./"R1ESG0S Y AM3NAZ4S.EXE"

tekium.mx:/home/ciberseguridad:$ cat ./expositor.txt

Enrique Vaamonde M. - @_ejvm - ev@tekium.mx

ESTADISTICAS

tiempo promedio de detección de intruso (nivel mundial):

3 meses

tiempo dentro de red institución afectada (caso SPEI):

9 meses

ataques exitosos sufridos por entidades del sector financiero[1]:

43% grandes / 15% medianas / 6% pequeñas

ESTADISTICAS

promedio de costos asociados a ciberataques en México[1]:

USD $107M

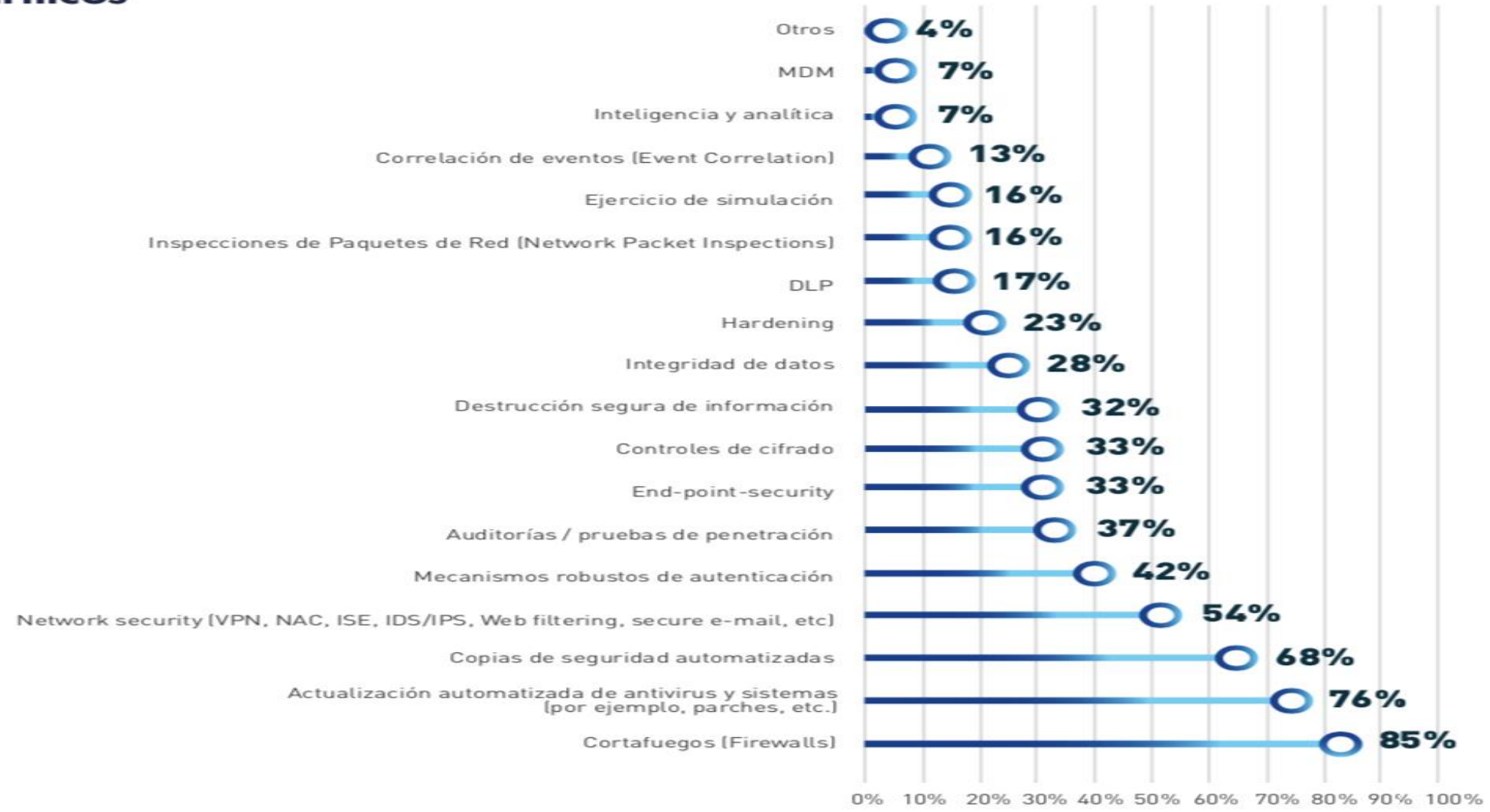
promedio de gastos asociados a respuesta y recuperación[1]:

USD $447k

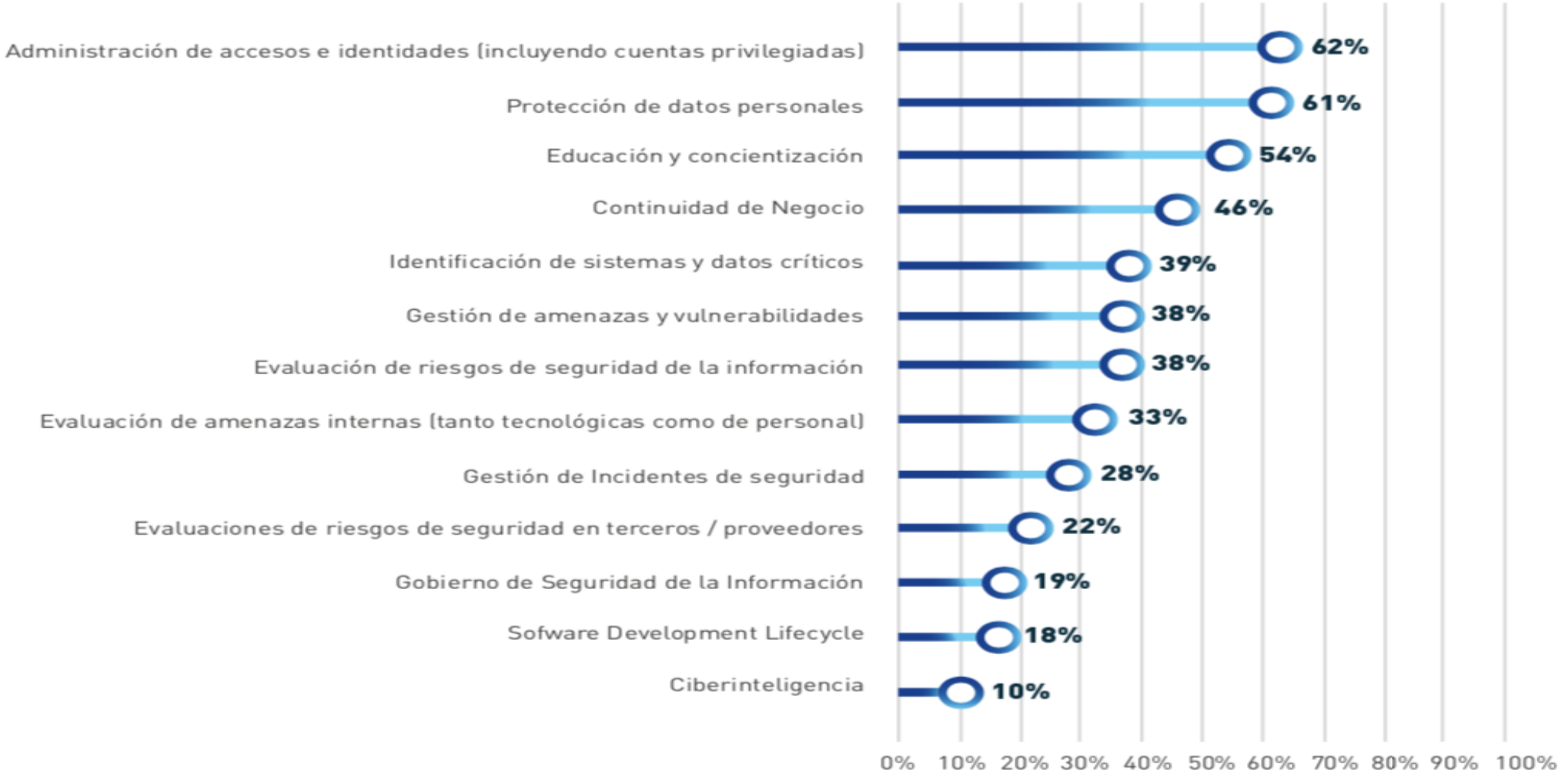
ataques que se detectan pero se desconoce como ocurrieron[2]:

27% de ataques

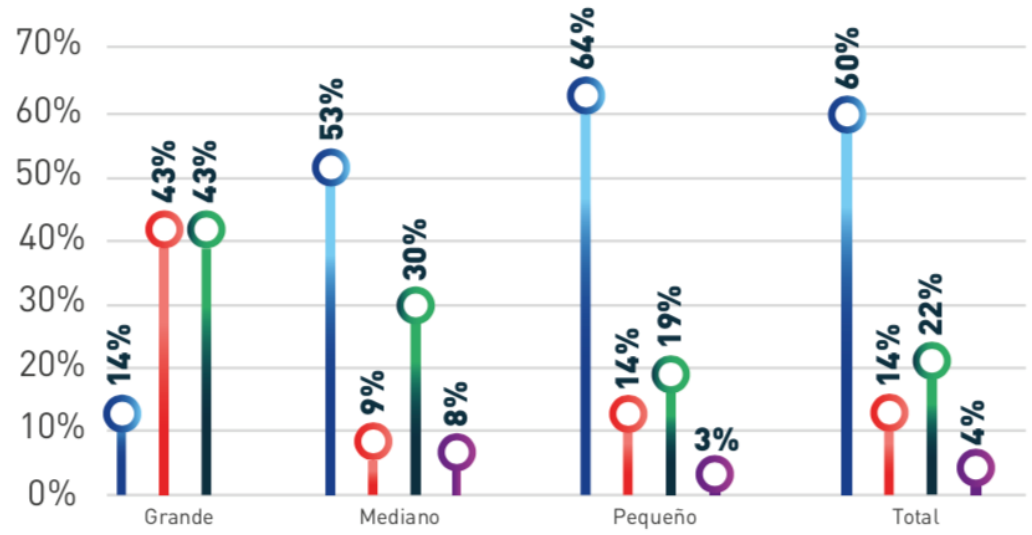
Gráfica 13. Acciones y medidas técnicas de seguridad de la información (incluyendo ciberseguridad) para proteger los sistemas de información críticos



Gráfica 14. Procesos / programas respecto a la seguridad digital implementados actualmente por las entidades e instituciones financieras



Gráfica 21. ¿La entidad / institución financiera a la cual usted pertenece ha sido evaluada externamente en los últimos dos (2) años bajo alguna metodología de seguridad de la información (incluyendo ciberseguridad) para determinar su nivel de madurez?



