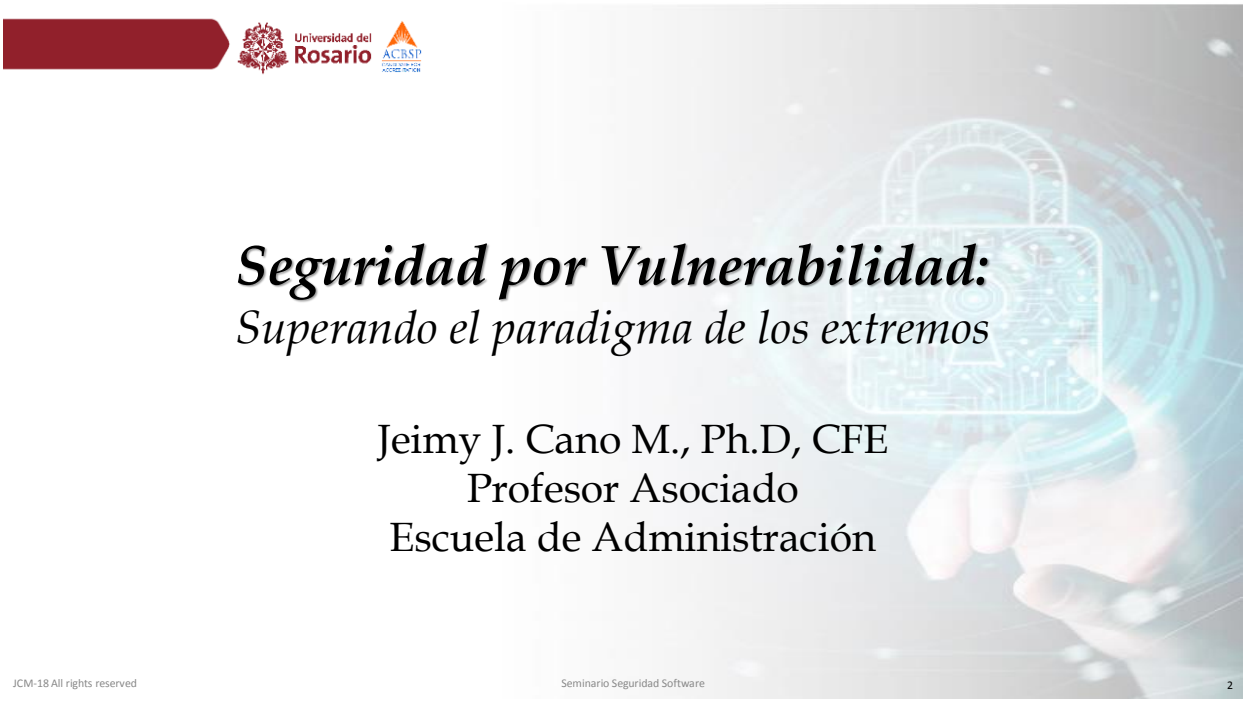

TECNOLÓGICO SUPERIOR CORDILLERA
25 años
CIDE
Centro de Investigación y Desarrollo Ecuador
SEMINARIO INTERNACIONAL DE
SEGURIDAD
EN EL DESARROLLO DE
SOFTWARE
JCM-18 All rights reserved
Seminario Seguridad Software
1


Universidad del Rosario
ACBSP
Seguridad por Vulnerabilidad:
Superando el paradigma de los extremos
Jeimy J. Cano M., Ph.D, CFE
Profesor Asociado
Escuela de Administración
JCM-18 All rights reserved
Seminario Seguridad Software
2

BREVE HOJA DE VIDA

El doctor Cano es Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Administración de Negocio por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás, Colombia. Cuenta con más de 20 años de experiencia como académico y profesional en temas de seguridad de la información, privacidad, ciberseguridad, sistemas de información, gobierno y Auditoría de TI. En 2016 recibió el reconocimiento como "Cybersecurity Educator of the Year 2016" para Latinoamérica por el Cybersecurity Excellence Awards. Es examinador certificado de fraude (CFE en inglés). Cuenta con más de 150 publicaciones en revistas y eventos internacionales, así como conferencista invitado a foros y conferencias nacionales e internacionales en temas de seguridad y control en Latinoamérica. A la fecha es Profesor Asociado de la Escuela de Administración de la Universidad del Rosario en Colombia.

Agenda

- Contexto
- Fundamentos de INFOSEC en las aplicaciones
- Prácticas de seguridad y control en las aplicaciones
- Seguridad por vulnerabilidad: Un ejercicio de confianza imperfecta
- PERIL. Propuesta conceptual y práctica para desarrollo de software confiable
- Evolución de la INFOSEC. De las prácticas a las capacidades
- Tensiones regulatorios
- Riesgos emergentes
- Conclusiones

Contexto

Definiciones de Ciber riesgo

Source	Definition
Mukhopadhyay et al. (2005, 2013)	Risk involved with malicious electronic events that cause disruption of business and monetary loss
Böhme and Kataria (2006)	Breach or failure of information systems
Cebula and Young (2010)	Operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems
Kshetri (2010)	A cybercrime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations.
Øgut et al. (2011)	Information security risk
The UK Cyber Security Strategy (2011)	Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.
World Economic Forum (2012)	"Cyber risks" are defined as the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.
World Economic Forum (2012)	"Cyber" refers to the interdependent network of information technology infrastructures, and includes technology "tools" such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
Hua and Bapna (2013)	Cyber terrorism: Attacks unpleasanted by cyber terrorists via information systems to (1) significantly interfere with the political, social or economic functioning of a critically important group or organization of a nation, or (2) induce physical violence and/or create panic.
National Association of Insurance Commissioners (2013)	Defines cyber by providing typical examples: Identity theft, business interruption, damage to the firm's reputation, disclosure of sensitive information and business interruption
National Institute of Standards and Technology (NIST, 2013)	Defines cyber space as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
Tallinn Manual (Schmitt, 2013)	Cyberspace: The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks.
Willis (2013a)	Cyber risk can be defined as the risk connected to activity online, internet trading, electronic systems and technological networks, as well as storage of personal data
Swiss Re (2014)	Any risk emanating from the use of electronic data and its transmission. This encompasses physical damage caused by cyber-attacks, loss or corruption of data and its financial consequences, fraud committed by misuse of data, as well as any liability arising from a failure to maintain the availability, integrity, and confidentiality of electronically stored information – be it related to individuals, companies, or government. In this context, cyber risk insurance addresses the first and third party risks associated with e-business, the internet, networks and informational assets.
CRO Forum (2014)	Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or government.
Institute of Risk Management (2014)	Any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.
Refsdal, Solhaug, and Stølen (2015)	Definition consisting of three elements: -A cyber-risk is a risk that is caused by a cyber-threat -A cyber-threat is a threat that exploits a cyberspace -Cyberspace is a collection of interconnected computerized networks, including services, computer systems, embedded processors, and controllers, as well as information in storage or transit.
Lloyds (2015)	Losses relating to damage to, or loss of information from, IT systems and networks.
Lloyd's (2015a)	Definition of Cyber-Attack: exposures arising from a malicious electronic act which for the purpose of this bulletin we label as 'cyber-attack'. Cyber-attack is therefore the proximate cause of loss, although the consequences may include property damage, bodily injury, financial loss or other forms of damage.
CRO Forum (2016)	Cyber risk [is] defined as the risk of doing business in the cyber environment. The definition of cyber risk covers: • Any risks emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. • physical damage that can be caused by cyber attacks. • fraud committed by misuse of data. • any liability arising from data use, storage and transfer, and • the availability, integrity and confidentiality of electronic information be it related to individuals, companies or government.

https://doi.org/10.1108/JRF-09-2016-0122

Elementos claves de las definiciones de Ciber riesgo

Actividad No autorizada:

Acciones realizadas de manera intencional o no en el contexto de la organización.

