CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

BC CR BANCO CENTRAL DE COSTA RICA

BANCO DE ESPAÑA
Eurosistema

SEMINARIO SOBRE GESTIÓN DOCUMENTAL Y DE ARCHIVOS EN LOS BANCOS CENTRALES

Ciberseguridad y protección de la información

Álvaro G. Jaikel ajaikel@smartgovern.cr
Cel +506 8390-6397

22-11-04, Sesión 9

OBJETIVOS GENERAL Y ESPECÍFICOS DE PRESENTACIÓN

Objetivo general: Ofrecer un vistazo al estado global de la ciberseguridad y cómo puede afectar la seguridad de los activos de nuestras instituciones, entendiendo la ciberseguridad como un elemento del sistema de seguridad de la Información.

Objetivos específicos:

1. Revisar el estado de la ciber seguridad a nivel mundial.
2. Comprender la diferencia entre ciberseguridad y otros términos utilizados en la seguridad de la información.
3. Reiterar la importancia de incorporar estos conceptos en las responsabilidades de los **gestores documentales**.
4. Tendencias en ciber seguridad para los bancos centrales.

TEMARIO DE LA CHARLA: "CIBER SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN

1. Definiciones relacionadas con la ciber seguridad
2. Informe del ciber riesgos en bancos centrales
   a. Principales amenazas a la ciber seguridad
   b. Panorama de la ciber seguridad en los bancos centrales
   c. Evaluación de ciber riesgos en el sector financiero
   d. Conclusiones del informe
3. Gestión de riesgos y controles cibernéticos
4. Pilares de la seguridad de la información
5. Lecciones aprendidas

FSB DEFINICIONES DEL “CYBER LEXICOM”

TÉRMINOS	DEFINICIONES
Activos	Algo de valor tangible o intangible que debe ser protegido, incluyendo gente, información, infraestructura, finanzas y reputación.
Ciber	Relacionado con, dentro de, o a través de medios de conectividad de infraestructura de la información por interacciones de personas, procesos, datos y sistemas de información.
Ciber resiliencia	La habilidad de una organización para llevar a cabo su misión, anticipando y adaptándose a las ciber amenazas y otros cambios relevantes del entorno para soportar, contener y recuperarse rápidamente de un ciber incidente.
Ciber seguridad	Preservación de la confidencialidad, integridad, autenticación y disponibilidad de la informción o de los sistemas de información, a través de ciber medios.

OTRAS DEFINICIONES RELACIONADAS CON SEGURIDAD

DEFINICIÓN DE CIBERSEGURIDAD, SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

CIBERSEGURIDAD

Es la **práctica de defender**, con tecnologías o prácticas ofensivas, las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos **de ataques maliciosos.**

SEGURIDAD INFORMÁTICA

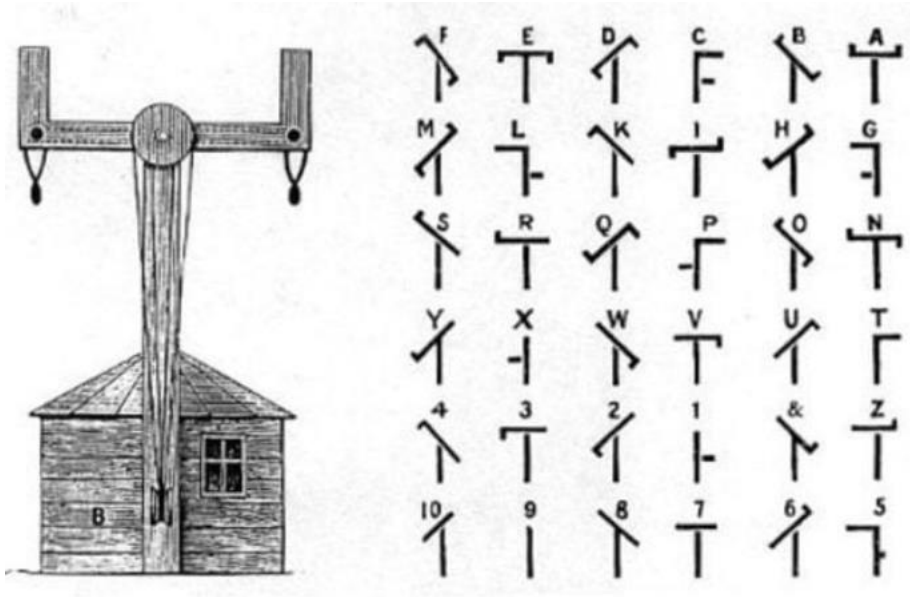
Es la disciplina que se encarga de **proteger la integridad y la privacidad** de la información almacenada en el sistema informático de cibercriminales.

SEGURIDAD DE LA INFORMACIÓN

Es el conjunto de **medidas preventivas y reactivas** que afectan al tratamiento de los datos almacenados y que permiten almacenar y proteger la información.

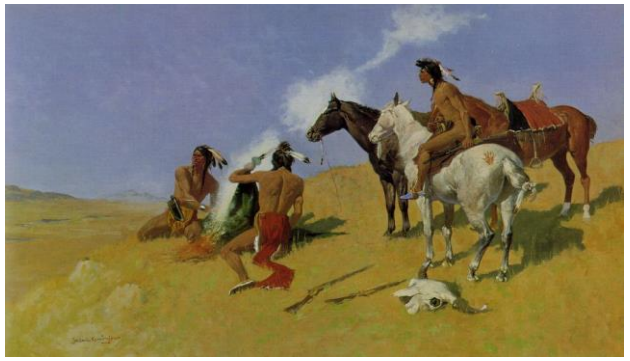
LISA Institute

ALGUNOS LO CONSIDERAN EL PRIMER CIBER ATAQUE



- Ocurrió en Francia en 1834,
- En telégrafo óptico de Claude Chappe 1790,
- Consistió en puestos de torres de transmisión con brazos móviles, visibles con telescopio desde las adyacentes, utilizado por el gobierno,
- Como los datos de los mercados locales y externos tardaban días en llegar, sobornaron a los operadores para que filtraran información de su interés y aprovecharse de estas primicias.
- Perpetrado por los banqueros François y Joseph Blanc, con un carácter clave que invalidaban,
- Se descubrió la trama por el sustituto de un operador que enfermó,
- No hubo condena por carencia de tipificación del hecho como delito.

