El Ciberefecto mariposa

Las implicaciones de una mala programación dse aplicaciones

10° CONGRESO DE PREVENCIÓN DEL FRAUDE Y SEGURIDAD
protección, confianza y defensa.

M. Farias-Elinos

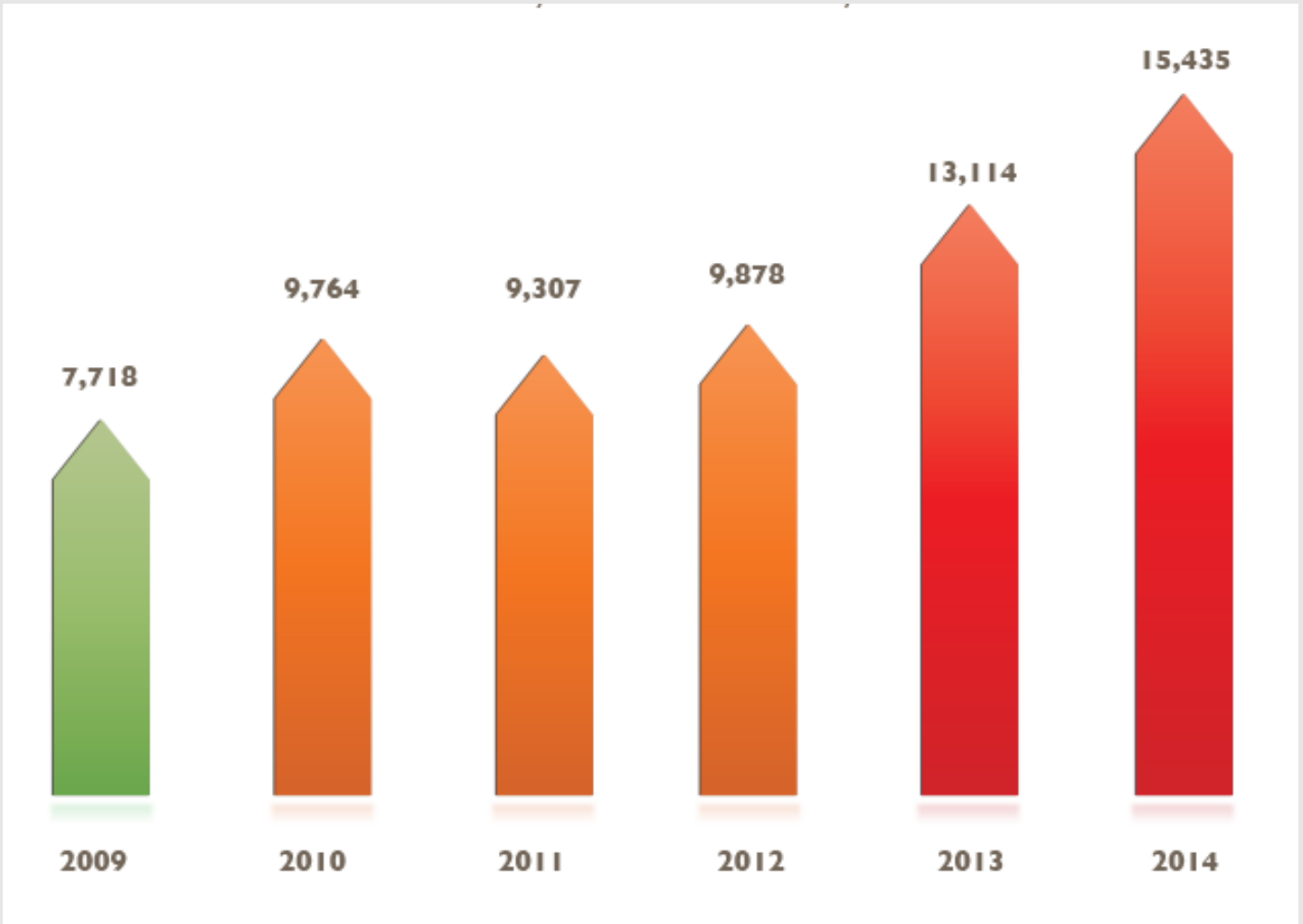
ITESM, CUDI, Kalan T'aan, Rogue, EC-Council