Agresor:

Actores estatales y no estatales, crimen organizado, empleados internos, mercenarios digitales

Vulnerabilidad:

Determinadas por las prácticas y estándares que la organización tiene sobre la gestión de la tecnología, sus procesos y las personas.

Ataque:

Aprovechamiento de las vulnerabilidades conocidas o desconocidas para concretar acciones que interrumpan, deterioren, alteren, revelen o destruyan activos y/o servicios claves de la empresa. P.e: Malware, DDos.

Consecuencia:

Los efectos que se generan basados en las intencionalidades de los atacantes. P.e: Revelar información, espionaje, extorsión, robo de información, sabotaje, fraude.

Tipos de atacantes

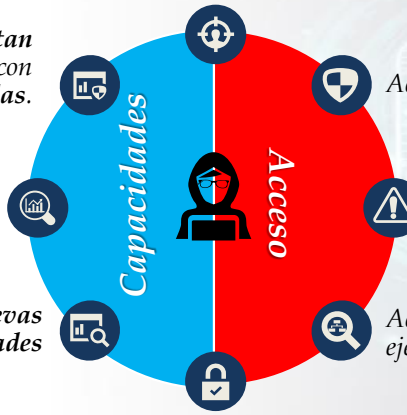
Basados en sus capacidades y el tipo de acceso que tienen a un sistema

Vulnerabilidades

*Aquellos que solo **ejecutan ataques existentes** con **vulnerabilidades conocidas**.*

*Aquellos que pueden analizar un sistema para **encontrar nuevas vulnerabilidades** y **desarrollar código que las explote**.*

*Aquellos que **crean nuevas vulnerabilidades***



Acceso físico al hardware

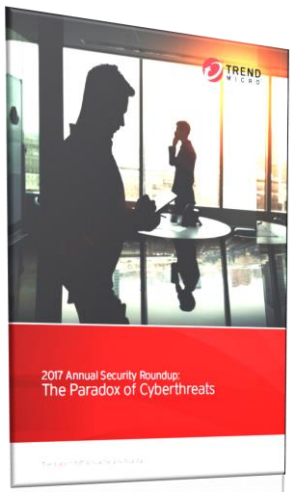
Acceso al software o a los datos

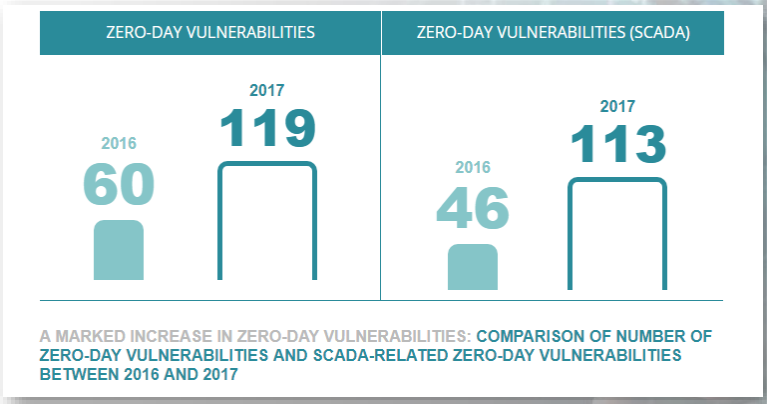
Acceso a las personas que usan o ejecutan el sistema

Falseación de supuestos

Con ideas de: DoD (2013) Resilient Military Systems and the Advanced Cyber Threat. *Task Force Report*. Defense Science Board. January. Recuperado de: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

Tendencias en vulnerabilidades





Fuente: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2017-annual-roundup-the-paradox-of-cyberthreats

Ciber seguros y sus retos

Fuente: https://www2.deloitte.com/insights/us/en/industry/financial-services/demystifying-cybersecurity-insurance.html

Figure 6. Costs of a data breach

Above the surface: Well-known cyber incident costs

1. Customer breach notifications
2. Post-breach customer protection
3. Regulatory compliance (fines)
4. Public relations/crisis communications
5. Attorney fees and litigation
6. Cybersecurity improvements
7. Technical investigations

Below the surface: Hidden or less visible costs

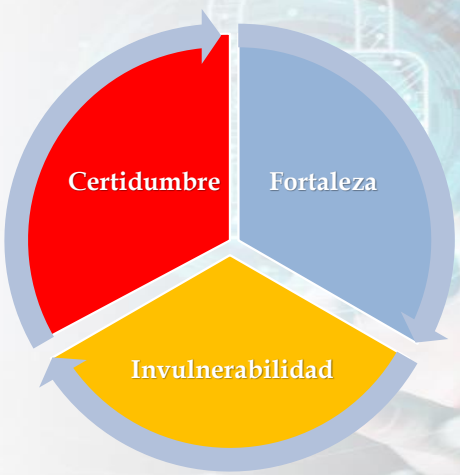
1. Insurance premium increases
2. Increased cost to raise debt
3. Operational disruption or destruction
4. Lost value of customer relationships
5. Value of lost contract revenue
6. Devaluation of trade name
7. Loss of intellectual property

Source: "Beneath the surface of a cyber attack: A deeper look at business impacts," Deloitte Cyber Risk Services.

Deloitte University Press | dupress.deloitte.com

Declaraciones actuales sobre la INFOSEC

- *La **seguridad y la complejidad** no son compatibles.*
- *Las **fallas de seguridad** de la información revelan las limitaciones de la gestión de la seguridad.*
- *Los **incidentes de seguridad** deben ser la excepción de la operación de un programa de seguridad.*
- *Los **errores en las prácticas de seguridad de la información** no son admisibles en ninguna parte de la empresa.*
- *La **incertidumbre de la operación del negocio** es amenaza para la seguridad de la información.*



Fundamentos de INFOSEC en las aplicaciones

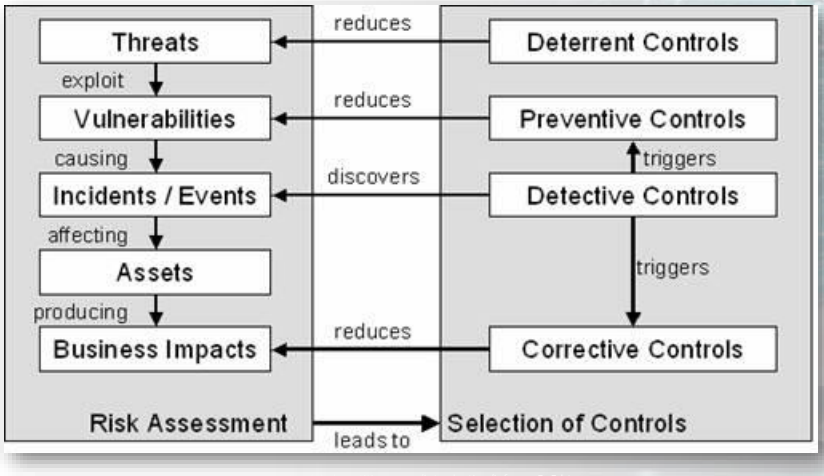
Definiciones

01 *Es un **problema inherente en el diseño** mismo de la aplicación y está embebido en la manera como se plantea la solución que se construye* → **FALLA**