- No, nuestra entidad / institución no ha sido evaluada
- Sí se realizó la evaluación y se ejecutaron satisfactoriamente las acciones correspondientes
- Sí se realizó la evaluación y se están ejecutando actualmente las acciones correspondientes
- Sí se realizó la evaluación, pero no ha sido posible ejecutar las acciones correspondientes

REFLEXIÓN

“preocupa que más del 70% de las entidades e instituciones financieras de los sectores Ahorro y Crédito Popular (SOCAP y SOFIPO) e Intermediarios financieros no bancarios de México indican que no han sido evaluadas” [1]

1)Fuente:

Reporte 2019 de la Organización de Estados Americanos:

“ESTADO DE LA CIBERSEGURIDAD EN EL SISTEMA FINANCIERO MEXICANO”

2) Fuente:

Sophos Security Labs

ADVERSARIOS

CARACTERÍSTICAS

PACIENTES

RECURSOS

DETERMINADOS

CONOCIMIENTOS

Hackers
- oportunistas -

Crimen organizado

AVANCE "Bruselas prevé que el triunfo de Macron dé un impulso a la UE", en la portada de este martes

CIBERDELINCUENCIA

Corea del Norte ordena a su ejército de hackers robar a bancos de todo el mundo

El intento de robo a entidades polacas deja al descubierto un rastro de objetivos norcoreanos

Un robo de 81 millones

Investigadores privados que han tenido acceso a los datos del ataque fallido concluyen que los que estaban detrás del intento son los mismos responsables que **robaron 81 millones de dólares del Banco Central de Bangladesh** –mediante otro hackeo- y del ataque y sustracción de datos a **Sony** tras el estreno de la película *The Interview*, que se mofaba del régimen norcoreano.

CÁRTELES Y FUERZAS ARMADAS CRECEN PRESENCIA EN HACKEOS AVANZADOS

Bandas criminales comienzan a tercerizar servicios de hackers en ciberataques de alto impacto para espiar, robar datos industriales y vulnerar la infraestructura crítica.

Lunes, 25 de julio de 2016 a las 7:52 AM

Portada / Actualidad /

Forbes Staff
octubre 3, 2018 @ 5:13 pm

Hackers norcoreanos estarían detrás del ataque a Bancomext

Un estudio elaborado por la firma de ciber seguridad FireEye determinó que el grupo de hackers norcoreanos APT38 estaría detrás de los ataques a varios bancos del mundo

Newsweek U.S. WORLD BUSINESS TECH & SCIENCE CULTURE SP

WORLD

NORTH KOREA'S HACKERS FUND NUCLEAR, MISSILE PROGRAMS BY STEALING FROM BANKS, OTHERS

BY GREG PRICE ON 5/16/17 AT 2:05 PM

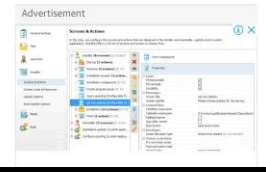
supporter | subscribe | search | jobs | dating | more | International edition

theguardian

otball | opinion | culture | business | lifestyle | fashion | environment | tech | travel | browse all sections

Ransomware attack 'not designed to make money', researchers claim

Digital security researchers say malware attack that spread from Ukraine appeared to be focused on damaging IT systems



QUARTZ

JUMPING THE AIR GAP

Wikileaks: The CIA can remotely hack into computers that aren't even connected to the internet

HOME | SEARCH

The New York Times

Inside a Secretive Group Where Women Are Branded

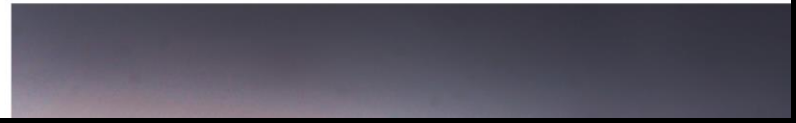
2. CONTRIBUTING OP-ED WRITER Yes, This Is a Witch Hunt. I'm a Witch and I'm Hunting You.

