Ciberseguridad empresarial:
De las prácticas de aseguramiento a las capacidades de defensa

Jeimy J. Cano M., Ph.D, CFE
GECTI – Facultad de Derecho
Universidad de los Andes
COLOMBIA

ACFCS | ASOCIACIÓN DE ESPECIALISTAS CERTIFICADOS EN DELITOS FINANCIEROS

FORO INTERNACIONAL SOBRE DELITOS FINANCIEROS
DE LA PONTIFICIA UNIVERSIDAD JAVERIANA Y ACFCS
BOGOTÁ, COLOMBIA | 19 - 20 DE ABRIL DE 2017

Pontificia Universidad JAVERIANA Bogotá

Introducción

- Introducción
- Fundamentos conceptuales: ciberseguridad empresarial
- Transformación de prácticas de protección de la información
- Capacidades organizaciones: ecosistemas digitales
- De las prácticas a las capacidades
- Referencias

Introducción

Introducción

The Political Issues Board Directors Care About, by Industry

PERCENTAGE OF DIRECTORS WHO SAY THE ISSUE IS IMPORTANT	Consumer discretionary	Consumer staples	Energy/ Utilities	Financial & professional services	Health care	IT/Telecom	Industrials	Materials
The economy	76%	75%	62%	73%	52%	61%	67%	71%
Regulatory environment	51	58	69	73	64	50	55	59
Cybersecurity	43	45	28	48	31	57	35	25
Corporate tax rates	25	21	17	17	24	32	28	25
Political instability	16	17	17	17	17	14	21	24
Health care costs	15	19	9	12	51	17	9	8
Environmental sustainability	12	17	29	8	9	7	17	27
Education	11	7	4	9	10	14	8	7
Energy costs	6	6	29	3	3	3	11	18
National budget deficits	4	6	5	8	11	10	11	6
Unemployment	8	4	2	7	1	5	6	3
Equal rights for women	8	4	2	6	3	4	6	3
Foreign policy	4	4	2	2	3	7	3	3
Economic justice	4	2	2	3	4	3	3	3
Immigration policy	3	3	2	2	1	7	3	1
Personal tax rates	6	2	3	2	5	5	1	1
Natl. retirement program costs	2	2	0	5	2	0	3	2
Carbon tax	1	1	14	1	0	2	1	7
Other	6	5	3	4	3	5	8	5
NUMBER POLLED →	251	124	232	572	258	241	262	154

SOURCE BORIS GROYSBERG AND J. YO-JUD CHENG, BASED ON A 2015 SURVEY OF OVER 4,000 GLOBAL BOARD DIRECTORS

© HBR.ORG

Groysberg, B. y Cheng, Y. (2016) The Political Issues Board Directors Care Most About. *Harvard Business Review*. Febrero. Recuperado de: https://hbr.org/2016/02/the-political-issues-board-directors-care-most-about

Introducción

Computación cognitiva

Grandes datos y analítica

Redes sociales

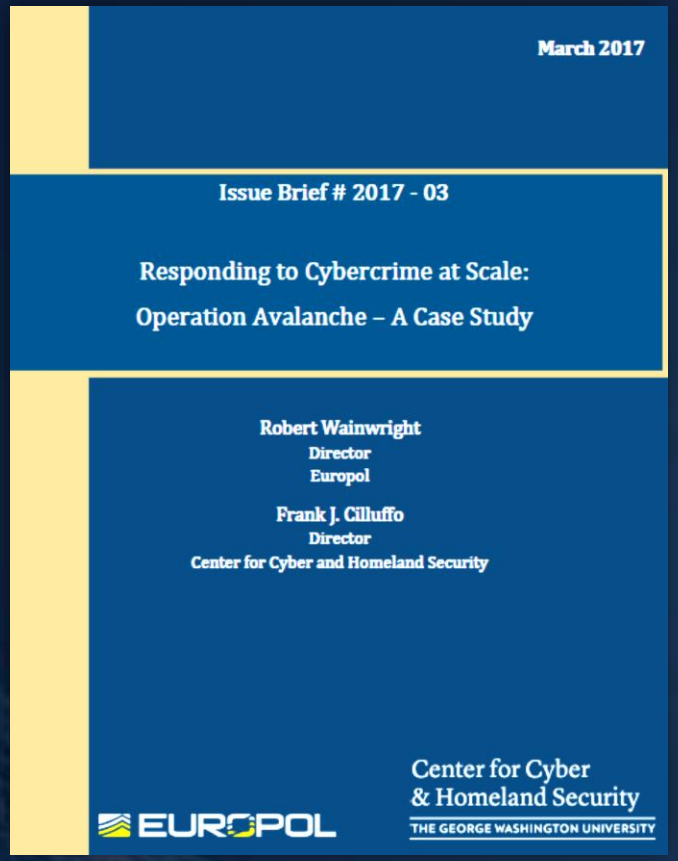
Computación móvil

Computación en la nube

Internet de las cosas

Datos personales y corporativos

Introducción



Tomado de:
https://cchs.gwu.edu/sites/cchs.gwu.edu/files/Responding%20to%20Cybercrime%20at%20Scale%20FINAL.pdf