October 27, 2016

80 años ASOBANCARIA

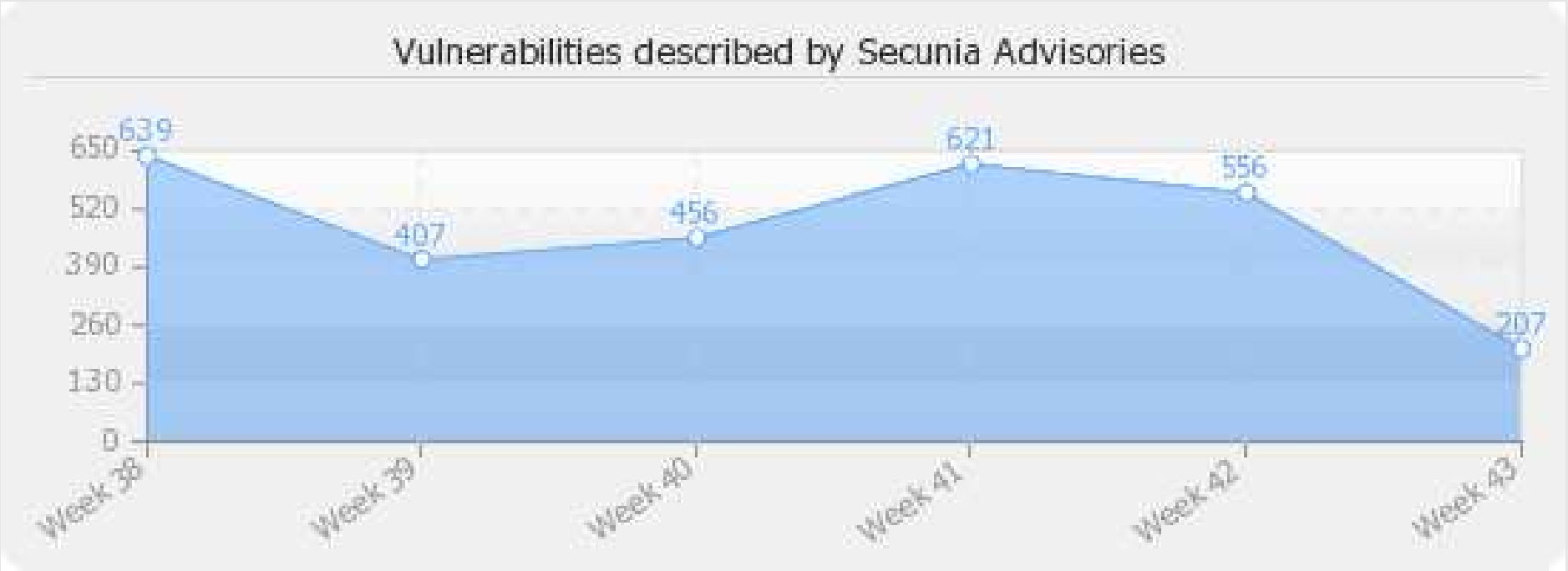
ASOBANCARIA

Vulnerabilidades en los últimos 5 años



10° CONGRESO DE PREVENCIÓN DEL FRAUDE Y SEGURIDAD
protección, confianza y defensa.