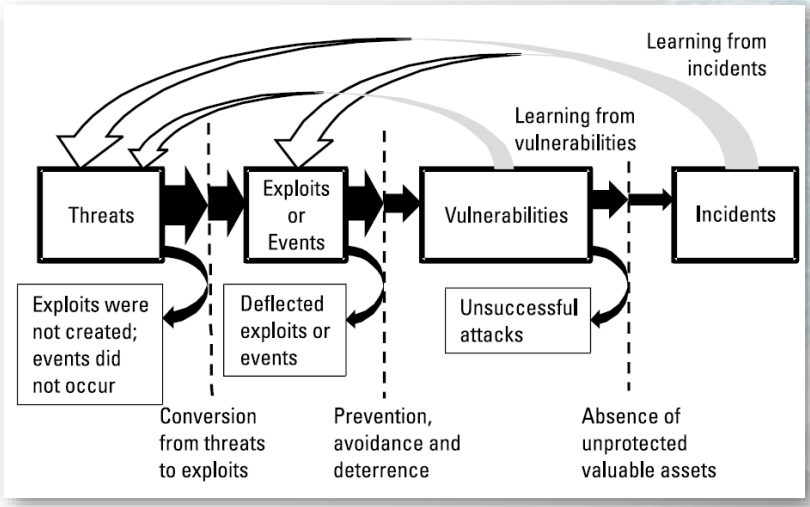
02 ***Es una falla conocida o desconocida en el software**, que bien puede ser producto de su configuración o de las funciones propias del lenguaje utilizado.* → **VULNERABILIDAD**

03 *Es una **limitación operacional** propia de la utilización del software; un evento causado por un usuario o interconexión con otro proceso* → **ERROR**

Enfoque tradicional de riesgos y controles



Dinámica de los incidentes de INFOSEC



Tomado de: Axelrod, C. W.(2013) *Engineering Safe and Secure Software Systems*. Norwood, MA. USA: Artech House. P. 110

Prácticas de modelaje de amenazas/riesgos

OWASP

1. Identification of security objectives;
2. Review of the application;
3. Decomposition of the application;
4. Identification of threats;
5. Identification of vulnerabilities.

STRIDE

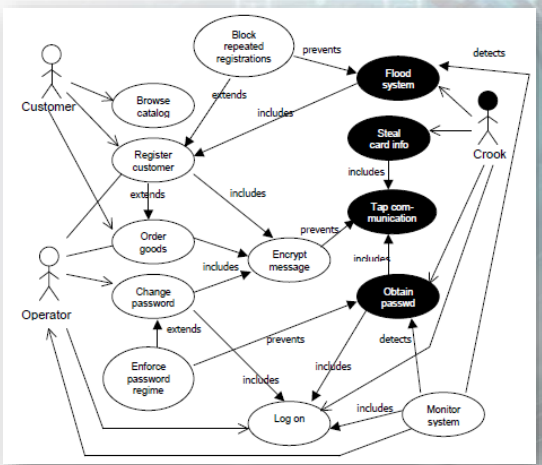
- *Spoofing identity:* One user must not be able to assume the attributes of another user.
- *Tampering:* Users must not be able to modify data or program code in unauthorized ways.
- *Repudiation:* Users must not be able to deny having done something that they actually did.
- *Information disclosure:* Users must be prevented from disclosing sensitive information.
- *Denial of service:* The system must protect against attacks that cause the system not to be available to authorized users.
- *Elevation of privilege:* Users must not be allowed to gain increased capability beyond what they are authorized to perform.

Tomado de: Axelrod, C. W.(2013) *Engineering Safe and Secure Software Systems*. Norwood, MA. USA: Artech House. P. 110

Prácticas de modelaje de amenazas/riesgos

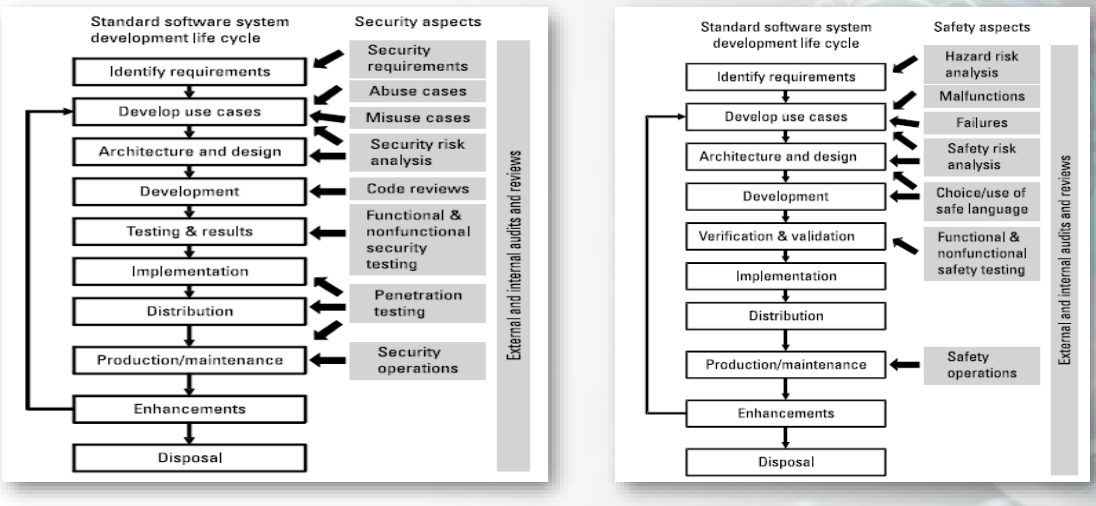
CASOS DE MAL USO – MISUSE CASE

- A *misuse case* is the inverse of a use case, i.e., a function that the system should not allow. Just as [1] defines a use case as a completed sequence of actions which gives increased value to the user, one could define a misuse case as a completed sequence of actions which results in loss for the organization or some specific stakeholder.
- A *mis-actor* is the inverse of an actor, i.e., an actor that one does not want the system to support, an actor who initiates misuse cases.