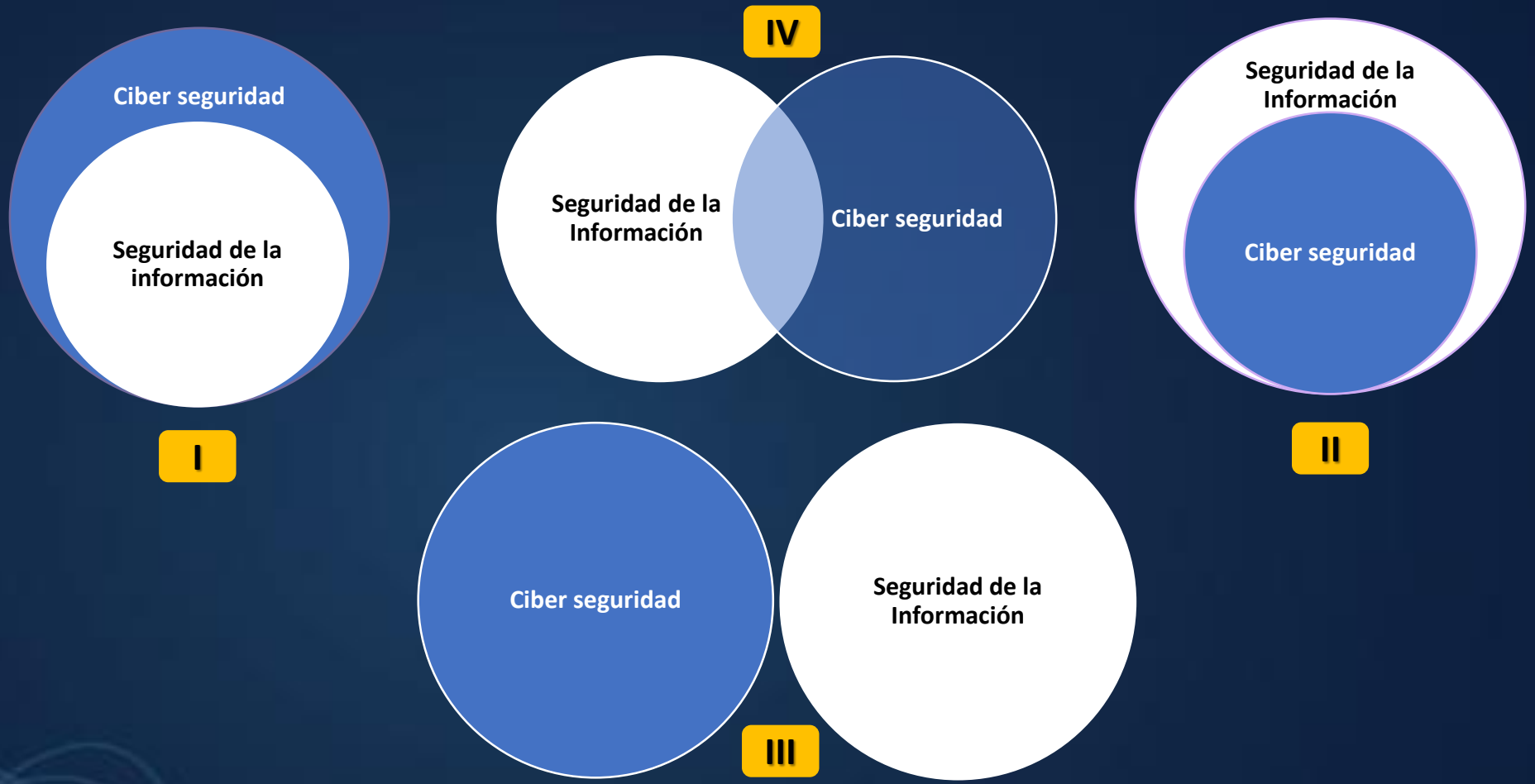
Do it yourself	Malware as a Service	Botnet as a Service	Distribution as a Service	Crime as a Service
Collect and launder money	Collect and launder money	Collect and launder money	Collect and launder money	Collect and launder money
Distribute malware	Distribute malware	Distribute malware	Distribute malware	Distribute malware
Infect target machines	Infect target machines	Infect target machines	Infect target machines	Infect target machines
Develop and test malware	Develop and test malware	Develop and test malware	Develop and test malware	Develop and test malware