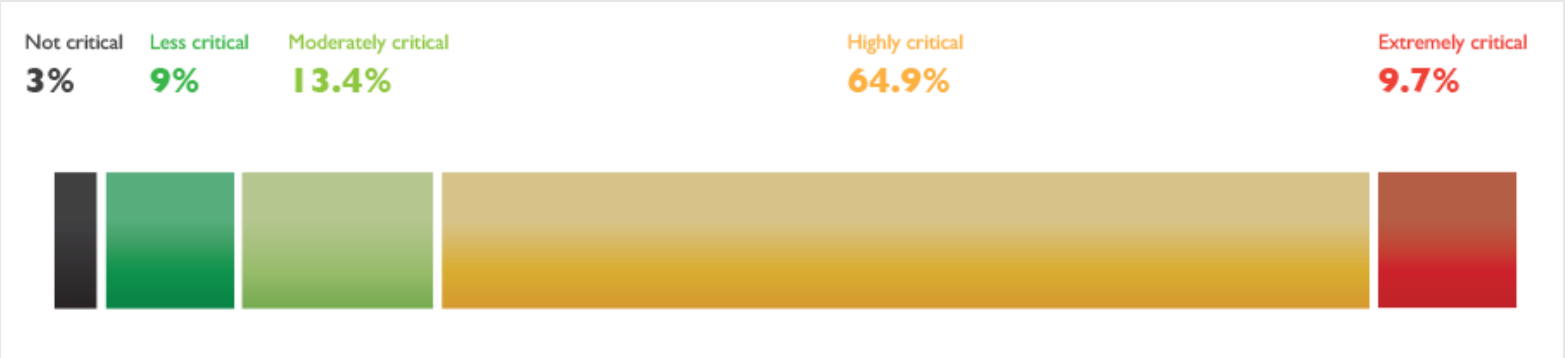
Vulnerabilidades en las últimas semanas



80 años ASOBANCARIA

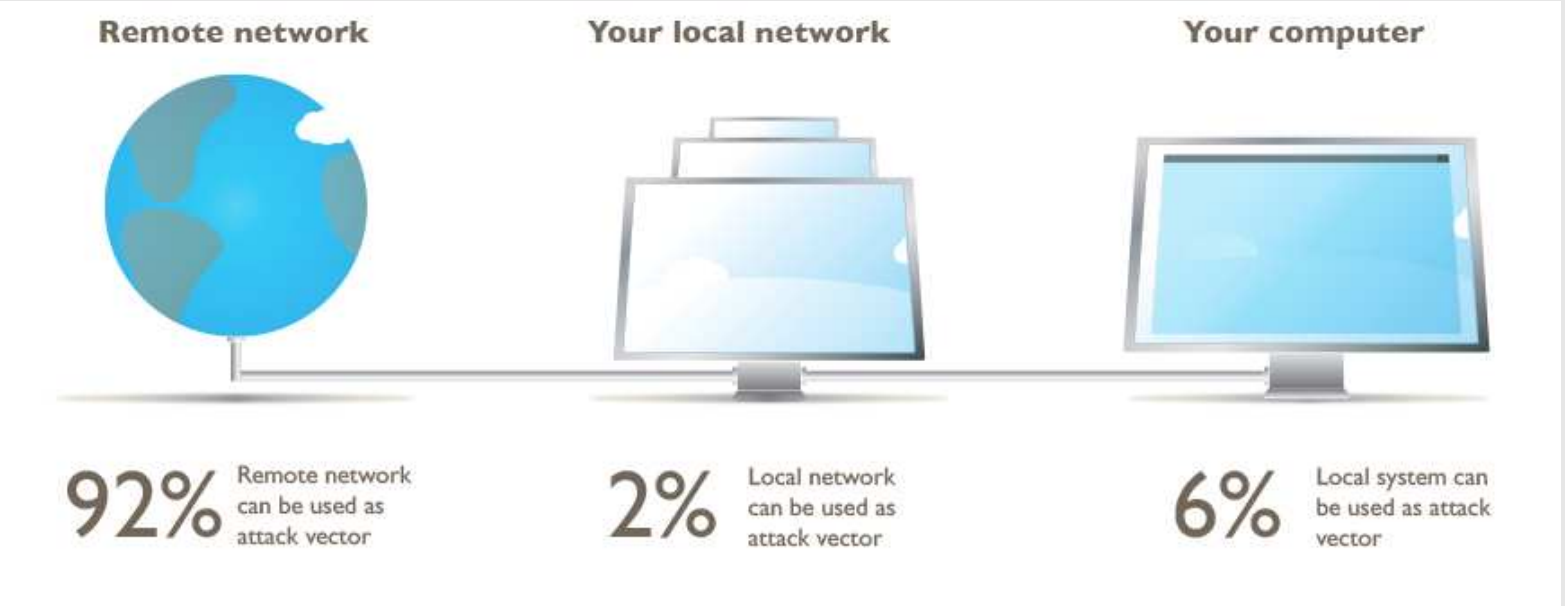
10° CONGRESO DE PREVENCIÓN DEL FRAUDE Y SEGURIDAD
protección, confianza y defensa.