TELECOMUNICACIONES DEL PASADO



PÁGINA DE CIBER AMENAZAS EN TIEMPO REAL

https://cybermap.kaspersky.com/es

REGIÓN	CIBERATAQUES SEMANALES POR ORGANIZACIÓN (X)	INCREMENTO ANUAL ENTRE IIIT 2021-2022
África	1,758	3%
Asia	1,684	25%
Latino América	1,602	29%
Europa	963	26%
ANZ	937	82%
América del Norte	854	54%

Fuente: Check Point informe estadístico para ciberseguridad

ESTADÍSTICAS DE CIBER RIESGOS EN BANCA CENTRAL

BIS

BIS Working Papers
No 1039

Cyber risk in central banking

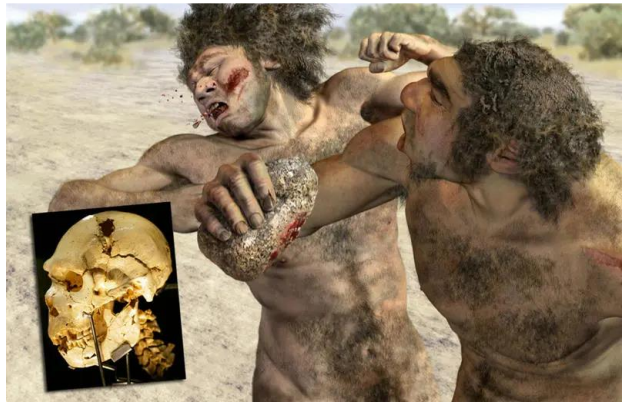
by Sebastian Doerr, Leonardo Gambacorta,
Thomas Leach, Bertrand Legros and David Whyte

Monetary and Economic Department

September 2022

JEL classification: E5, E58, G20, G28.

Keywords: cyber risk, central banks, financial institutions, cloud services, cyber regulation.



DEFINICIONES BREVES PARA LOS GRÁFICOS

- **AEs** (Advanced Economies) representan a las economías consideradas como avanzadas.
- **EMEs** (Emerging Market Economies) son las que imperan en los mercados emergentes.
- **BIG TECH** corresponde a los gigantes tecnológicos como Google, Amazon, Apple, Meta y Microsoft, grandes proveedores.
- **FINTECH** de Finance and Technology, son todas aquellas actividades que impliquen el empleo de la innovación y los desarrollos tecnológicos para el diseño, oferta y prestación de productos y servicios financieros.

PRINCIPALES CIBER INCIDENTES Y ORIGEN

- Phishing,
- Ataques de denegación de servicio,
- Ransomeware,
- Malware avanzado,
- Robo de identidad.
- Ataques a la cadena de suministros.

PERPETRADORES

- Crimen organizado,
- Agencias respaldadas por el Estado.
- Activistas,
- Internos.