Step managed by criminal

Step managed and provided as a service to criminal

Fundamentos conceptuales: ciberseguridad empresarial

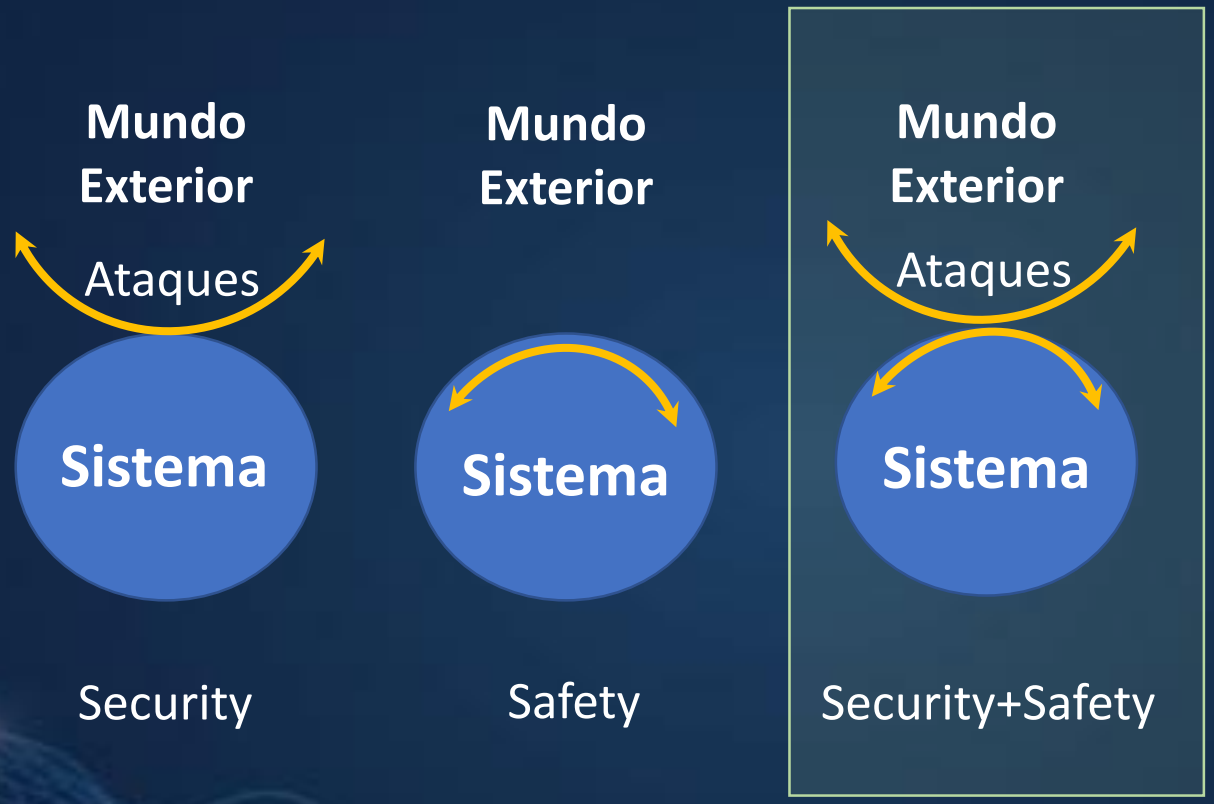
Fundamentos conceptuales: ciberseguridad empresarial



Fundamentos conceptuales: ciberseguridad empresarial

Tomado de: ALXELROD, W.C (2013) *Engineering Safe and Secure Software Systems*. Artech House

Fundamentos conceptuales: ciberseguridad empresarial



Tomado de: ALXELROD, W.C (2013) *Engineering Safe and Secure Software Systems*. Artech House

Ciberseguridad empresarial

Es una capacidad empresarial definida para **defender y anticipar** las amenazas digitales propias del ecosistema donde la organización actúa, con el fin de desarrollar y fortalecer la **resiliencia** de las operaciones y la reputación de la empresa.