Tomado de: Sindre, G. & Opdahl.(2005) Capturing security requirements through misuse case. *Requirements Engineering*. 10(1). 34-44. doi: https://doi.org/10.1007/s00766-004-0194-4

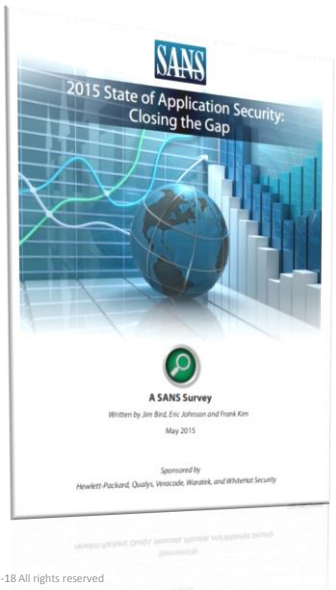
Desarrollo software: Security + Safety



Tomado de: Axelrod, C. W.(2013) *Engineering Safe and Secure Software Systems*. Norwood, MA. USA: Artech House. P. 184 y 205

Prácticas de seguridad y control en aplicaciones

Estándares más usados



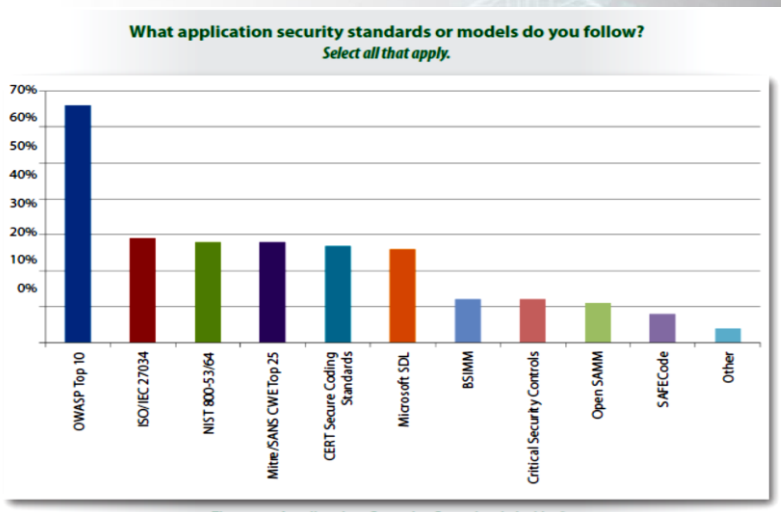
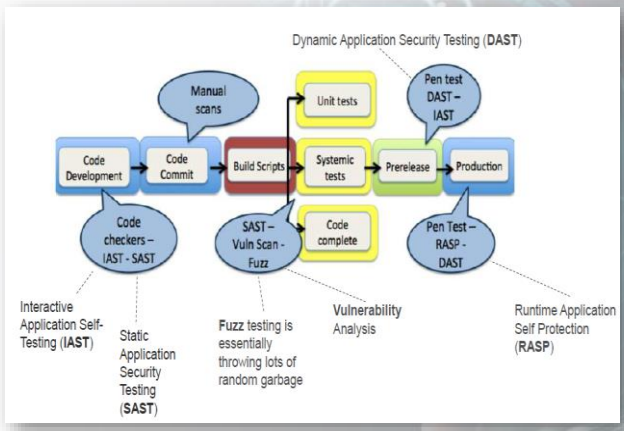


Figure 1. Application Security Standards in Use[5]

Prácticas claves

To be effective, application security has to be included throughout the complete development life cycle:

- **Design and build.** Consider compliance and privacy requirements; design security features; develop use cases and abuse cases; complete attack surface analysis; conduct threat modeling; follow secure coding standards; use secure libraries and use the security features of application frameworks and languages.
- **Test.** Use dynamic analysis (DAST), static analysis (SAST), interactive application security testing (IAST), fuzzing, code reviews, pen testing, bug bounty programs and secure component life-cycle management.
- **Fix.** Conduct vulnerability remediation, root cause analysis, web application firewalls (WAF) and virtual patching and runtime application self-protection (RASP).
- **Govern.** Insist on oversight and risk management; secure SDLC practices, metrics and reporting; vulnerability management; secure coding training; and managing third-party software risk.



"2015 State of Application Security: Closing the Gap," SANS Institute InfoSec Reading Room, May 2015, www.sans.org/reading-room/whitepapers/analyst/2015-state-application-security-closing-gap-35942

Lane, A. (2015) Putting Security Into DevOps. *Securosis*. P. 17 Recuperado de: https://securosis.com/assets/library/reports/Security_Into_DevOps_Final.pdf

Principios de diseño de software confiable

Con ideas de: Rice et al. (2018) Fundamental practices for secure software development. *SAFECode*. Recuperado de: https://bit.ly/2q2smwl

Seguridad por Vulnerabilidad

Un ejercicio de confianza imperfecta

Seguridad Vs Inseguridad

SEGURIDAD	Elemento de análisis	INSEGURIDAD
INTANGIBLE →	*Visibilidad*	← TANGIBLE
SUBJETIVA →	*Comprensión*	← OBJETIVA
EMERGENTE →	*Propiedad*	← INHERENTE
CERTIDUMBRE →	*Foco*	← INCERTIDUMBRE
REQUIERE MODELO →	*Implementación*	← NO REQUIERE MODELO

Seguridad Vs Inseguridad

Seguridad = 1 - Inseguridad

La inevitabilidad de la falla

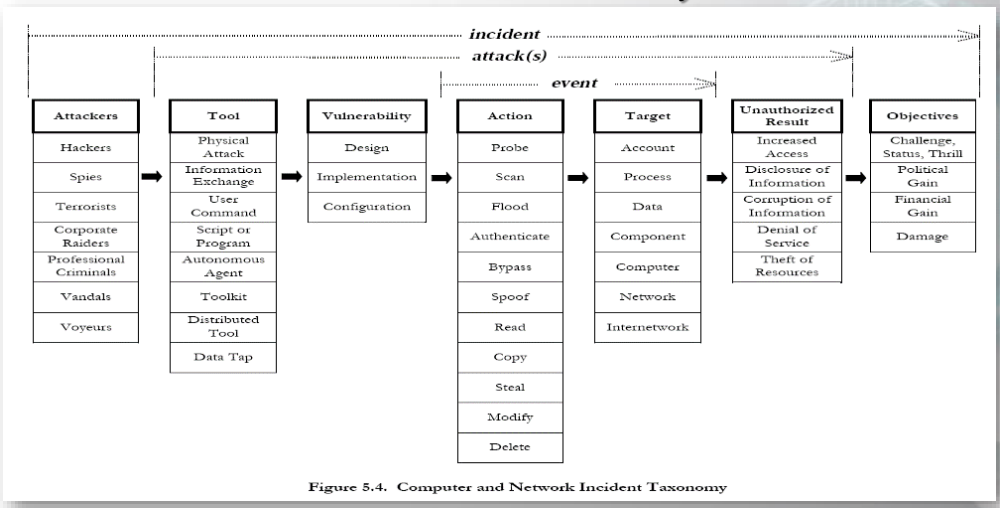
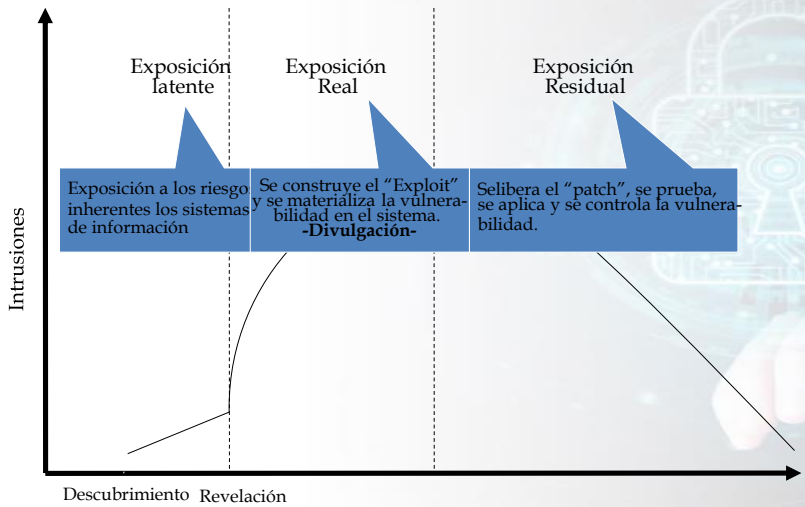