SITIOS PARA APRENDER A HACKEAR Y ENTIDADES

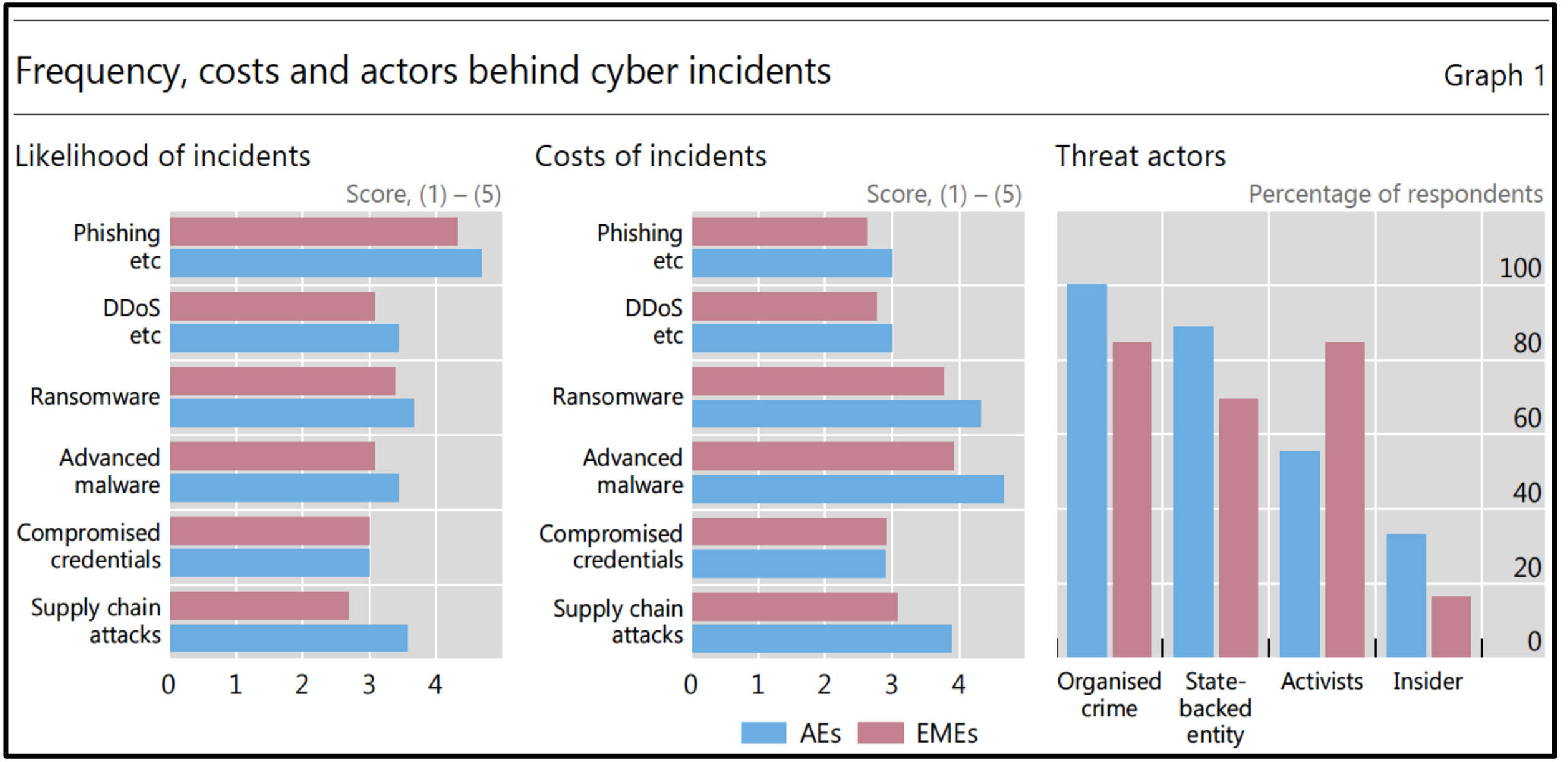
NOMBRES DE SITIOS

1. Pwn College
2. We Chall
3. Over The Wire
4. Smash The Stack
5. Crypto Pals
6. Google Gruyere APPSOT
7. Guyinatuxedo
8. CNIT 127
9. PWNABLE tw
10. PWNable xyz

GRUPOS DE HACKERS

1. Conti
2. globalHell
3. Los iraníes Tarh Andishan
4. TeaMp0isoN
5. Chaos Computer Club (CCC)
6. Network Crack Program Hacker (NCPH)
7. Leven Seven Crew
8. Anonymous
9. LulzSec
10. Lizard Squad

PROBABILIDAD, COSTOS Y ACTORES DETRÁS DE LOS CIBER INCIDENTES

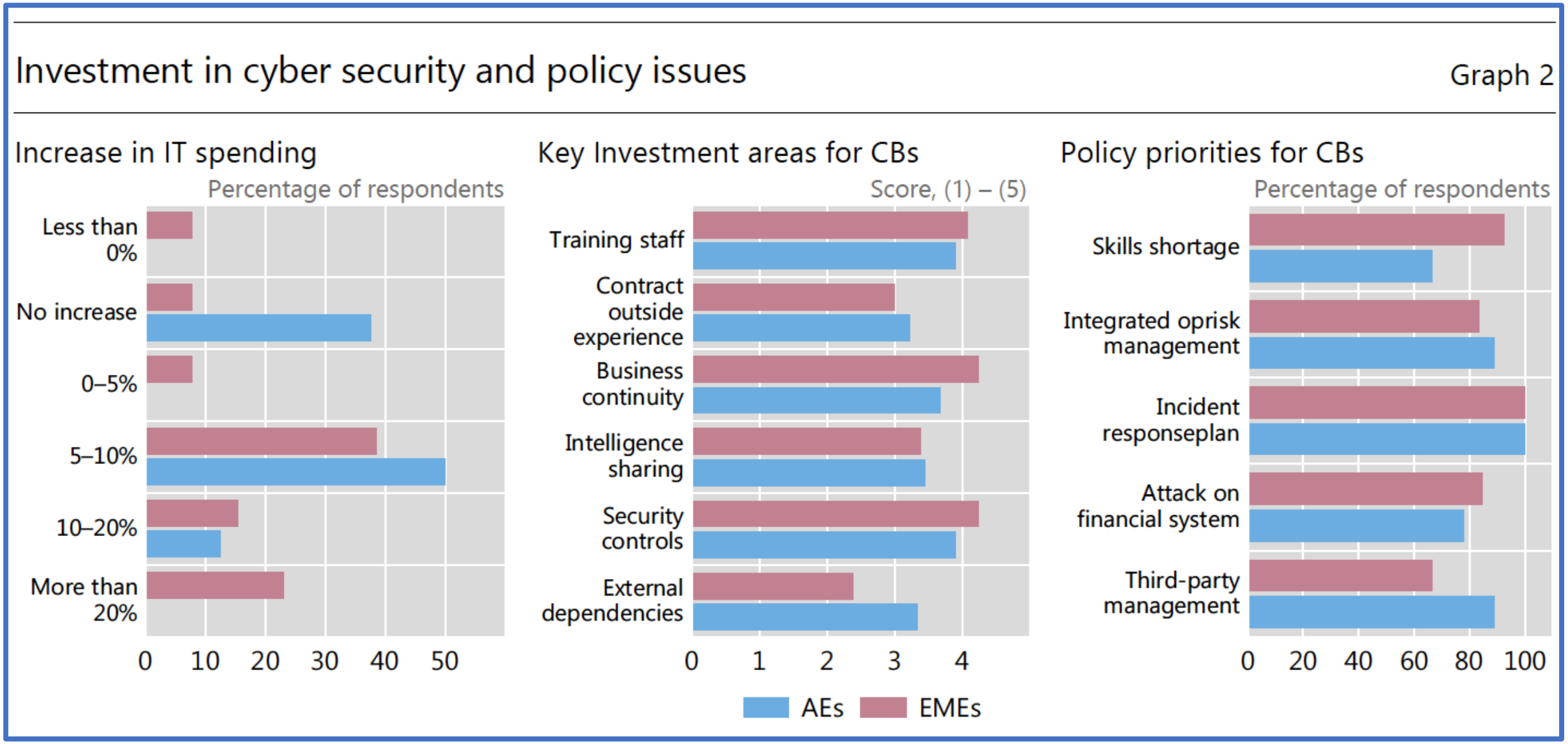


ÁREAS DE INVERSION Y ENFOQUES EN POLÍTICA DE BC

- Capacitación al personal,
- Tercerías de conocimiento especializado,
- Continuidad de negocio,
- Controles de seguridad
- Dependencias externas

- Escasez de idoneidad,
- Gestión integrada de riesgo operativo (oprisk),
- Respuesta a incidentes,
- Ataques al sistema financiero,
- Gestión de partes interesadas.