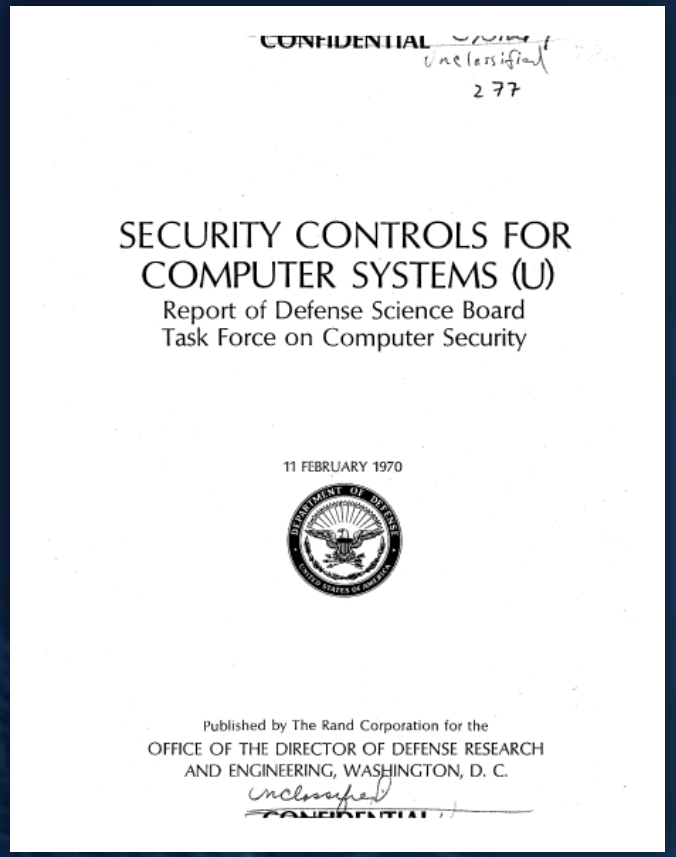
Transformación de prácticas de protección de la información

ACFCS | ASOCIACIÓN DE ESPECIALISTAS CERTIFICADOS EN DELITOS FINANCIEROS

FORO INTERNACIONAL SOBRE DELITOS FINANCIEROS
DE LA PONTIFICIA UNIVERSIDAD JAVERIANA Y ACFCS
BOGOTÁ, COLOMBIA | 19 - 20 DE ABRIL DE 2017