3. OP-ED COLUMNIST What's the Matter With Republicans?

4. Top General's Grief Becomes Political Talking Point for Trump

Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny

By NICOLE PERLROTH, MICHAEL WINES and MATTHEW ROSENBERG SEPT. 1, 2017



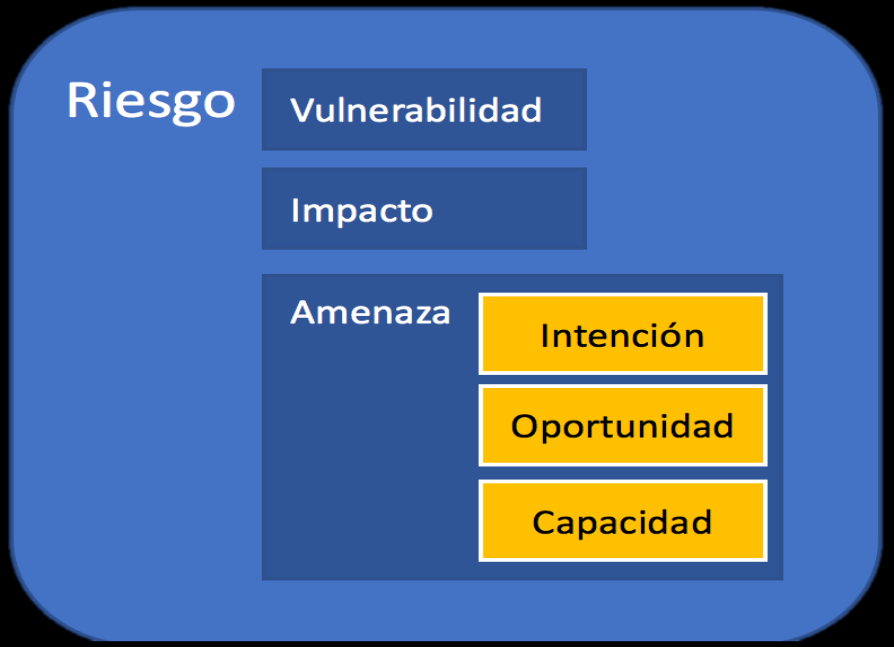
Hacktivistas

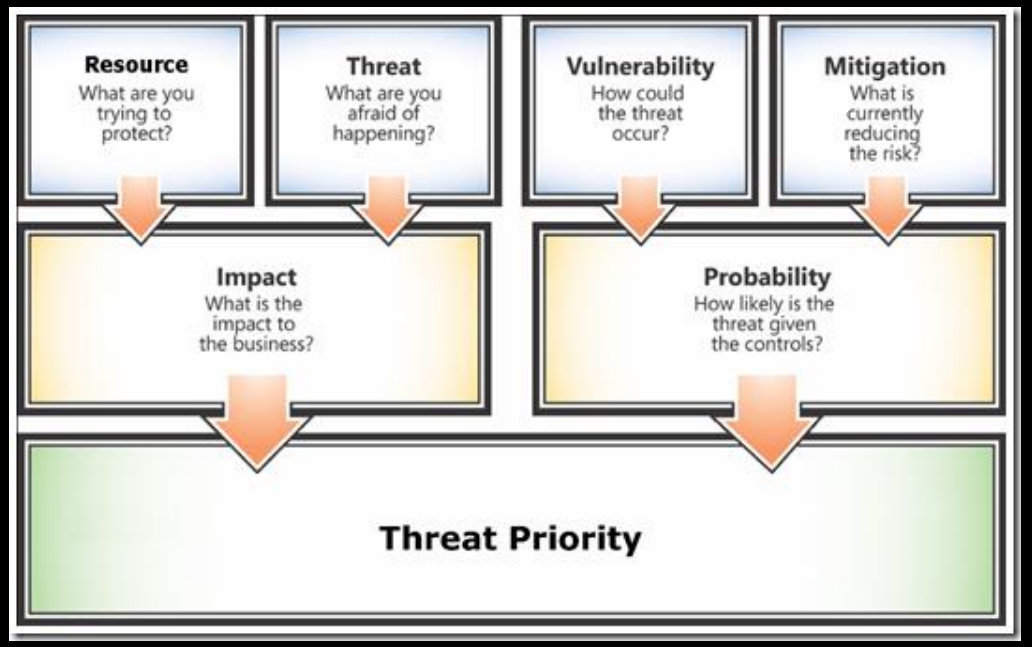
Error de usuario

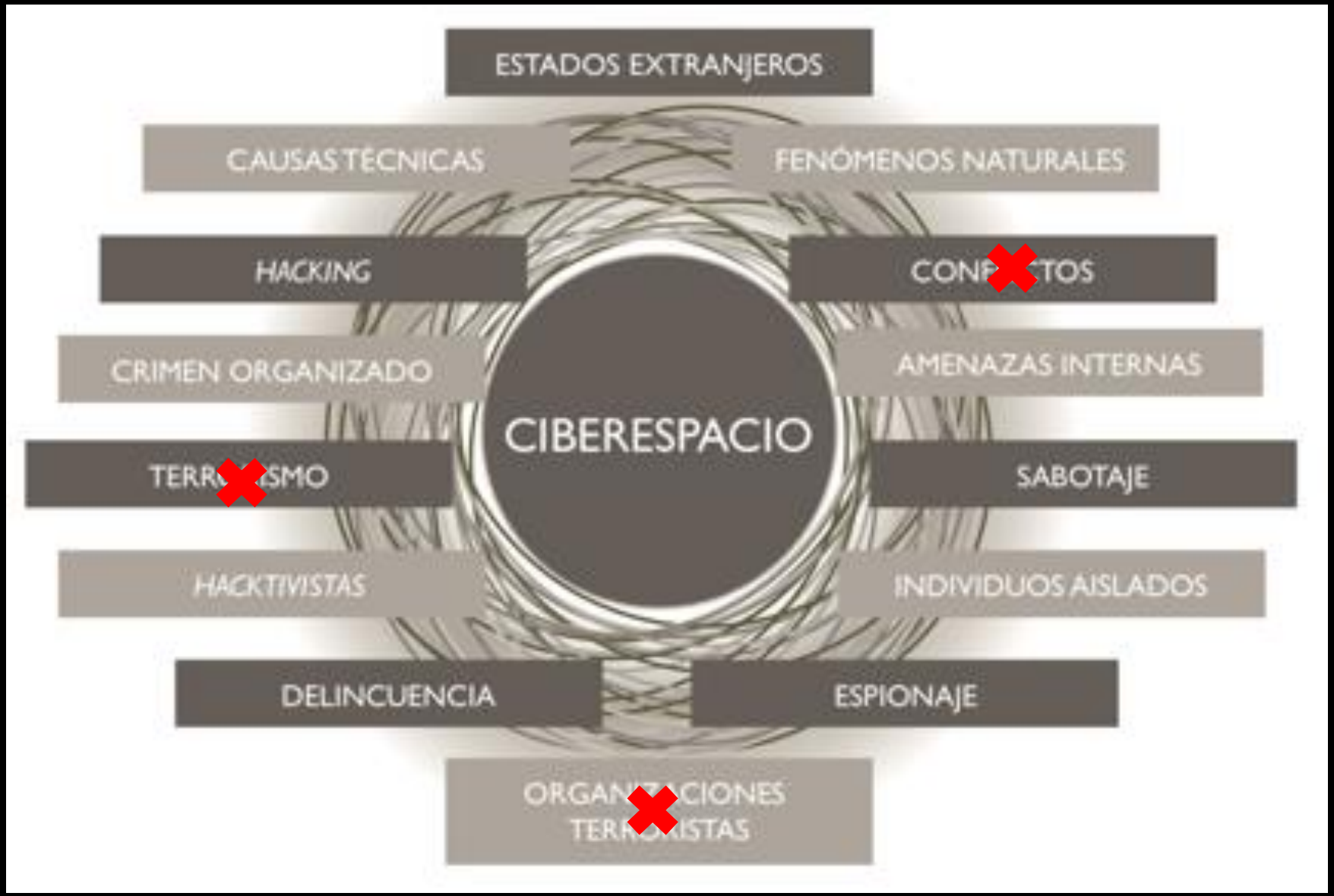

INSIDERS

Principales Vectores de Ataque

- Puntos de venta (Malware, Sniffing, aprobaciones fraudulentas, ataques MiTM).
- Números de Tarjetas (Especialmente casos HALF-EMV).
- Vulnerabilidades en la banca en línea.
- Robo de semillas de Tokens.
- Phishing & ingeniería social.
- Bases de datos.
- Sistemas (CRM, cajas, Core banking, Etc.).
- SPEI, SWIFT, Procesadores de pagos… entre otros.


Riesgo
Vulnerabilidad
Impacto
Amenaza
Intención
Oportunidad
Capacidad


Resource
What are you trying to protect?
Threat
What are you afraid of happening?
Vulnerability
How could the threat occur?
Mitigation
What is currently reducing the risk?
Impact
What is the impact to the business?
Probability
How likely is the threat given the controls?
Threat Priority



Fuente: Estrategia Nacional de Ciberseguridad 2013 – Gobierno Español.

CIBERAMENAZAS Y ACCIONES QUE USAN EL CIBERESPACIO CON FINES MALICIOSOS

Disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos.
La acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas.

CIBERESPIONAJE

Amenazas
Persistentes
Avanzadas

AMENAZAS HÍBRIDAS

Acciones militares
Ciberataques
Manipulación de
la información

CIBERCRIMEN

Ciberterrorismo
Ciberdelito

HACKTIVISMO

Ciberataques

Fuente: Estrategia Nacional de Ciberseguridad 2019 – Gobierno Español.

...san el ciberespacio como medio para realizar actividades ...

CIBERESPIONAJE

Amenazas
Persistentes
...azadas

AMENAZAS HÍBRIDAS

Acciones militares
Ciberataques
Manipulación de
la información

CIBERCRIMEN

Ciberterrorismo
Ciberdelito

HACKTIVISMO

Ciberataques

Fuente: Estrategia Nacional de Ciberseguridad 2019 – Gobierno Español.

PRINCIPIOS RECTORES

01 Unidad de Acción

Toda respuesta ante un incidente en el ámbito de la ciberseguridad que pueda implicar a distintos agentes del Estado se verá reforzada si es coherente, coordinada y se resuelve de manera rápida y eficaz, cualidades alcanzables a través de la adecuada preparación y articulación de la unidad de acción del Estado.

02 Anticipación

La especificidad del ciberespacio y de los actores implicados demanda que existan mecanismos de anticipación en organismos especializados, que orienten la Acción del Estado en situaciones de crisis.