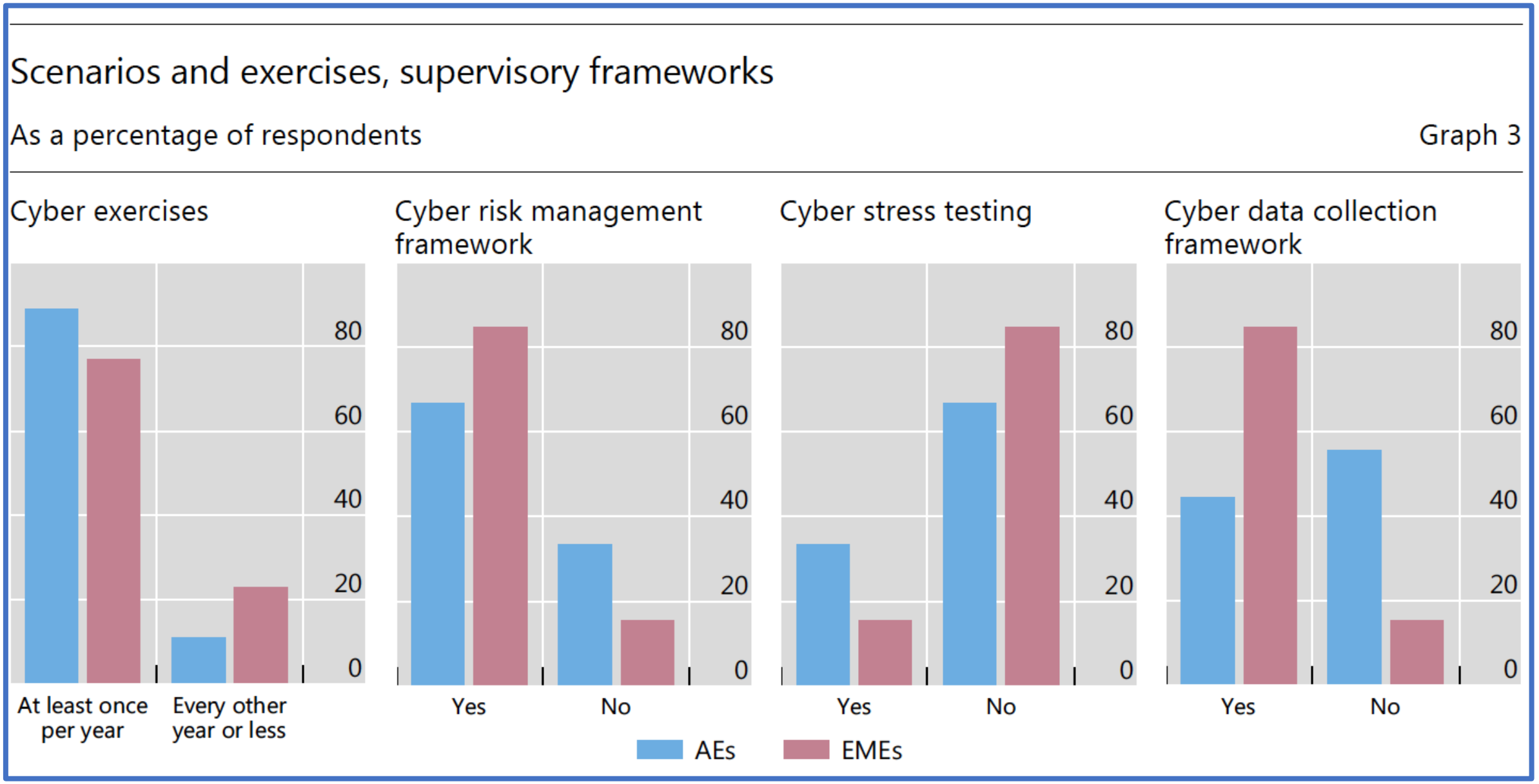
INVERSIONES EN CIBERSEGURIDAD Y POLÍTICAS



PREPARACIÓN PARA ENFRENTAR CIBER INCIDENTES

- Pruebas y simulacros,
- Marcos de referencia para abordar los ciber riesgos,
- Pruebas de estrés,
- Marcos de referencia para la recolección de ciber datos.

ESCENARIOS Y PRUEBAS, NORMAS REGULATORIAS (%)