Pontificia Universidad JAVERIANA Bogotá

Vulnerabilidades en redes de computadores



CONFIDENTIAL

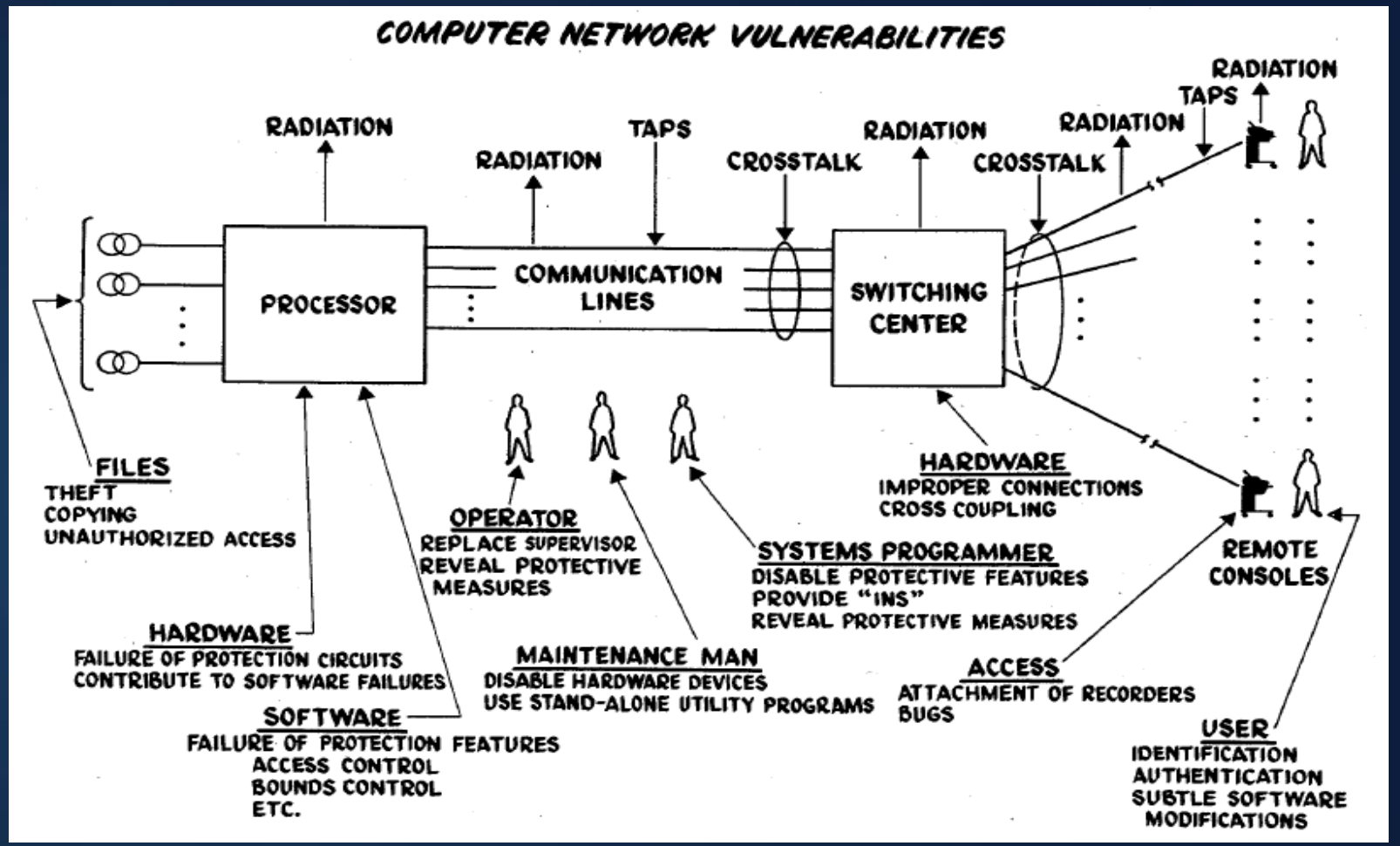
277

SECURITY CONTROLS FOR COMPUTER SYSTEMS (U)

Report of Defense Science Board Task Force on Computer Security

11 FEBRUARY 1970

Published by The Rand Corporation for the OFFICE OF THE DIRECTOR OF DEFENSE RESEARCH AND ENGINEERING, WASHINGTON, D. C.



ACFCS | ASOCIACIÓN DE ESPECIALISTAS CERTIFICADOS EN DELITOS FINANCIEROS

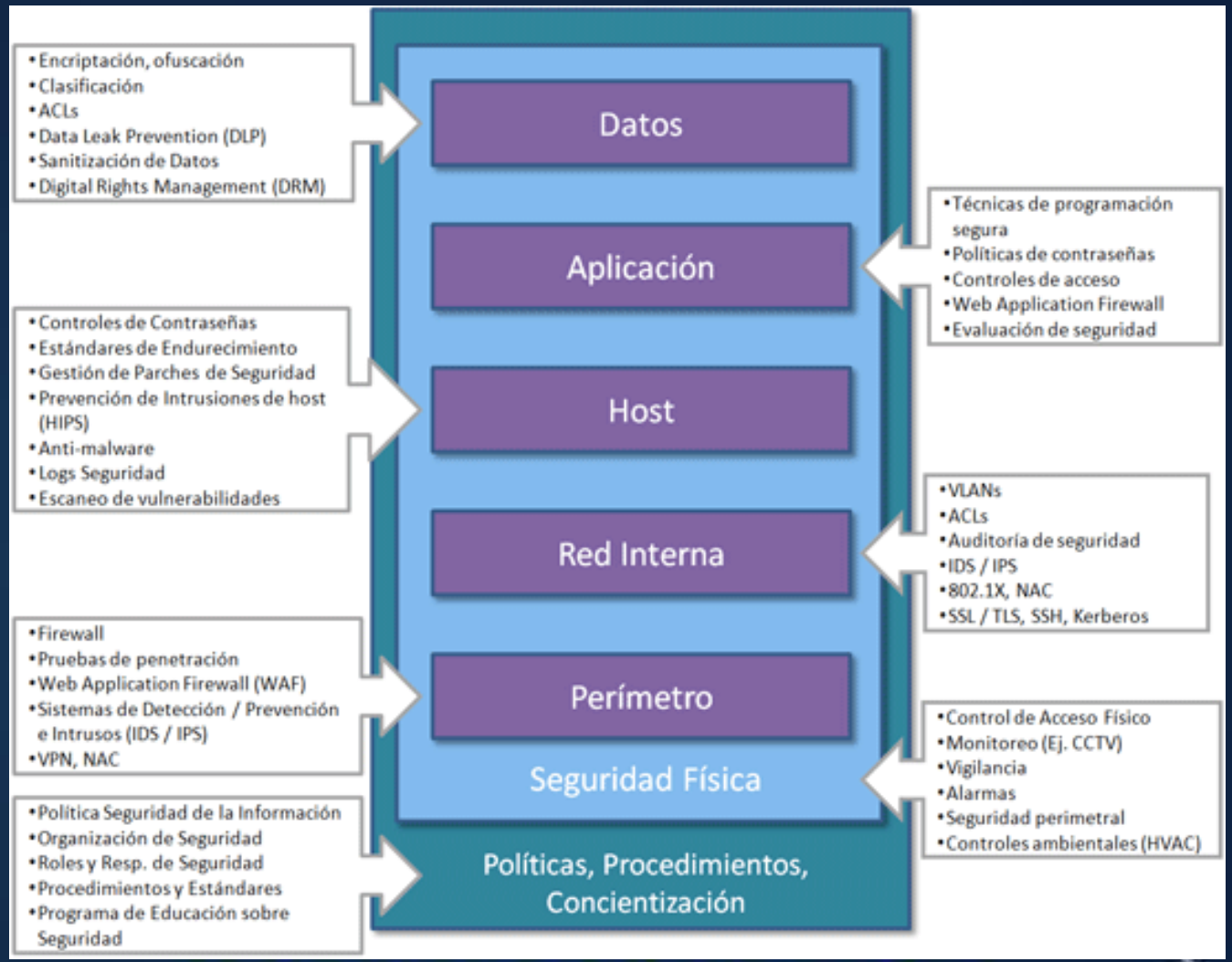
FORO INTERNACIONAL SOBRE DELITOS FINANCIEROS