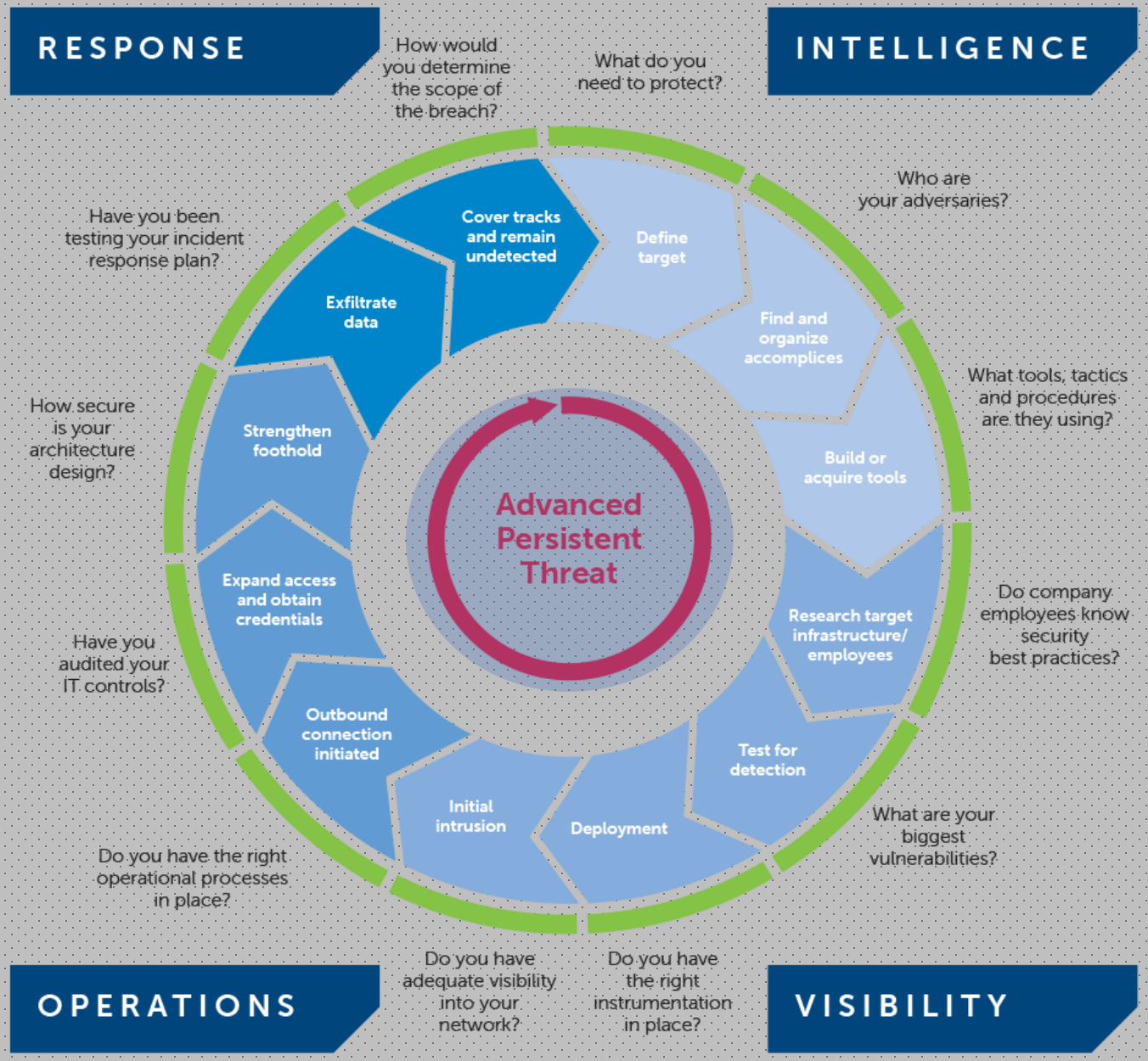
03 Eficiencia

La ciberseguridad precisa del empleo de sistemas multipropósito de gran valor y elevado nivel tecnológico, que llevan asociadas unas necesidades muy exigentes y un alto coste derivado de su desarrollo, adquisición y operación.

04 Resiliencia

La resiliencia es una característica fundamental que deben poseer los sistemas e infraestructuras críticas. El Estado está obligado a asegurar la disponibilidad de los elementos que se consideren esenciales para la nación, mejorando su protección contra las ciberamenazas.

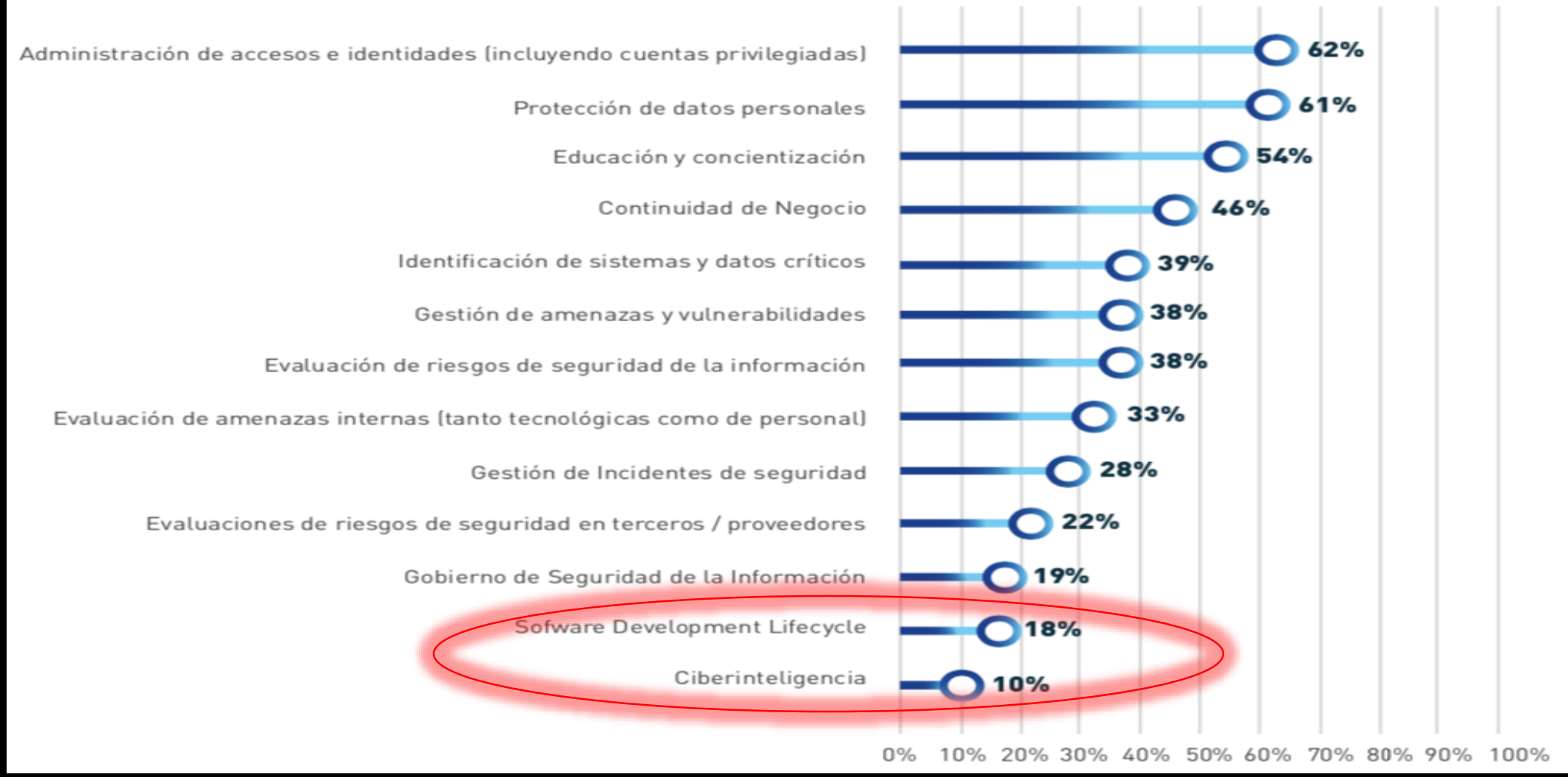
y... nosotros?