Figure 5.4. Computer and Network Incident Taxonomy

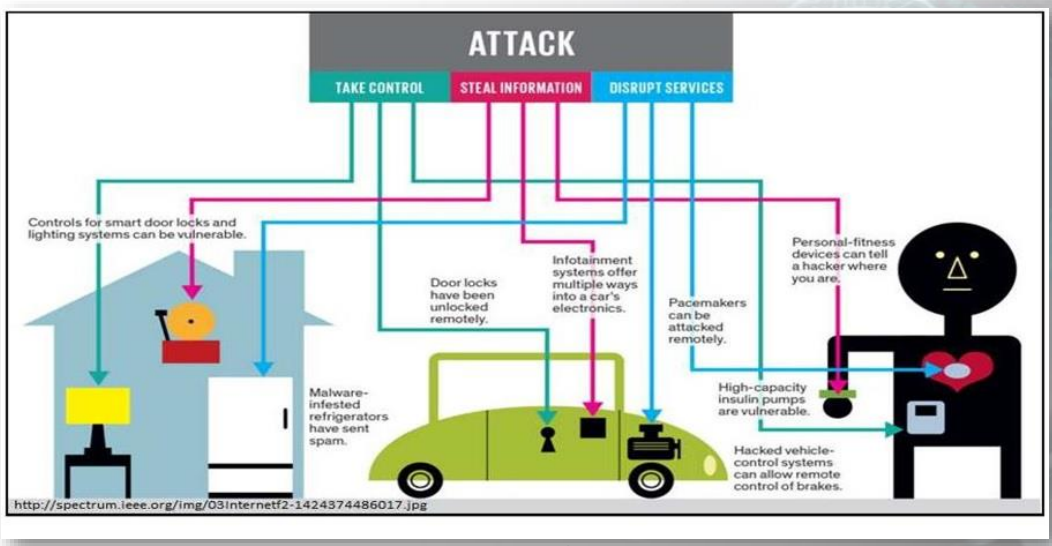
HOWARD, J. y LONGSTAFF, T. (1998) A common language for computer security incidents. *SANDIA REPORT*. Disponible en: http://www.cert.org/research/taxonomy_988667.pdf . Pág.16

La ventana de exposición



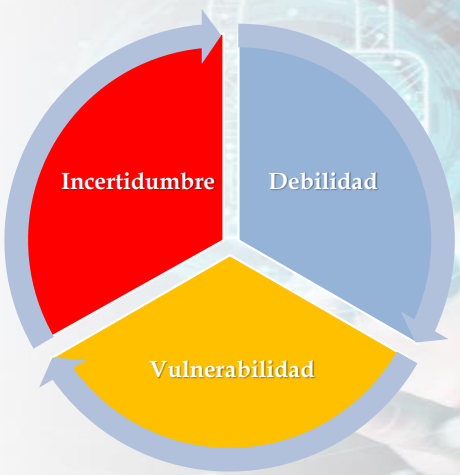
Basado en: W. A. Arbaugh, W. L. Fithen and J. McHugh, "Windows of vulnerability: a case study analysis," in *IEEE Computer*, vol. 33, no. 12, pp. 52-59, Dec 2000. doi: 10.1109/2.889093

Contexto de la vulnerabilidad



Declaraciones prácticas sobre la INFOSEC

- La **debilidad** es la base de la construcción de la confianza y no las certezas.
- La **incertidumbre** es el insumo para construir el futuro y no condenar el presente.
- Las **fallas** son la fuente para aprender y desaprender, y no la forma para infundir miedo o configurar un fracaso.

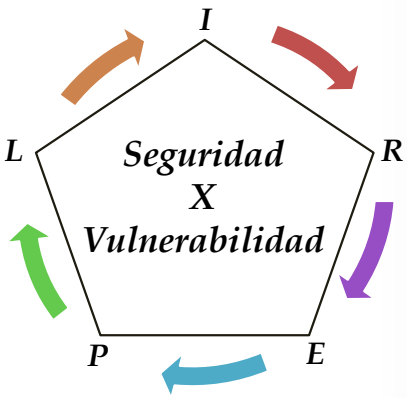


Confianza como fundamento de la INFOSEC

PERIL

Una propuesta conceptual y práctica para el desarrollo de software confiable

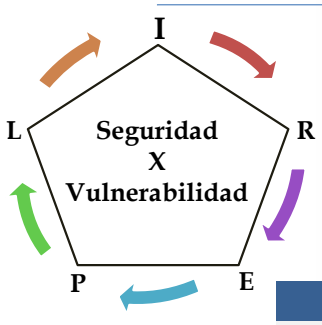
Modelo PERIL



Convenciones

I – Imaginarios *: Valores, actitudes y creencias*
E – Escenarios *: Posibles y probables*
R – Riesgos *: Conocidos, latentes, focales y emergentes*
P – Pruebas *: Controladas y no controladas (no avisadas)*
L – Lecciones *: Aprendidas y por aprender*

Identificando los imaginarios sociales



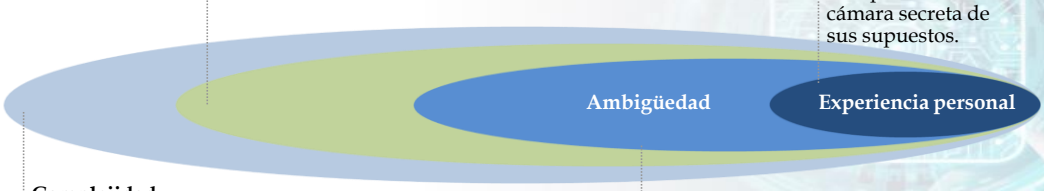
IMAGINARIOS

Enfatizar en los aciertos y fortalezas identificadas
Utilizar las fallas y errores como una forma de crear escenarios de aprendizaje
Incorporar lecciones aprendidas y por aprender

Aspectos claves de la percepción del riesgo

Incertidumbre
Estado de indeterminación entre una causa y sus efectos.

La historia particular de cada individuo interpretada en la cámara secreta de sus supuestos.



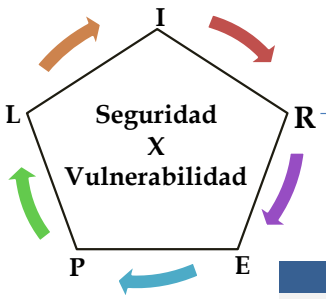
Complejidad
Resultado de la limitada capacidad para distinguir aspectos concretos de la realidad, que superan los saberes previos de los observadores.

Resultado de las interpretaciones legítimas basadas en significados socialmente aceptados y en hechos reales evidenciados.

Riesgo: *Una situación o un evento en el que algo de valor humano está en juego y donde el resultado es incierto.*

Ideas tomadas de: Rosa, E., Renn, O. y McCright, A. (2014) *The risk society revisited. Social theory and governance*. Philadelphia, Pennsylvania. USA: Temple University Press.