ÁREAS DE INVERSION Y ENFOQUE EN POLÍTICA EN EL SF

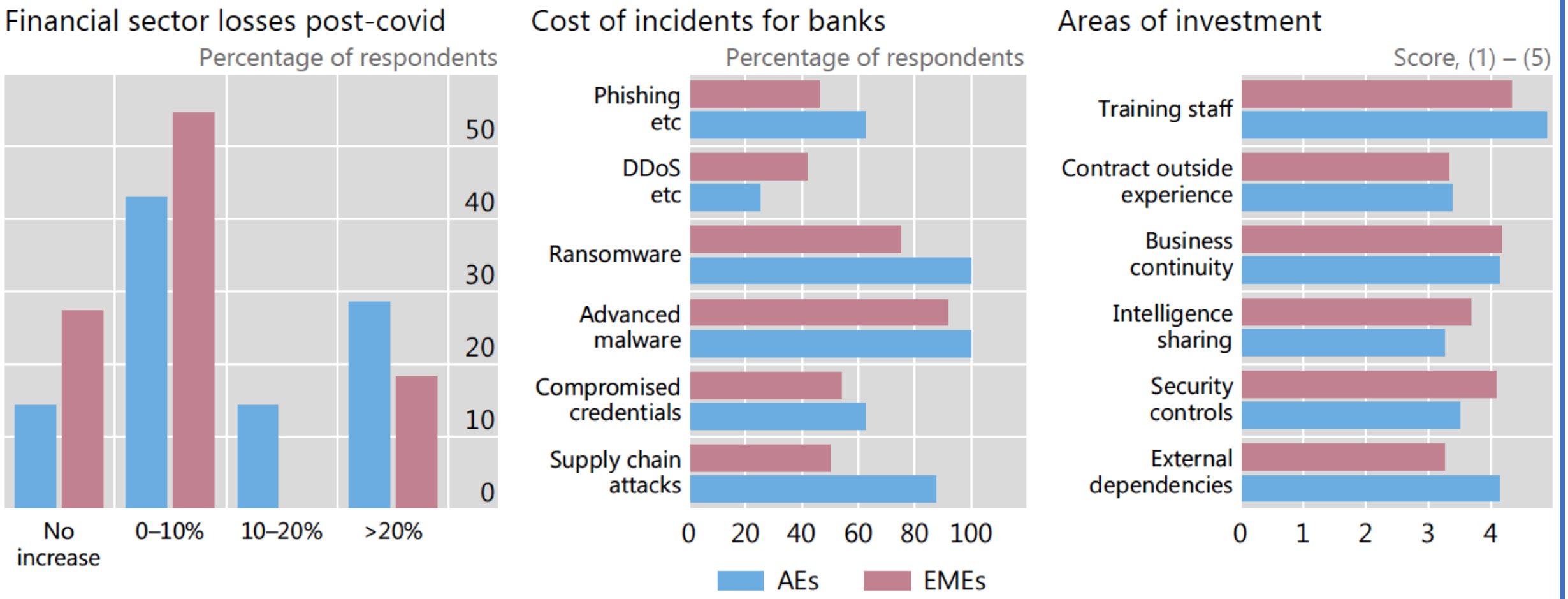
- Capacitación al personal,
- Tercerías de conocimiento especializado,
- Continuidad de negocio,
- Intercambio de inteligencia,
- Controles de seguridad,
- Dependencias externas.

- Escasez de idoneidad,
- Gestión integrada de riesgo operativo (oprisk),
- Respuesta a incidentes,
- Ataques al sistema financiero,
- Gestión de partes interesadas.