Criticidad de las Vulnerabilidades



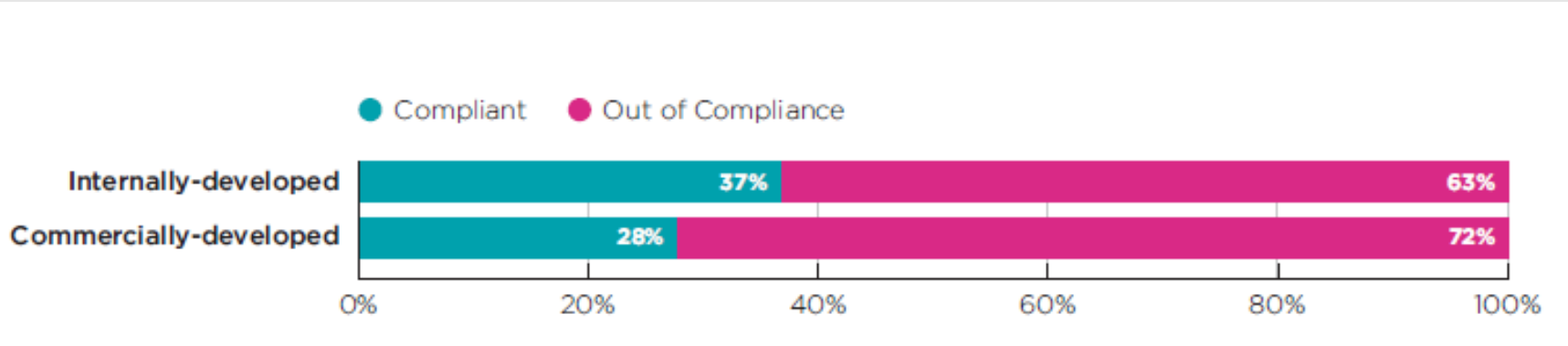
80 años ASOBANCARIA desde 1936 ASOBANCARIA

Forma de explotar las Vulnerabilidades



10° CONGRESO DE PREVENCIÓN DEL FRAUDE Y SEGURIDAD
protección, confianza y defensa.