DE LA PONTIFICIA UNIVERSIDAD JAVERIANA Y ACFCS

BOGOTÁ, COLOMBIA | 19 - 20 DE ABRIL DE 2017

Pontificia Universidad JAVERIANA Bogotá

Defensa en profundidad



Tomado de: http://www.sentineldr.com/post/estrategias-basicas-de-seguridad-informatica-defensa-en-profundidad

Dominios de seguridad de la información

Seguridad Punto final	Seguridad Redes	Seguridad Datos
Seguridad Comunicaciones	Gestión Vulnerabilidades	Seguridad Software
Gestión Controles de TI	Gestión Identidad	Seguridad Móviles

Proteger y asegurar

Prácticas

Capacidades organizaciones: ecosistemas digitales

Valor de los ciberataques

Ideas adaptadas de: Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A. y Rezek, C. (2015) *Beyond cybersecurity. Protecting your digital business*. Hoboken, New Jersey. USA: Wiley.

INFOSEC: De saberes especializados a capacidades colectivas

- Juegos de guerra
- Ejercicios de ingeniería social
- Inteligencia de amenazas
- Análisis de riesgos de INFOSEC
- Auditorías de INFOSEC
- Análisis de vulnerabilidades

ACFCS | ASOCIACIÓN DE ESPECIALISTAS CERTIFICADOS EN DELITOS FINANCIEROS

FORO INTERNACIONAL SOBRE DELITOS FINANCIEROS
DE LA PONTIFICIA UNIVERSIDAD JAVERIANA Y ACFCS
BOGOTÁ, COLOMBIA | 19 - 20 DE ABRIL DE 2017

Pontificia Universidad JAVERIANA Bogotá

Cibersegurdad empresarial: Capacidades claves

1. PERCIBIR O SENSAR

Buscar oportunidades y/o amenazas nuevas o emergentes.

2. CAPTAR

Aprovechar y capturar las oportunidades después de que sean reconocidas.

3. RECONFIGURAR

Transformar, cambiar y modificar los procesos existentes.

4. VISUALIZAR

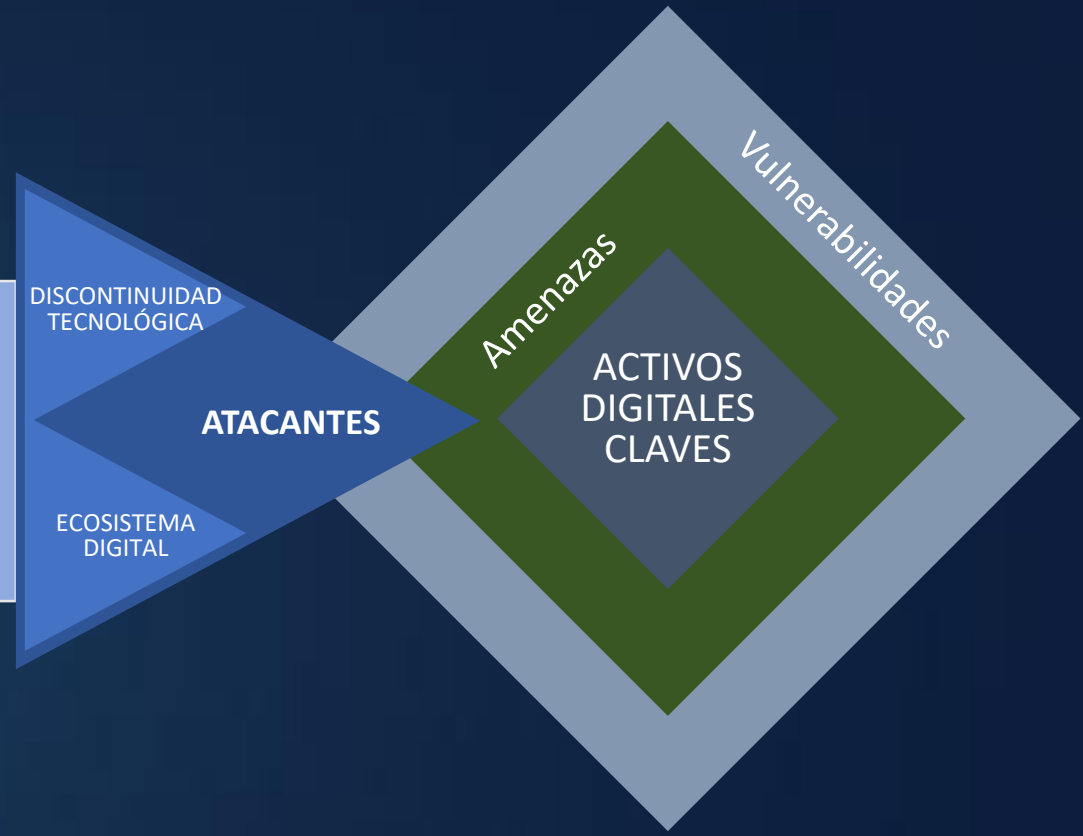
Identificar patrones y tendencias en medio de la incertidumbre estructural vigente.