PÉRDIDAS, COSTO DE INCIDENTES E INVERSIONES EN EL SF

Cyber attacks and costs in the financial sector

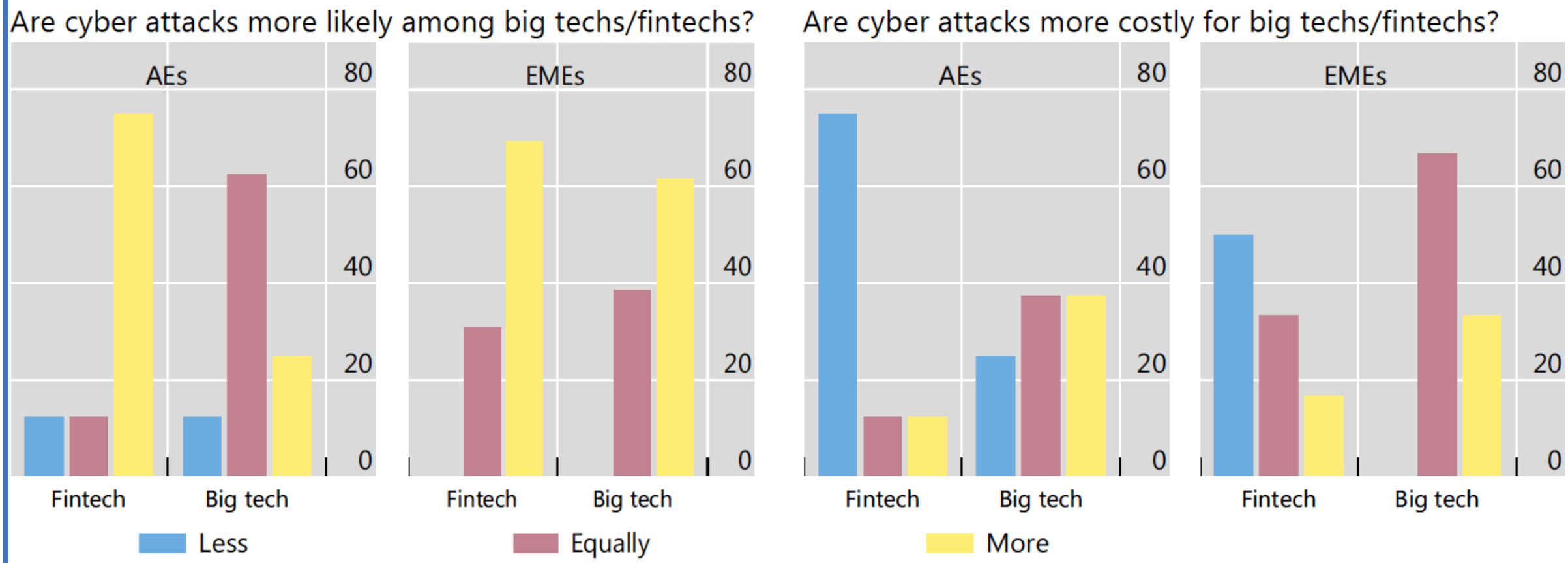
Graph 4



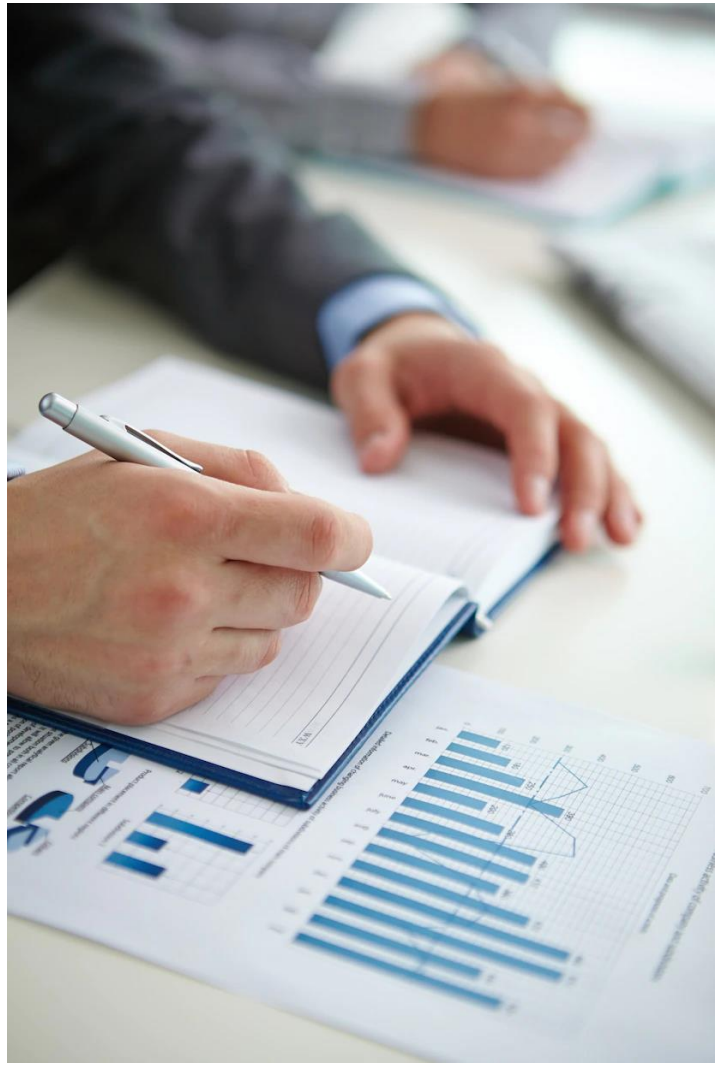
CIBER ATAQUES Y COSTOS ASOCIADOS (%)

Cyber attacks and associated costs: Financial institutions vs big techs and fintechs