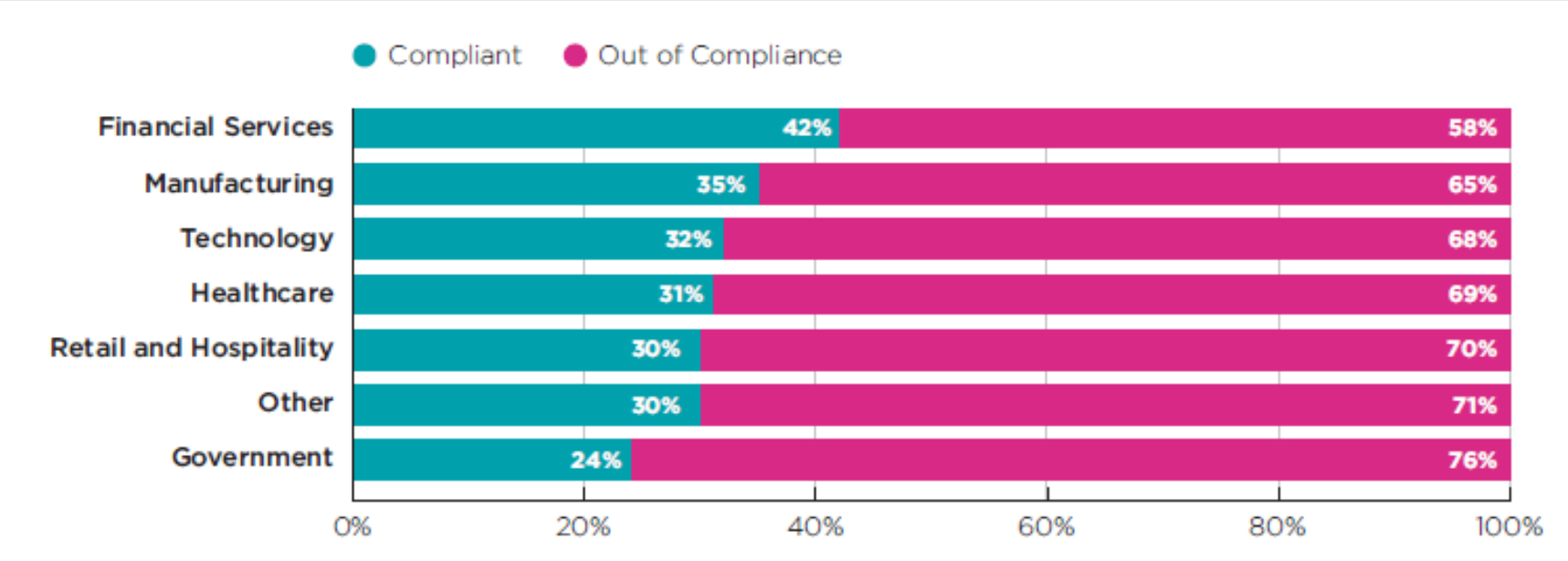
Cumplimiento con OWASP



80 años ASOBANCARIA desde 1936 ASOBANCARIA

10° CONGRESO DE PREVENCIÓN DEL FRAUDE Y SEGURIDAD
protección, confianza y defensa.