5. ANTICIPAR

Concretar escenarios posibles y probables.

6. SIMULAR

Experimentar y validar patrones y escenarios para tomar posiciones estratégicamente claves en el entorno.

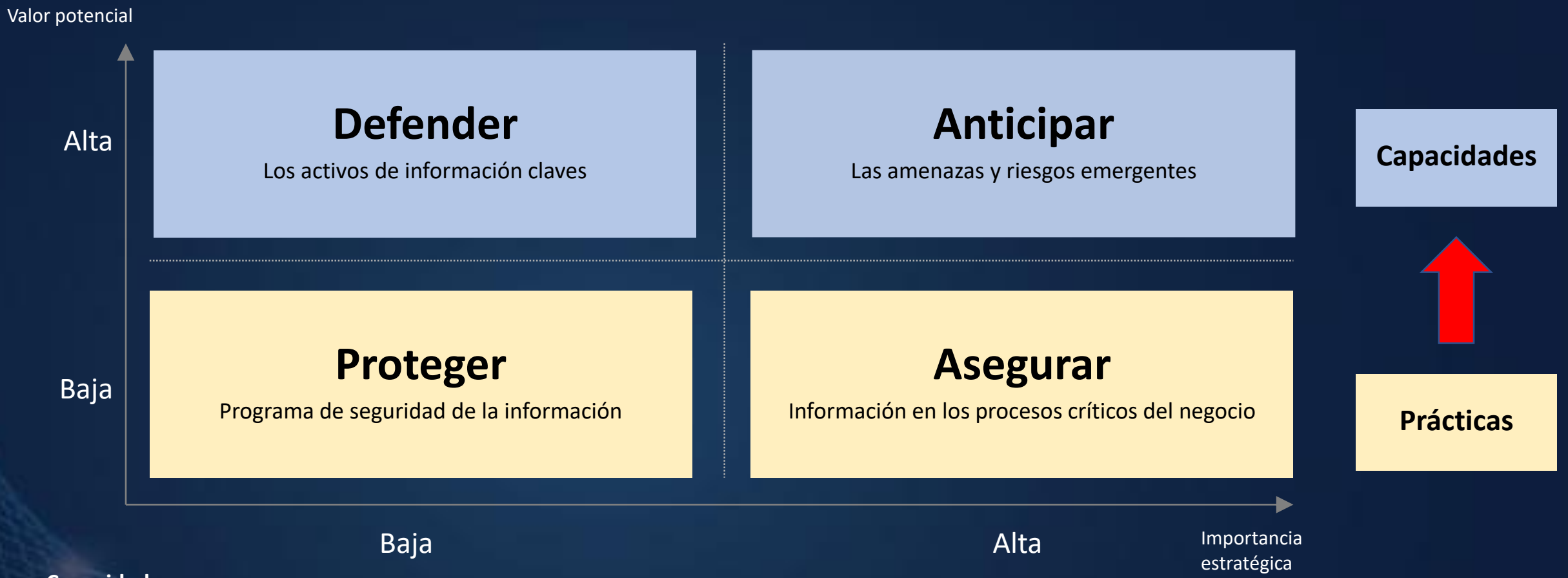


Capacidad:

Un patrón de aprendizaje y desaprendizaje de construcción colectiva a través del cual una organización y sus colaboradores generan, modifican y actualizan sistémica y sistemáticamente sus reflexiones ejecutivas y rutinas operativas para alcanzar una mayor efectividad en sus procesos y un mejor posicionamiento estratégico. Adaptado de: Su, H. y Linderman, K. (2016) An Empirical Investigation in Sustaining High-Quality Performance. *Decision Sciences*. 47, 5. October.

De las prácticas a las capacidades

De las prácticas a las capacidades



Capacidad:

Un patrón de aprendizaje y desaprendizaje de construcción colectiva a través del cual una organización y sus colaboradores generan, modifican y actualizan sistémica y sistemáticamente sus reflexiones ejecutivas y rutinas operativas para alcanzar una mayor efectividad en sus procesos y un mejor posicionamiento estratégico. Adaptado de: Su, H. y Linderman, K. (2016) An Empirical Investigation in Sustaining High-Quality Performance. *Decision Sciences*. 47, 5. October.