As a percentage of respondents — Graph 5



CONCLUSIONES

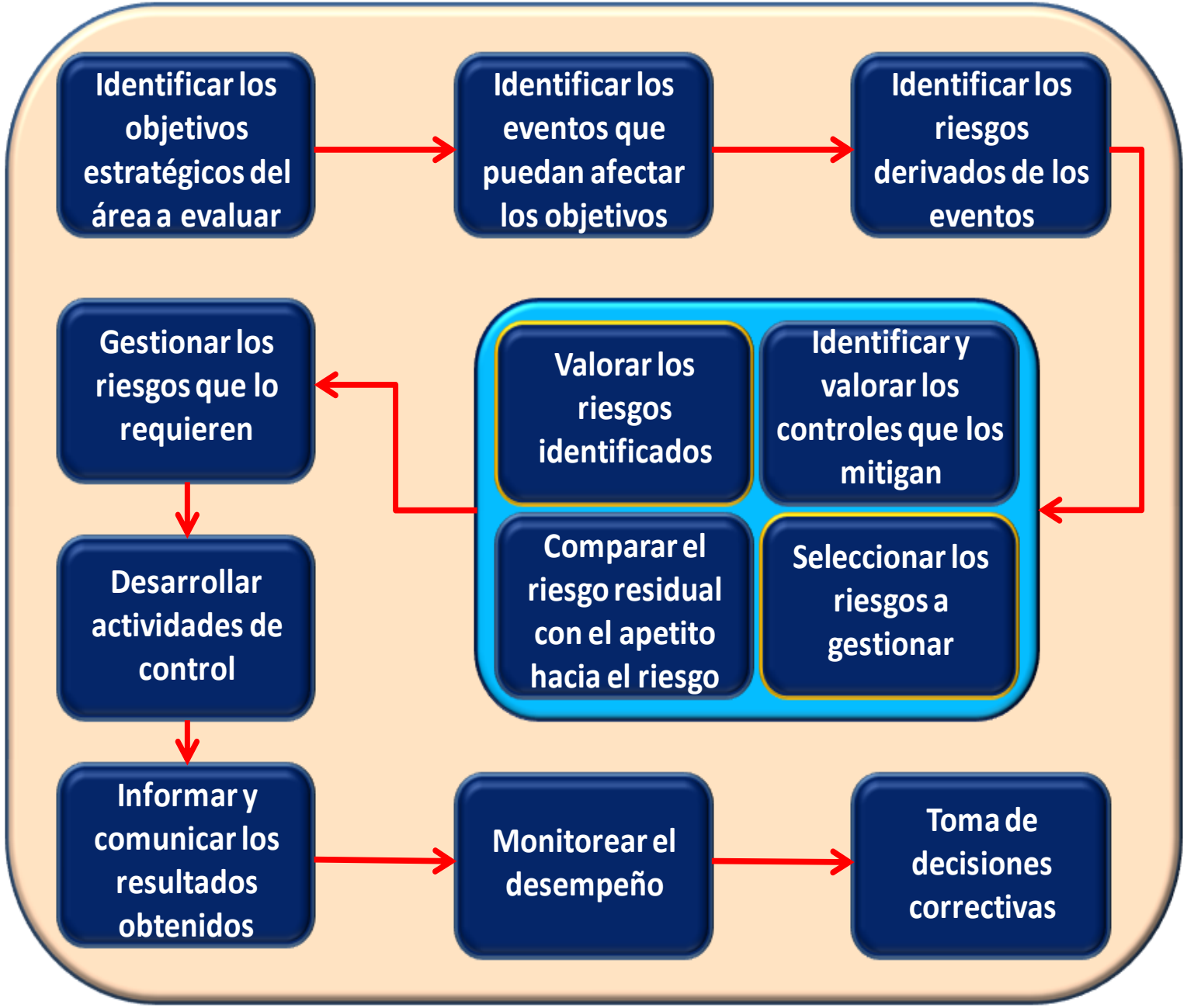


- Aumento de ciber ataques, cada vez más complejos y sofisticados, que se incrementan con migración a la nube y la adopción del teletrabajo.
- Mayor inversión en la gestión de ciberseguridad, riesgos, controles y resiliencia.
- Incremento de la cooperación local con alta participación interinstitucional, regional y global.
- Marcos de referencia y guías con mejores prácticas para la resiliencia por parte del G-7, Financial Stability Board, FSB, y el Bank for International Settlements, BIS.

BANCOS ATACADOS, NO SIEMPRE AFECTADOS

- Banco Central de Rusia
- Reserva Federal
- Banco Central de Nueva Zelanda
- Banco Central Europeo
- Banco Central de Zambia
- Banco Central de Bangladesh
- Banco de Israel

El ciclo de la gestión de riesgo, comprende y se sirve en forma exhaustiva del sistema de control interno



ALGUNAS PERSPECTIVAS PARA ASUMIR RIESGOS: CONSERVADORA, MEDIA Y TOMADORA DE RIESGOS

CONSERVADOR CONGRUENTE CON VALOR ESPERADO

0,9	0,09	0,27	0,45	0,63	0,81
0,7	0,07	0,21	0,35	0,49	0,63
0,5	0,05	0,15	0,25	0,35	0,45
0,3	0,03	0,09	0,15	0,21	0,27
0,1	0,01	0,03	0,05	0,07	0,09
	0,1	0,3	0,5	0,7	0,9

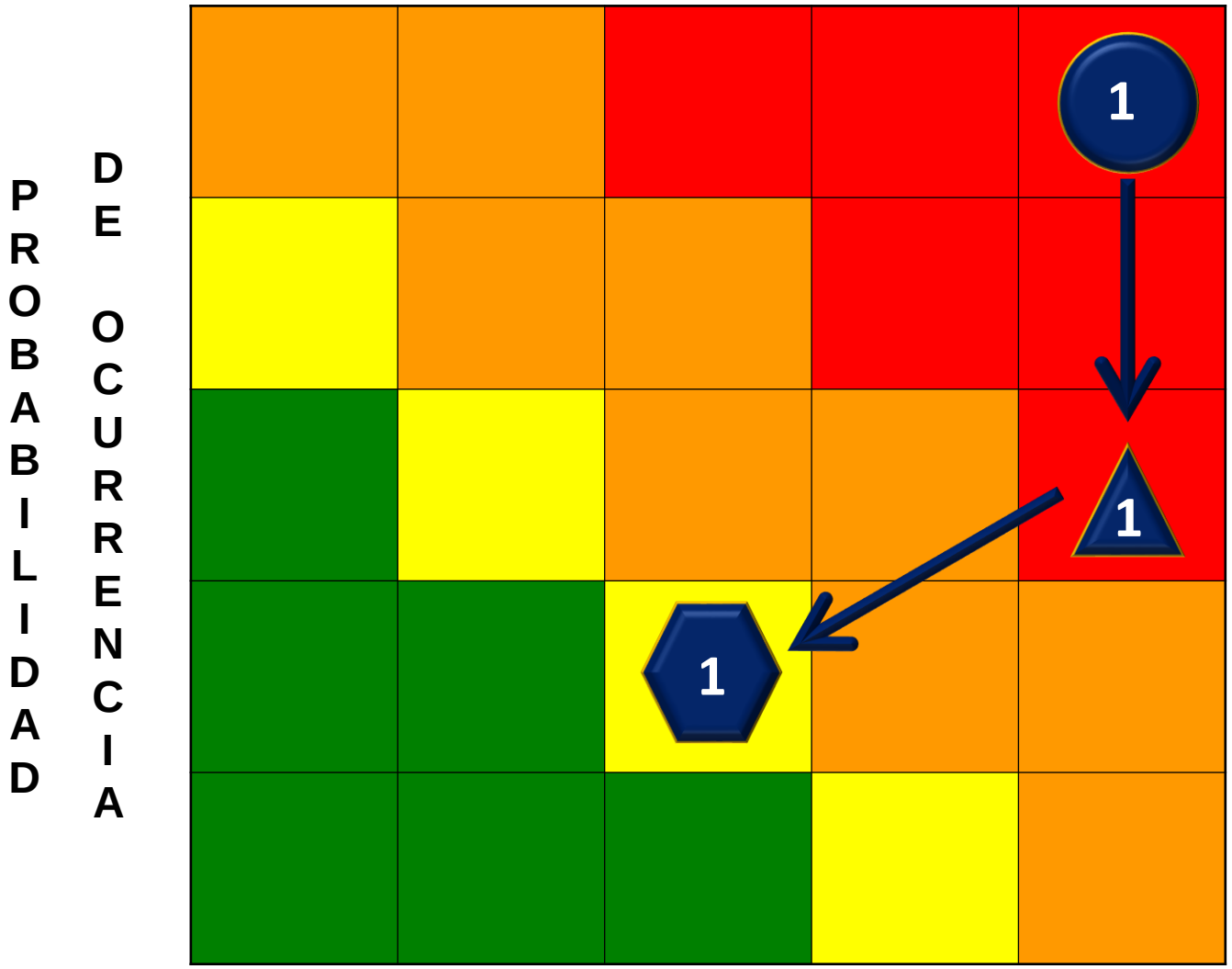
NORMAL O MEDIO, CONGRUENTE CON VALOR ESPERADO