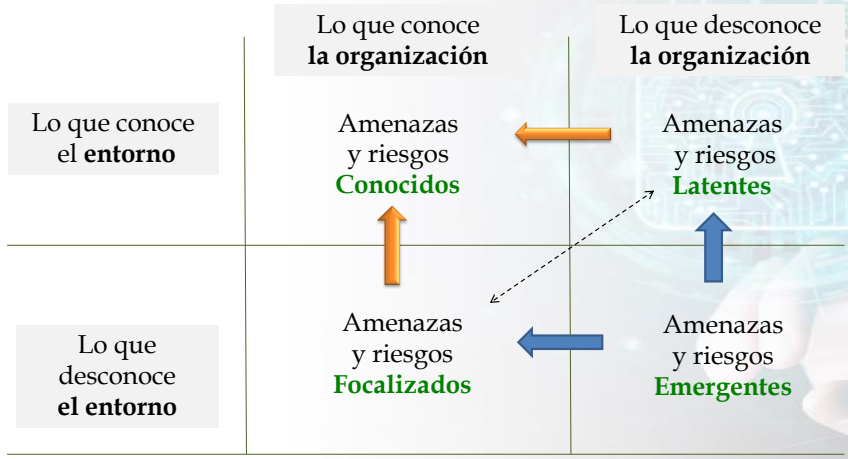
Gestión sistémica de los riesgos



RIESGOS

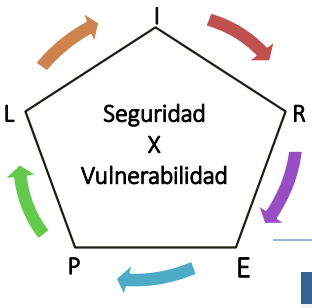
Incorporar vista sistémica de los riesgos en seguridad de la información
Superar la vista exclusiva de los riesgos conocidos
Introducir la vista de los riesgos latentes, focalizados y emergentes

Ventana de AREM



Instrumento diseñado por Jeimy J. Cano M., Ph.D

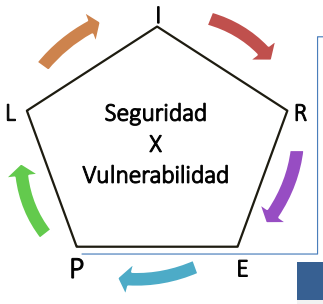
Diseño y gestión de escenarios

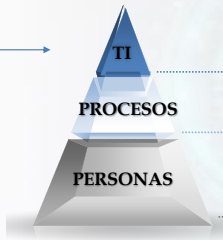


ESCENARIOS

Proyectar los contextos posibles y probables
Desarrollar la capacidad de imaginar situaciones retadoras
Construir una vista compartida de las amenazas, capacidades de los atacantes y postura táctica de protección de la empresa

Pruebas de Uso y Abuso





Pruebas de vulnerabilidades técnicas especializadas

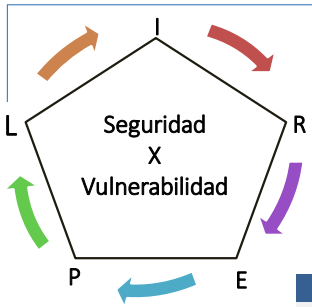
Pruebas de fortaleza y verificación del correcto funcionamiento de los controles definidos

Pruebas de ingeniería social y resistencia a los engaños

PRUEBAS

Verificar el nivel de vulnerabilidad inherente en sistemas objetivo
Tensionar y tratar de romper la confiabilidad de los controles
Manifestar las debilidades que puedan comprometer la confianza corporativa

Lecciones aprendidas



- ¿Qué cosas vamos a **dejar de hacer**, que no aportan al ejercicio?
- ¿Qué cosas vamos a **seguir haciendo**, que benefician y fortalecen la práctica?
- ¿Qué **cosas nuevas** vamos a hacer, que no hemos hecho antes para alimentar y mejorar la práctica?

LECCIONES

Mantener realimentación del modelo
Reconocer quiebres permanentes de la inseguridad
Evitar la falsa sensación de seguridad

Evolución de la INFOSEC

De las prácticas a las capacidades

Contraste entre práctica y capacidad

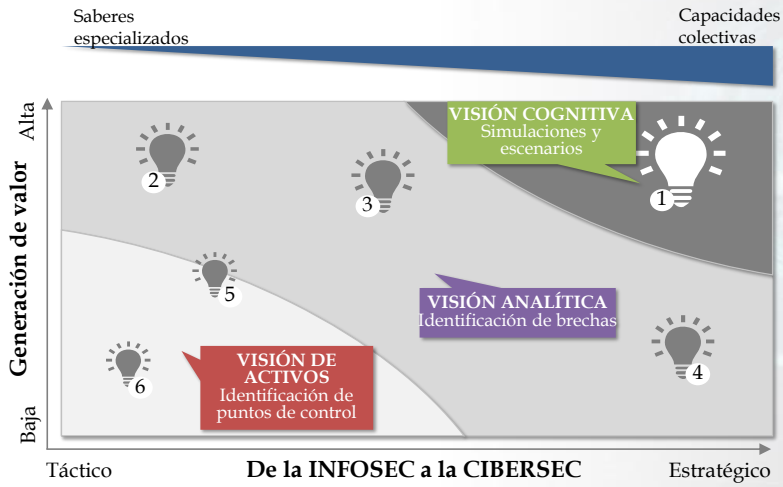
Características

- Cuerpos de conocimiento aplicados y probados
- Basadas en certidumbres
- Verificables y auditables
- **Riesgo**: Es una amenaza

Características

- Desarrolla aprendizajes
- Basada en escenarios inciertos y ambiguos.
- Reta saberes previos y elabora distinciones nuevas
- **Riesgo**: Una oportunidad

Evolución de las prácticas de seguridad y control



1. Juegos de guerra
2. Ejercicios de ingeniería social
3. Inteligencia y cacería de amenazas
4. Análisis de riesgos de INFOSEC
5. Auditorías de INFOSEC
6. Análisis de vulnerabilidades

Prácticas de INFOSEC y Capacidades de CIBERSEC

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

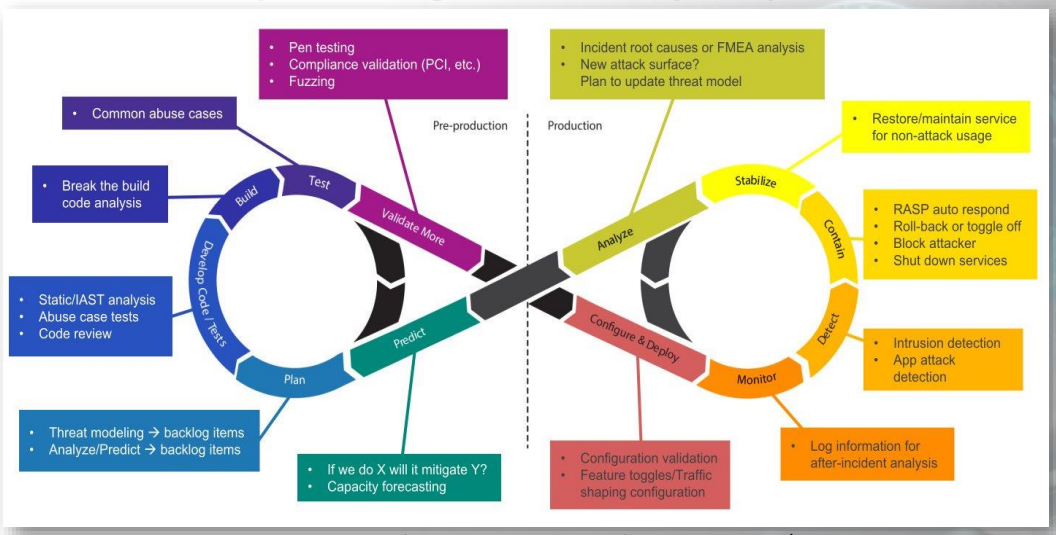
Ecosistema de ciberseguridad

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/

DevSecOps: Entrega continua y confiable



Autor: Larry Maccherone – Twitter @Lmaccherone – 27 Marzo/2017

Tensiones regulatorias

Tensiones claves en la protección de la información en el contexto digital

Interés particular

El derecho a la autodeterminación informática

Buenas prácticas internacionales

Procedimientos y actividades neutrales y académicos para una adecuada protección de los datos personales.