De las prácticas a las capacidades

Dominios de seguridad

Seguridad Punto final	Seguridad Redes	Seguridad Datos
Seguridad Comunicaciones	Gestión Vulnerabilidades	Seguridad Software
Gestión Controles de TI	Gestión Identidad	Seguridad Móviles

Proteger y asegurar

Prácticas

Ecosistema de seguridad

Defender y anticipar

Capacidades

Adaptado de: Falco, C. (2016) Unleashing the Immune System: How to Boost Your Security Hygiene. Recuperado de: https://securityintelligence.com/news/unleashing-the-immune-system-how-to-boost-your-security-hygiene/

Conclusiones

Conclusiones

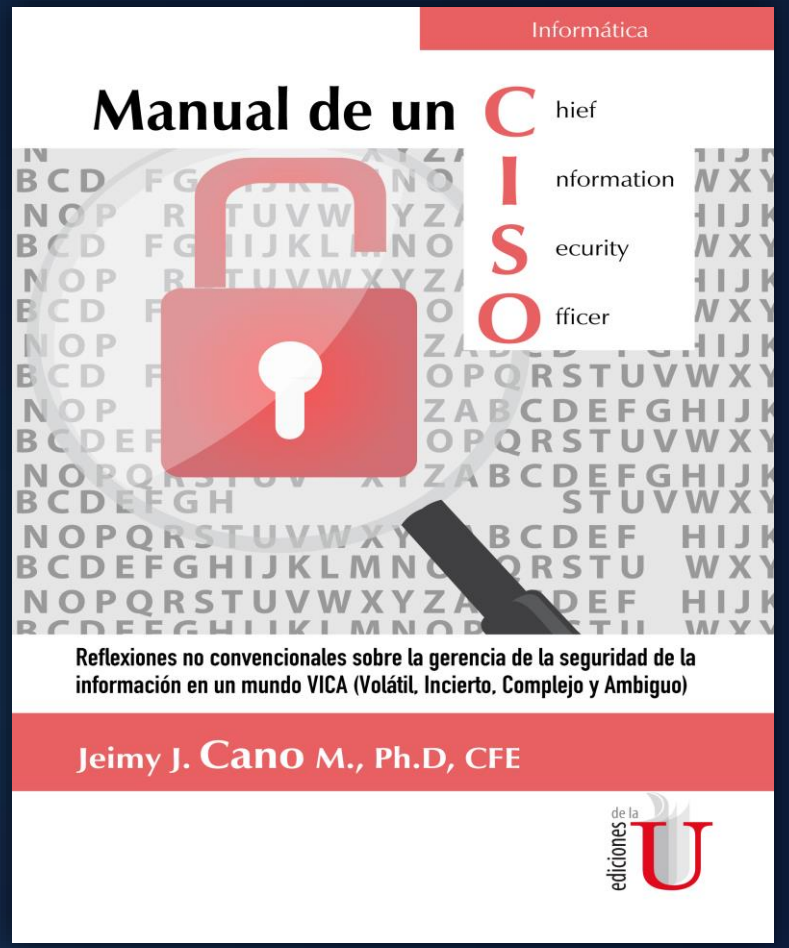
Ciberseguridad empresarial	Perímetros	Se mueven hacia las personas y sus relaciones digitales
	Procesos	De proteger y asegurar a defender y anticipar
	Tecnología	De la protección de la información a la seguridad cognitiva
	Ecosistema digital	Del control de acceso al control de uso: Productos y servicios digitalmente modificados

Para seguir reflexionando …

Referencia académica:

Cano, J. (2016) *Manual de un CISO. Reflexiones no convencionales sobre la gerencia de la seguridad de la información en un mundo VICA (Volátil, Incierto, Complejo y Ambiguo)*. Bogotá, Colombia: Ediciones de la U.

Enlace en la página de la Editorial: (Ebook)
https://edicionesdelau.com/producto/manual-de-un-ciso-2/



Ciberseguridad empresarial:
De las prácticas de aseguramiento a las capacidades de defensa

@itinsecure

Jeimy J. Cano M., Ph.D, CFE
GECTI – Facultad de Derecho
Universidad de los Andes
COLOMBIA

Blog:
http://insecurityit.blogspot.com.co

ACFCS | ASOCIACIÓN DE ESPECIALISTAS CERTIFICADOS EN DELITOS FINANCIEROS

FORO INTERNACIONAL SOBRE DELITOS FINANCIEROS
DE LA PONTIFICIA UNIVERSIDAD JAVERIANA Y ACFCS
BOGOTÁ, COLOMBIA | 19 - 20 DE ABRIL DE 2017

Pontificia Universidad JAVERIANA Bogotá