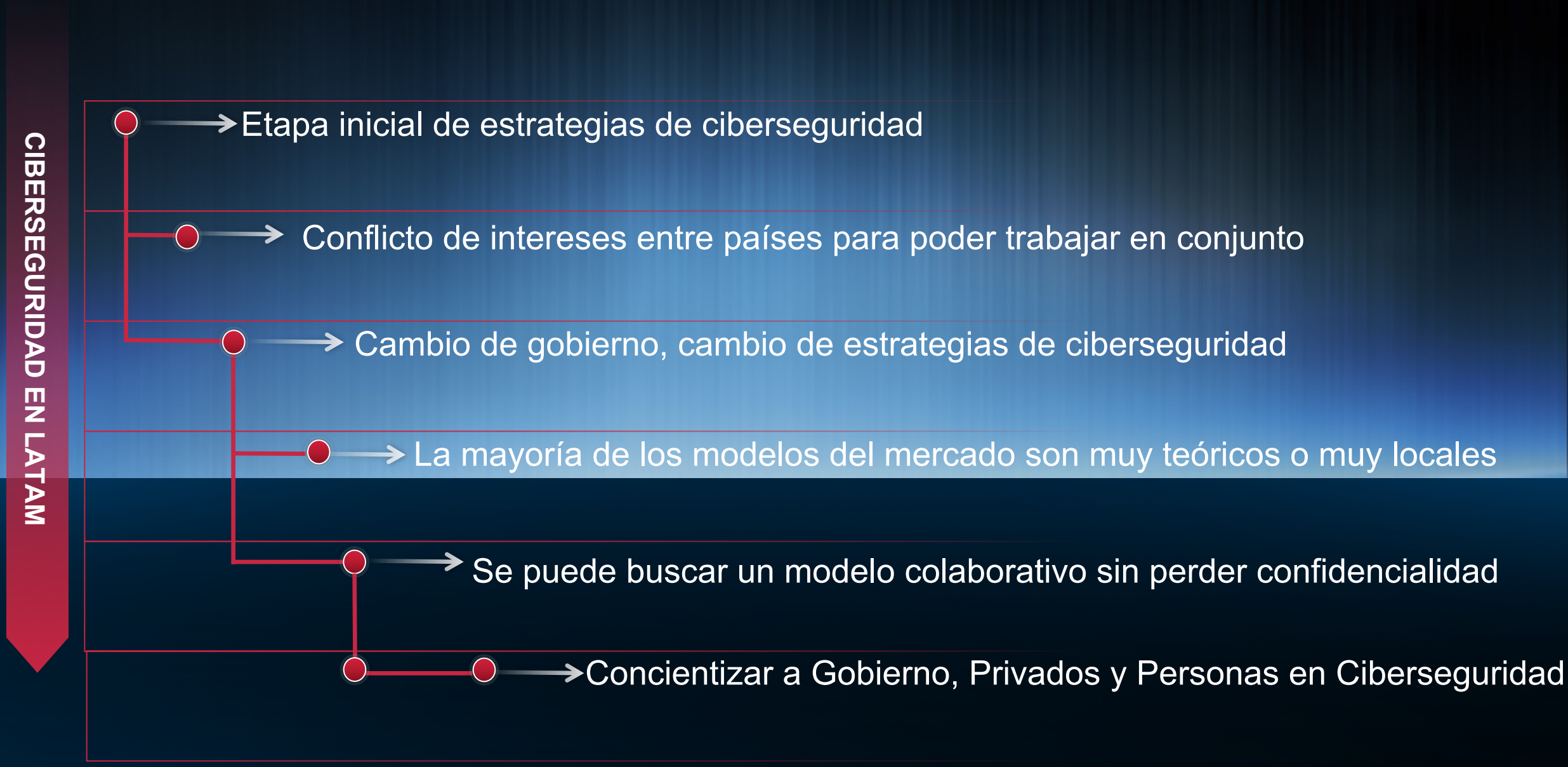
Tal como esperamos fallas…



Puntos clave para la estrategia

- Desarrollar un Marco de Ciberseguridad práctico y aplicable
- Entrenar equipos en Respuesta ante Incidentes
- Desarrollar entrenamientos y políticas para el Desarrollo de código seguro
- Entrenar equipos en técnicas de Hacking
- Desarrollar un plan de Gestión de Vulnerabilidades
- Desarrollar un plan de protección de datos

Conclusiones



Un modelo abierto de Ciberseguridad ¿Puede ayudar en Latinoamérica?

Mateo Martínez, CISSP, QSA
Foundstone Professional Services Consultant
mateo_martinez@mcafee.com