Interés general

Reconocimiento y respeto de los Estados para la protección de los datos personales y el derecho a la privacidad.

Interés comercial

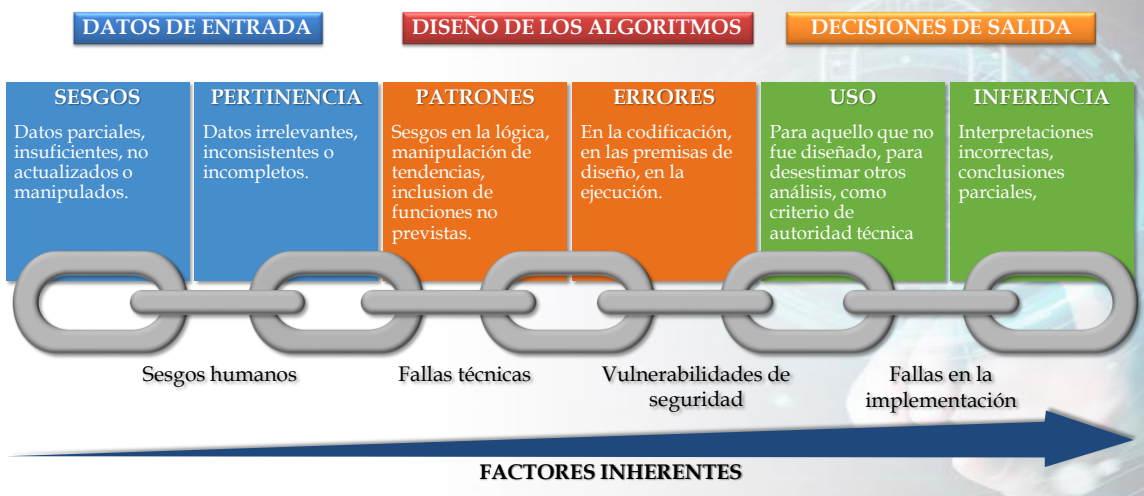
Las actividades legítimas de las empresas en el tratamiento de datos personales con arreglo a la ley y las buenas prácticas.

Principios de la Responsabilidad Digital Empresarial

Principio	Definición
Administración *digital*	*Asegurar que la gestión de los datos personales se realiza con arreglo a la ley y en consonancia con las expectativas de quienes lo proporcionan.*
Transparencia *digital*	*Demostrar apertura en el uso que hacen las empresas datos personales*
Empoderamiento *digital*	*Ofrecer a los clientes mayor control sobre sus datos personales.*
Equidad *digital*	*Aclarar y potencialmente aumentar los beneficios que los clientes reciben a cambio de compartir sus datos.*
Inclusión *digital*	*Usar los datos personales para multiplicar los resultados positivos en la sociedad.*

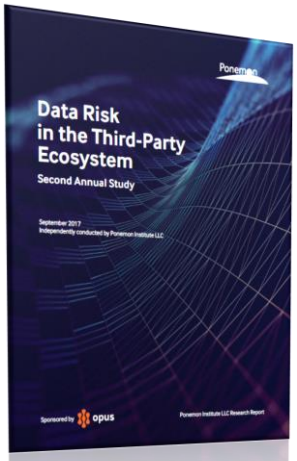
Riesgos emergentes

Inteligencia Artificial: Algoritmos

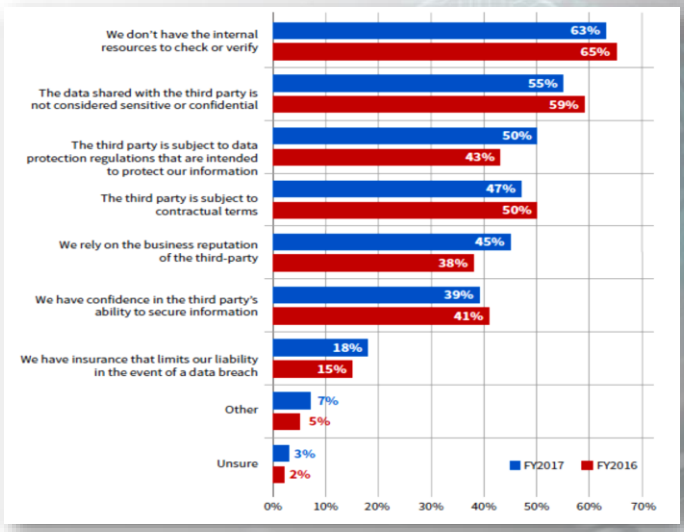


Con ideas de: Krishna, D., Albinson, N. & Chu, Y. (2017) Managing algorithmic risks. Safeguarding the use of complex algorithms and machine learning. Deloitte. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-algorithmic-machine-learning-risk-management.pdf

Terceros: Monitorización activa

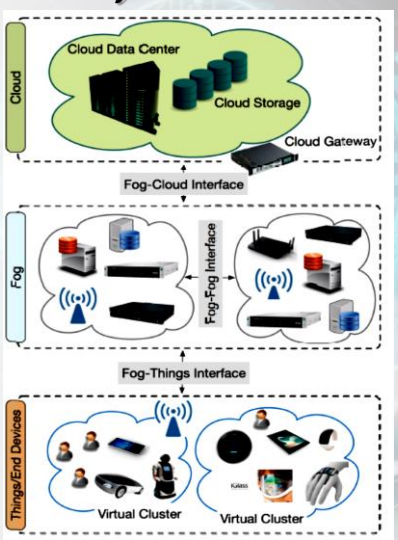


Fuente: https://www.opus.com/resource/data-risk-third-party-ecosystem-2nd-annual-study-ponemon-institute/



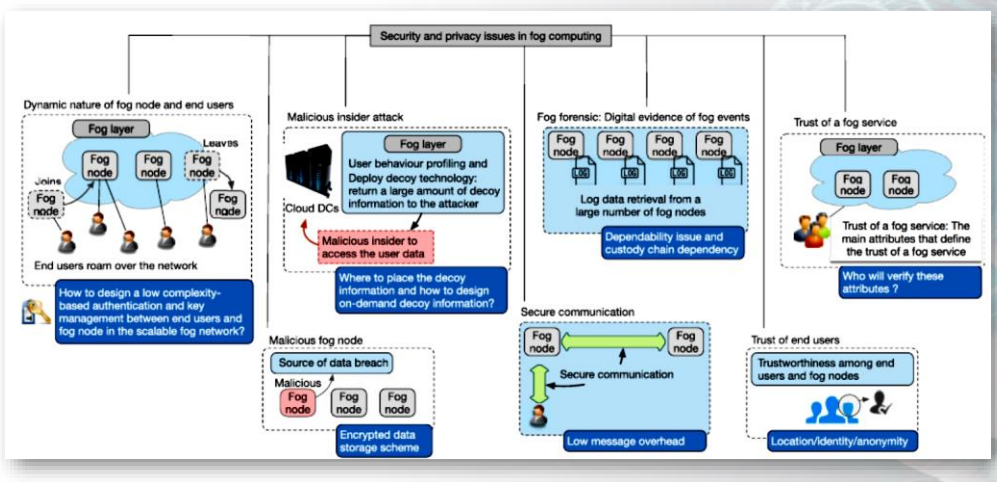
Computación en la niebla: Desafíos

Características de la "Computación en la niebla" – *Fog Computing*	Baja latencia y sensibilidad en la localización.
	Distribución geográfica
	Movilidad en dispositivo final
	Capacidad de procesamiento en un alto número de nodos
	Acceso inalámbrico
	Aplicaciones en tiempo real
	Heterogeneidad