RESPONSE
How would you determine the scope of the breach?
What do you need to protect?
INTELLIGENCE
Have you been testing your incident response plan?
Who are your adversaries?
Cover tracks and remain undetected
Define target
Exfiltrate data
Find and organize accomplices
How secure is your architecture design?
What tools, tactics and procedures are they using?
Strengthen foothold
Build or acquire tools
Advanced Persistent Threat
Expand access and obtain credentials
Research target infrastructure/ employees
Have you audited your IT controls?
Do company employees know security best practices?
Outbound connection initiated
Test for detection
Initial intrusion
Deployment
Do you have the right operational processes in place?
What are your biggest vulnerabilities?
Do you have adequate visibility into your network?
Do you have the right instrumentation in place?
OPERATIONS
VISIBILITY

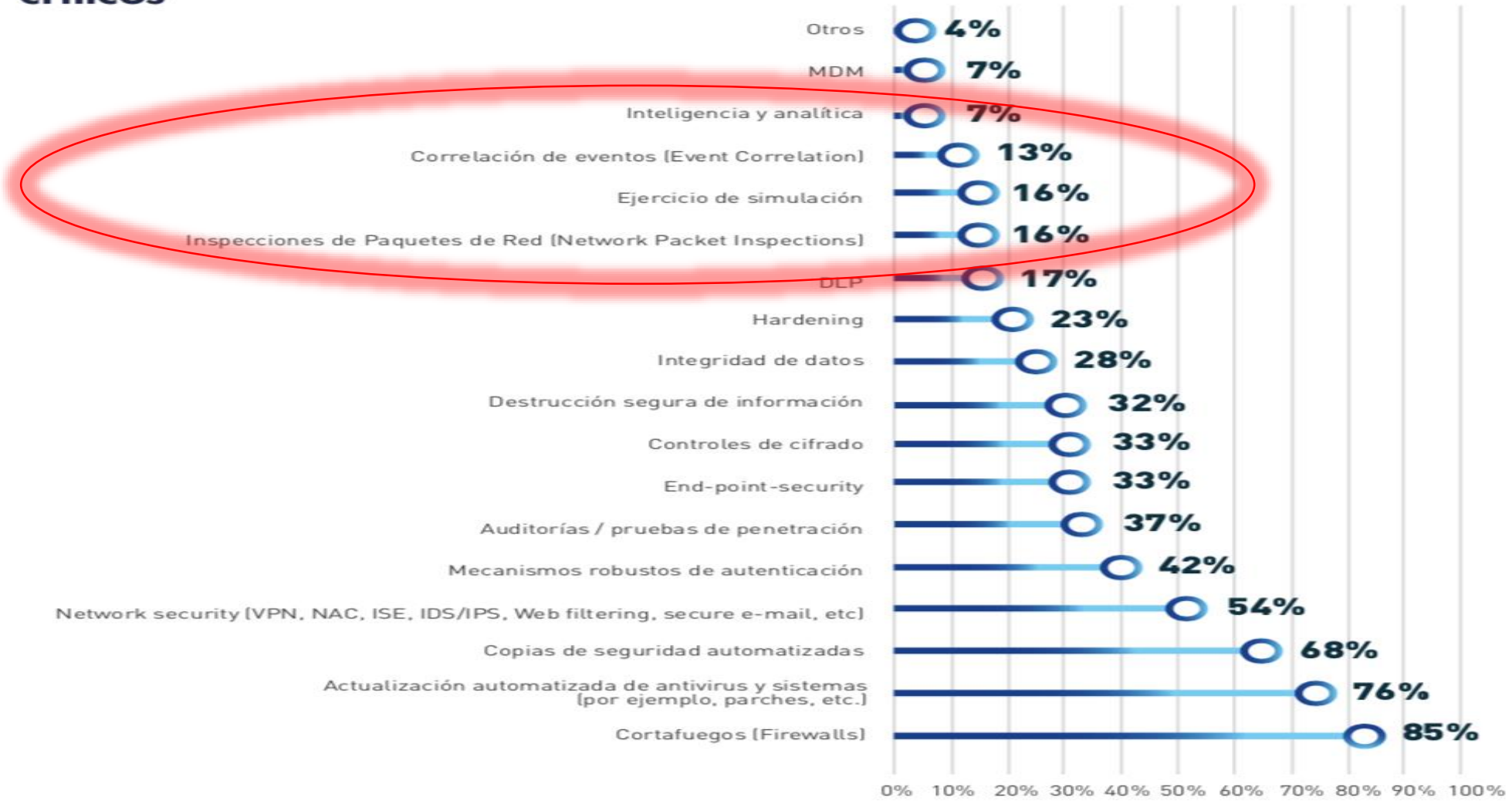

CYBERSECURITY
STOP

ACTITUD 101

Gráfica 14. Procesos / programas respecto a la seguridad digital implementados actualmente por las entidades e instituciones financieras



Gráfica 13. Acciones y medidas técnicas de seguridad de la información (incluyendo ciberseguridad) para proteger los sistemas de información críticos



Recuerdan?