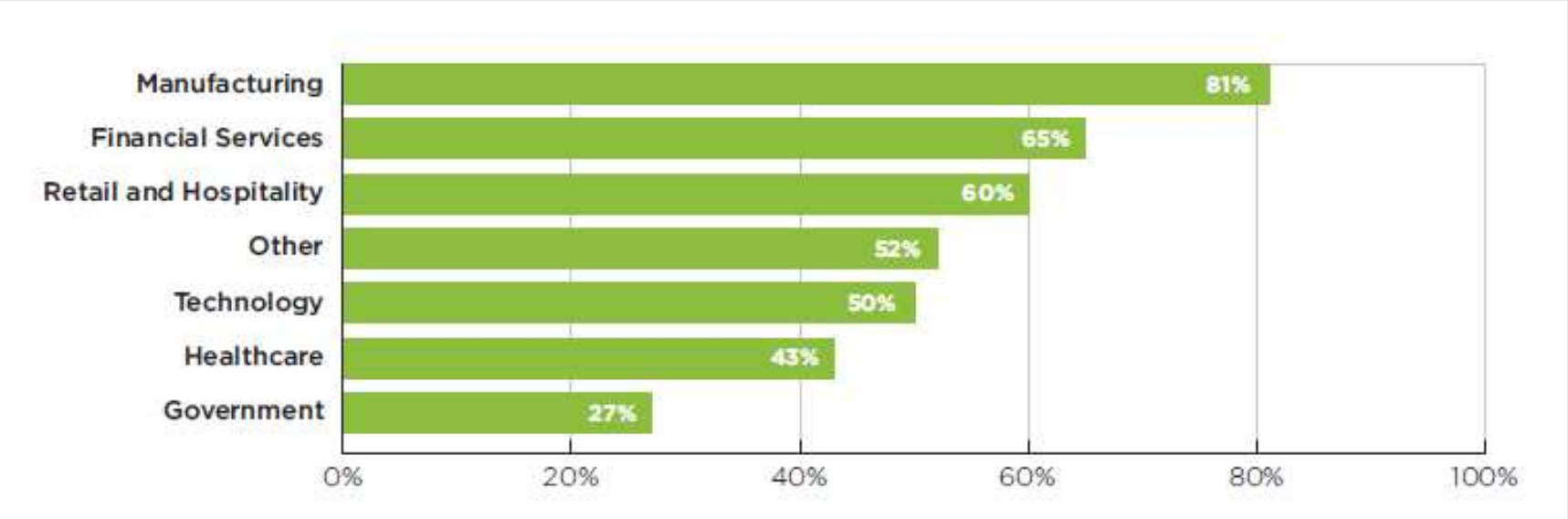
Cumplimiento con OWASP por sector



80 años ASOBANCARIA desde 1936 ASOBANCARIA

10° CONGRESO DE PREVENCIÓN DEL FRAUDE Y SEGURIDAD
protección, confianza y defensa.

Corrección de vulnerabilidades por sector



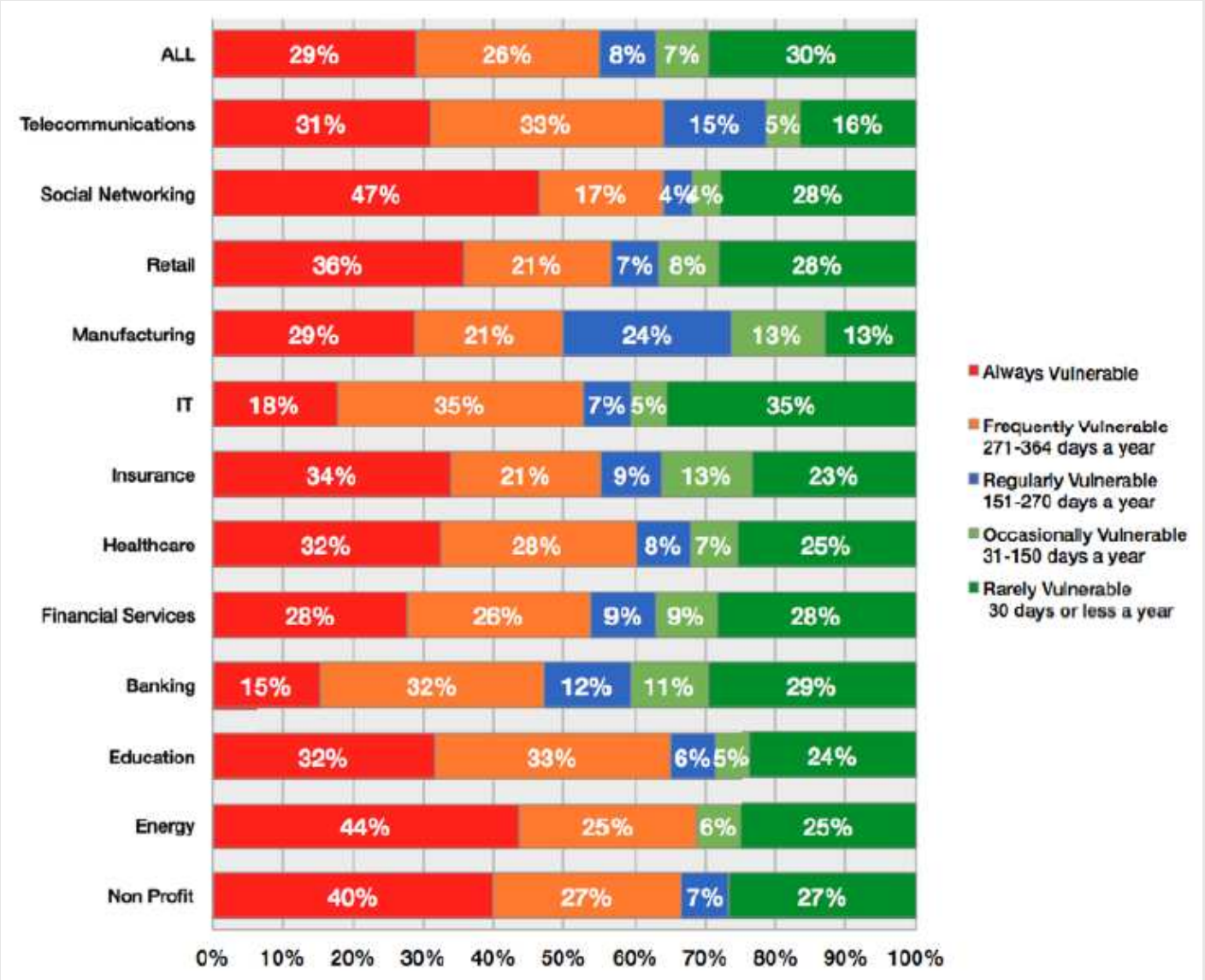
80 años ASOBANCARIA desde 1936 ASOBANCARIA