Fuente: Mukherjee, M. et al. (2017) Security and Privacy in Fog Computing. *IEEE Access*. 5. 19293-19304. doi: 10.1109/ACCESS.2017.2749422

Computación en la niebla: Desafíos



Fuente: Mukherjee, M. et al. (2017) Security and Privacy in Fog Computing. *IEEE Access*. 5. 19293-19304. doi: 10.1109/ACCESS.2017.2749422

El imperativo de las API

Con ideas de: Calabro, L., Púrpura, C., Vasa, V. & Perinkolam, A. (2018) El imperativo de API. Desde preocupación de TI hasta mandato de negocios. *Deloitte Insights*. Recuperado de: https://bit.ly/2HB5I73

Conclusiones

Lecciones aprendidas

1. **El atacante interno puede estar en cualquier parte**
   Mecanismos de control y aseguramiento interno
2. **La ingeniería social es la técnica más utilizada y efectiva**
   Aumentar la resistencia del firewall humano
3. **Servicios y productos digitalmente modificados heterogéneos e inseguros**
   Desarrollo de prácticas de seguridad y control para la industria 4.0
4. **Los móviles definen una mayor superficie para los ataques**
   Prácticas de aseguramiento de dispositivos móviles
5. **La gestión de contraseñas debe ser repensada**
   Se debe promover el uso de doble factor de autenticación
6. **Uso de las USB como vector de ataque**
   Reporte y control de USB desatendidas
7. **La fuga y/o pérdida de información como amenaza relevante**
   Uso del cifrado de información como estrategia resistente a estos ataques
8. **El secuestro de información es la norma para los atacantes**
   Aseguramiento de datos con respaldos en medios y localizaciones distintas
9. **Permanecen las configuraciones por defecto**
   Pruebas de vulnerabilidades periódicas
10. **Uso de criptomonedas para el pago de extorsiones**
    Monitoreo y cooperación frente a los ecosistemas digitales criminales

Basado en las ideas de: Pagnota, S. (2016) 10 lecciones de seguridad que nos dejó Mr. Robot S02. Recuperado de: http://www.welivesecurity.com/la-es/2016/09/23/lecciones-seguridad-mr-robot-s02/

Máximas de la InfoSEC y CiberSEC

Vista holística de la seguridad digital

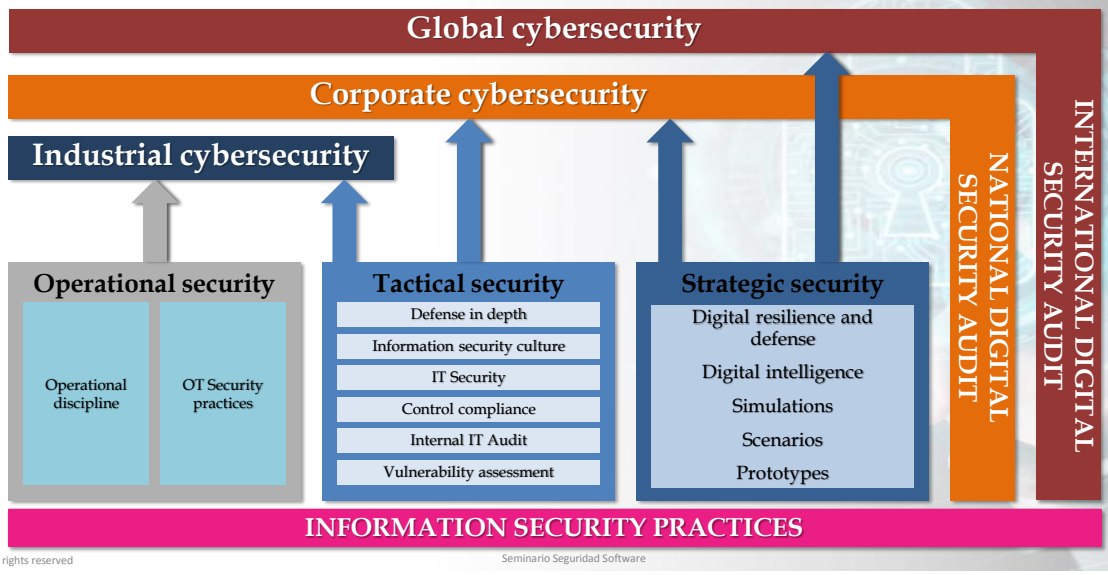


Imagen tomada de: https://i1.wp.com/www.kachwanya.com/wp-content/uploads/2015/02/CyberattacksExit.jpg

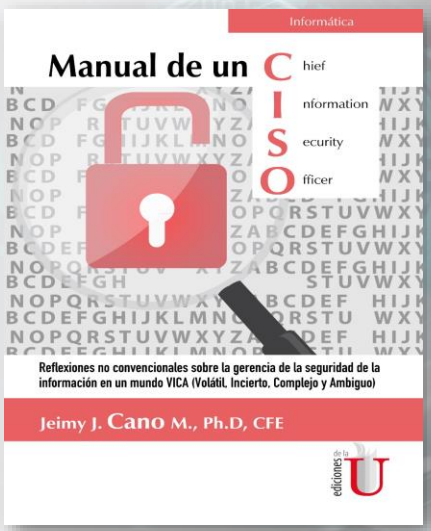
Universidad del Rosario ACBSP

Para continuar 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: (Formato Ebook)
https://edicionesdelau.com/producto/manual-de-un-ciso-2/



La ***seguridad por vulnerabilidad*** no es sólo un ejercicio de implementación de prácticas de seguridad y control, *es una apuesta conceptual y práctica que habilita la* ***resiliencia del software*** *frente a los* ***riesgos y amenazas emergentes*** *en un entorno digitalmente modificado.*

Jeimy J. Cano M.

@itinsecure

Universidad del Rosario

Seguridad por Vulnerabilidad:

Superando el paradigma de los extremos

Jeimy J. Cano M., Ph.D, CFE
Profesor Asociado
Escuela de Administración

Blog:
http://insecurityit.blogspot.com

@itinsecure


TECNOLÓGICO SUPERIOR CORDILLERA
25 AÑOS
CIDE
Centro de Investigación y Desarrollo Ecuador
SEMINARIO INTERNACIONAL DE
SEGURIDAD
EN EL DESARROLLO DE
SOFTWARE
WWW.CIDECUADOR.COM
Una vez finalizado el evento esta presentación sera publicada en su respectiva página web
JCM-18 All rights reserved
Seminario Seguridad Software
61