Ellos ya están detrás del

FIREWALL

IDENTIFICACIÓN

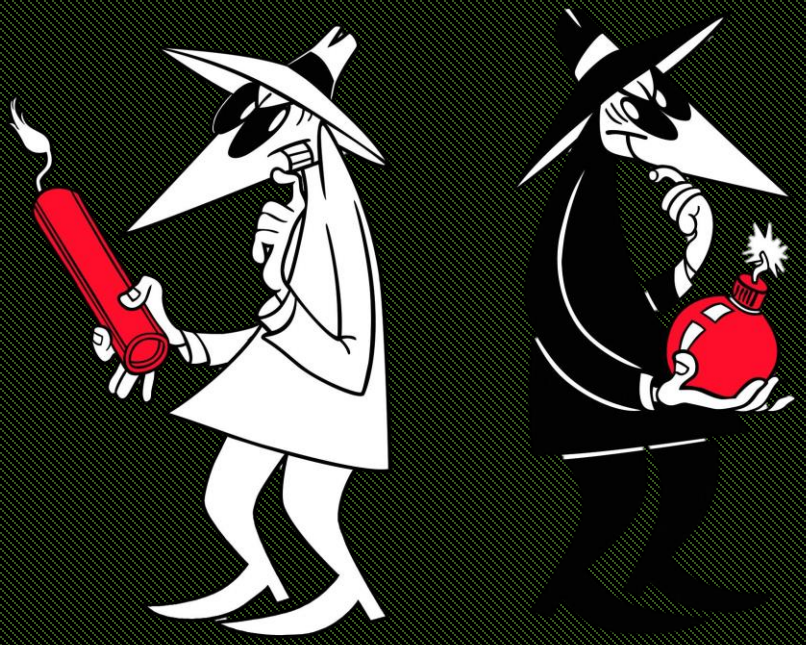
no se puede identificar lo que no se ve

CONTENCIÓN

no se puede detener lo que no se conoce

CAMBIO DE POSTURA

Reactivo + Damage Control → Preventivo → PREDICTIVO



CONCLUSIONES

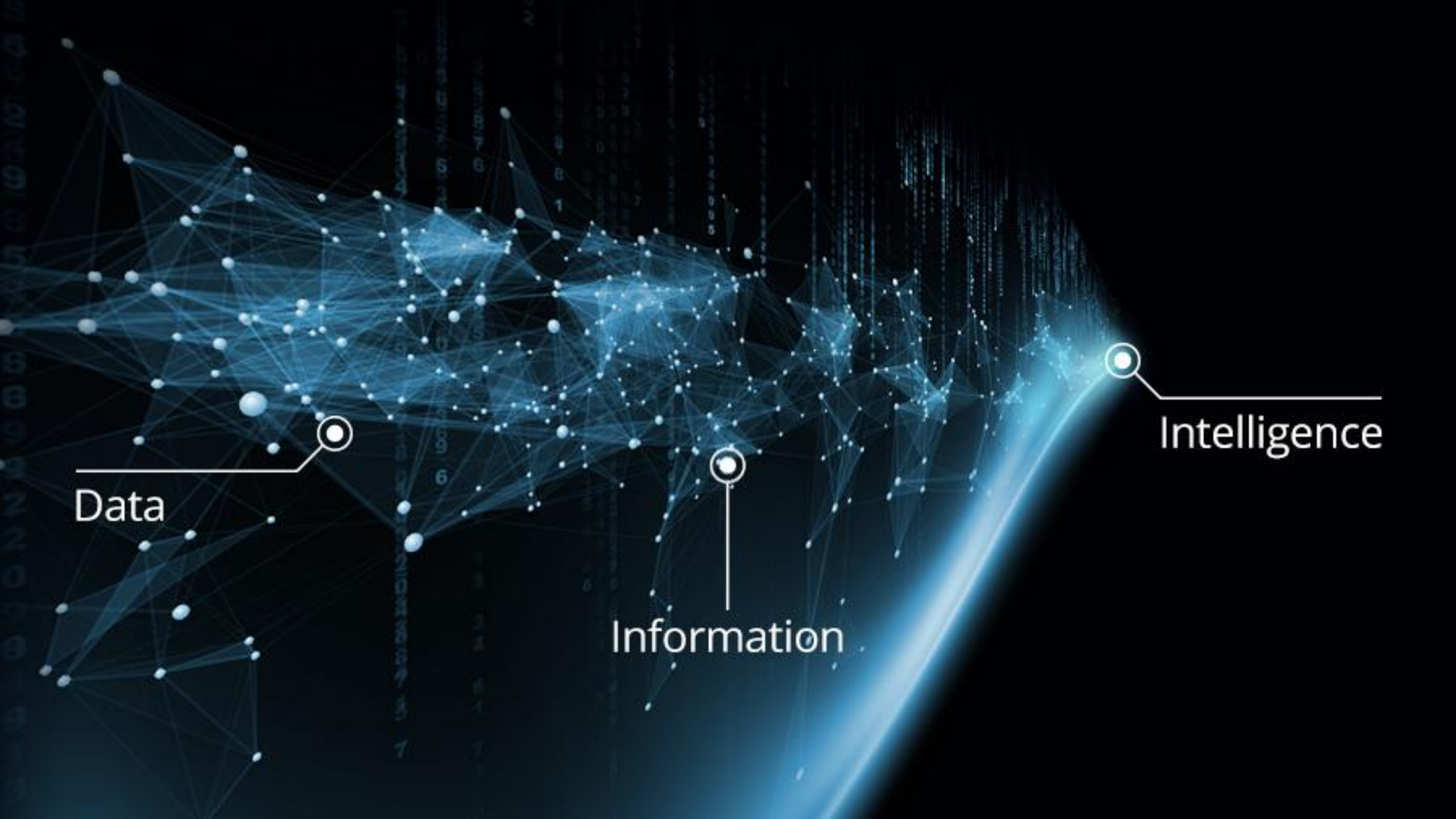
ANTICIPAR REQUIERE:

gestión de riesgos (modelado de amenazas y evaluación de madurez)

tener visibilidad (red, Hosts, flujos de datos)

contar con inteligencia de amenazas interna y externa

resolver el problema de origen (seguridad en el desarrollo de sw)


Data
Information
Intelligence

CAMBIO DE CULTURA - CONSCIENCIA - ENTRENAMIENTO...

GRACIAS

tekium.mx:/home/ciberseguridad:$ cat ./expositor.txt

Enrique Vaamonde M. - @_ejvm - ev@tekium.mx