DEMO

El *Top* de vulnerabilidades

Vulnerability	Financial Services	Government	Healthcare	Manufacturing	Retail & Hospitality	Technology	Other	Rank
Code Quality	65%	70%	80%	56%	68%	70%	65%	1
Cryptographic Issues	60%	66%	61%	51%	63%	62%	59%	2
Information Leakage	58%	62%	60%	49%	55%	62%	53%	3
CRLF Injection	52%	52%	48%	45%	54%	54%	48%	4
Cross-Site Scripting (XSS)	49%	51%	46%	45%	52%	49%	47%	5
Directory Traversal	48%	48%	45%	40%	44%	48%	46%	6
Insufficient Input Validation	41%	45%	43%	33%	44%	37%	37%	7
SQL Injection	29%	40%	32%	31%	25%	30%	34%	8
Credentials Management	25%	20%	26%	24%	24%	28%	32%	9
Time and State	23%	19%	23%	17%	21%	26%	23%	10

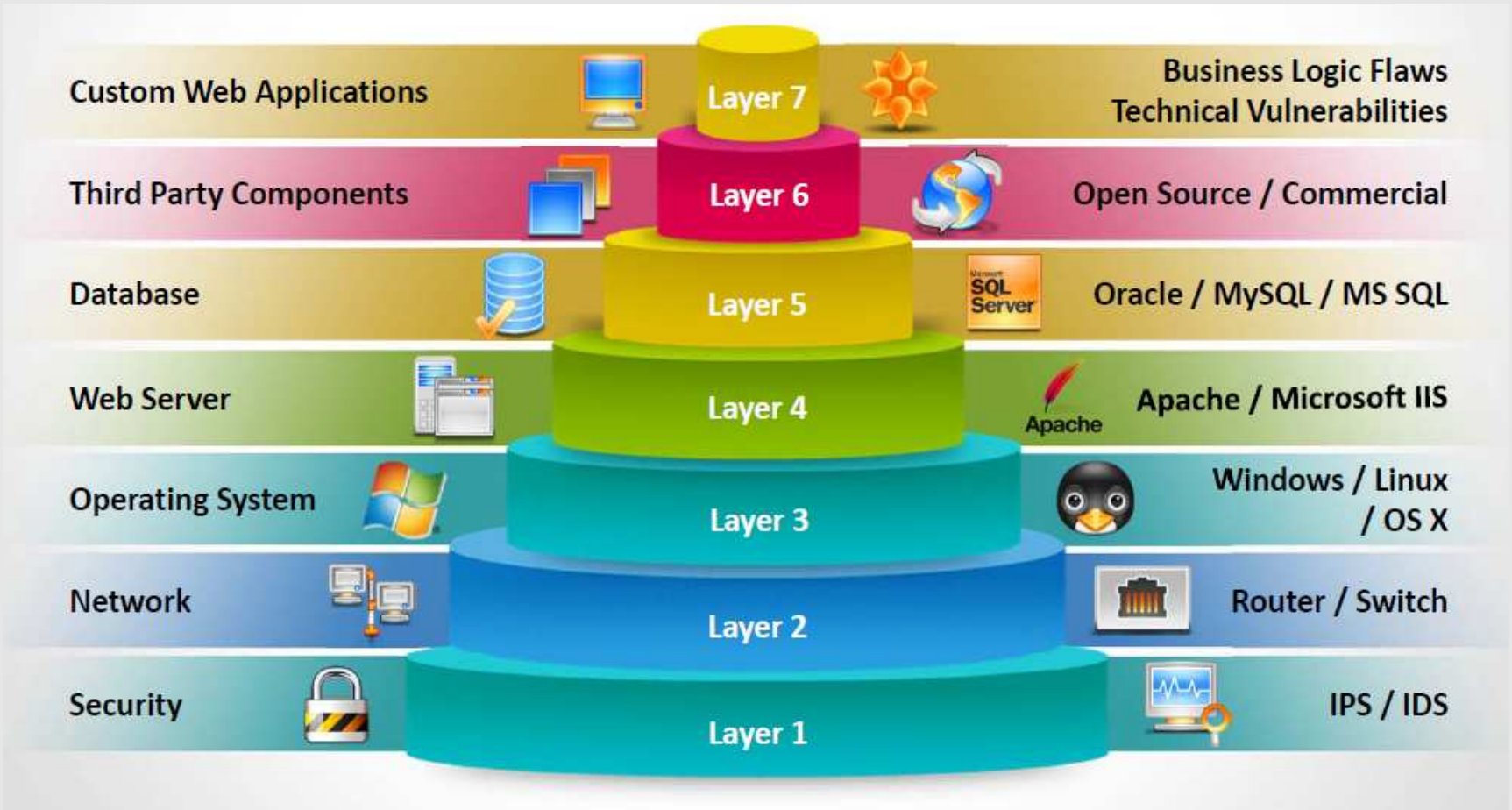
Vulnerabilidades por sector



Infraestructura crítica

10° CONGRESO DE PREVENCIÓN

Stack de vulnerabilidades



80 años ASOBANCARIA

ASOBANCARIA

Ciberpandemia

- Enfermendad epidémica: Vulnerabilidades
- Área geográficamente extensa: Internet
- Población: Computadoras smarphones, routers, switches, servers, etc

Predicciones

- Incremento de ataques al sector salud (expedientes médicos)
- Los intrusos se enfocaran al Internet de las cosas, como medio para acceder a las redes coorporativas
- El mercado negro de robo de tarjetas se transformarán en concesionarios de información
- Los ataques de equipos mobiles no van por los datos en ellos, sino por esquemas de autenticación (pago con celulares, el mobil personal/trabajo, etc)
- Nuevas vulnerabilidades surgirán de codigo fuente antiguo (falta de mantenimiento de aplicaciones viejas que siguen utilizandose)
- Incremento de complejidad/sofisticacion de amenazas vía correo electrónico

Predicciones (cont)

- Los intrusos se enfocarán a la nube más que en las redes organizacionales.
- Toma mayor relevancia los esquemas de ciberguerra, ciberespionaje y ciberterrorismo
- Java será siendo altamente explotable y altamente explotado - con grandes repercuisiones.
- Cibercriminales apuntarán al eslabón más débil de la cadena de intercambio de datos.
- Incremento de la ofensiva que se aprovecha de los errores en la programación de las aplicaciones.

Déficit de especialistas en Seguridad de TI

- Urge desarrollar una vacuna contra la pandemia
  - Vacuna: Programación Segura
  - Formar profesionales en Ingeniería de Software con solidas bases en programación segura.
- Todas las áreas de TI son responsables de la seguridad
- Existe un deficit de 10,000 especilistas en seguridad por año

El Ciberefecto mariposa

Las implicaciones de una mala programación dse aplicaciones

10° CONGRESO DE PREVENCIÓN DEL FRAUDE Y SEGURIDAD
protección, confianza y defensa.

M. Farias-Elinos

ITESM, CUDI, Kalan T'aan, Rogue, EC-Council

October 27, 2016

80 años ASOBANCARIA

ASOBANCARIA