0,9	0,09	0,27	0,45	0,63	0,81
0,7	0,07	0,21	0,35	0,49	0,63
0,5	0,05	0,15	0,25	0,35	0,45
0,3	0,03	0,09	0,15	0,21	0,27
0,1	0,01	0,03	0,05	0,07	0,09
	0,1	0,3	0,5	0,7	0,9

TOMADOR DE RIESGOS CONGRUENTE CON VALOR ESPERADO

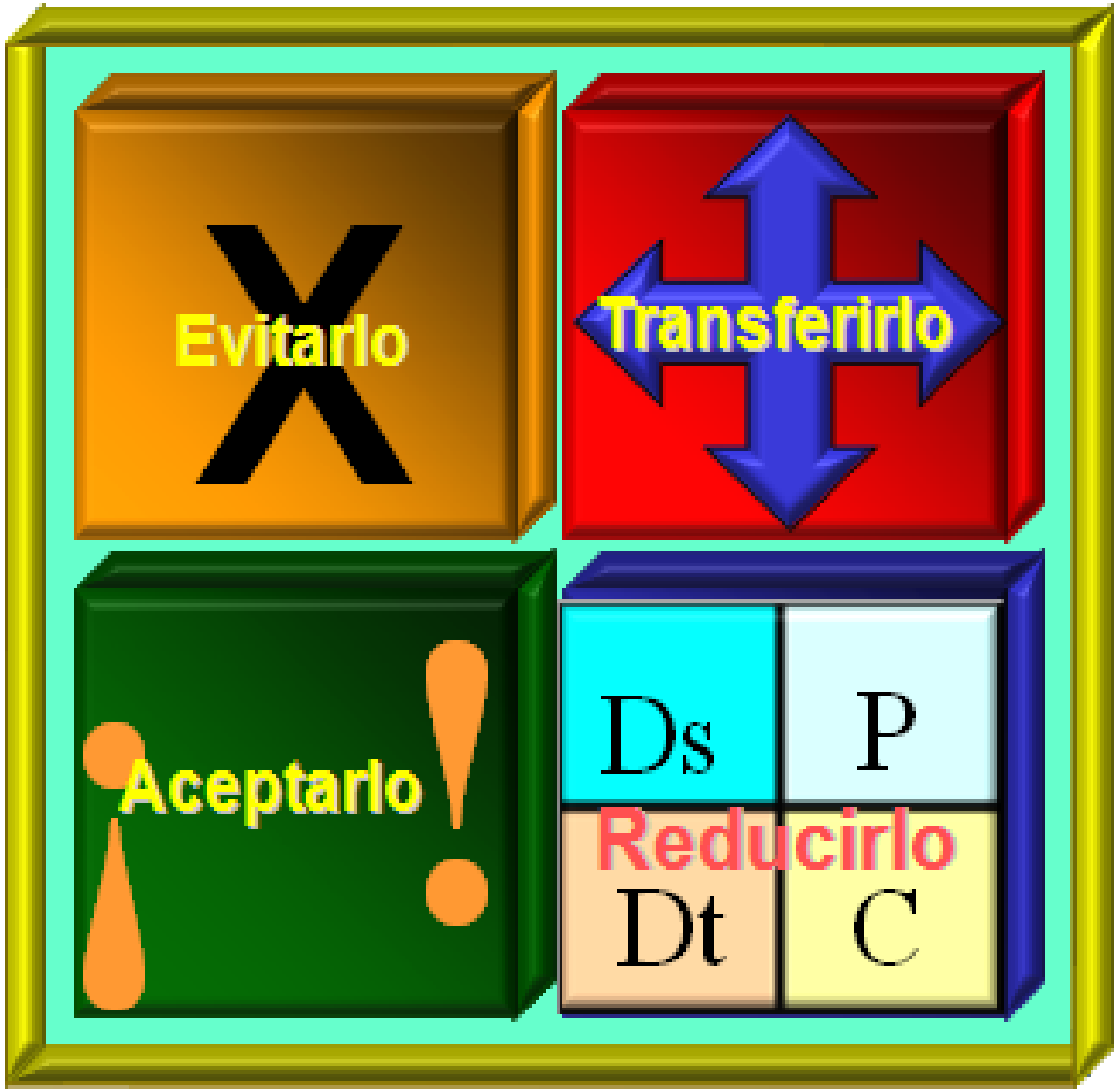
0,9	0,09	0,27	0,45	0,63	0,81
0,7	0,07	0,21	0,35	0,49	0,63
0,5	0,05	0,15	0,25	0,35	0,45
0,3	0,03	0,09	0,15	0,21	0,27
0,1	0,01	0,03	0,05	0,07	0,09
	0,1	0,3	0,5	0,7	0,9

VALORACION DE LOS RIESGOS DE LA ENTIDAD



RELACIÓN ENTRE RIESGO Y CONTROL

- Filosofía
- Apetito
- Tolerancia
- Riesgo inherente
- Riesgo residual
- Riesgo administrado
- Respuesta
- Cero tolerancia no es eliminar el riesgo



PILARES DE LA SEGURIDAD DIGITAL

1. **Confidencialidad:** Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.

2. **Integridad:** Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea requerido..

3. **Disponibilidad:** Los datos deben estar disponibles para los usuarios donde, cuando y como sea necesario.

4. **Autenticación:** Estás realmente comunicándote con los que piensas que te estás comunicando. Es quien dice ser?

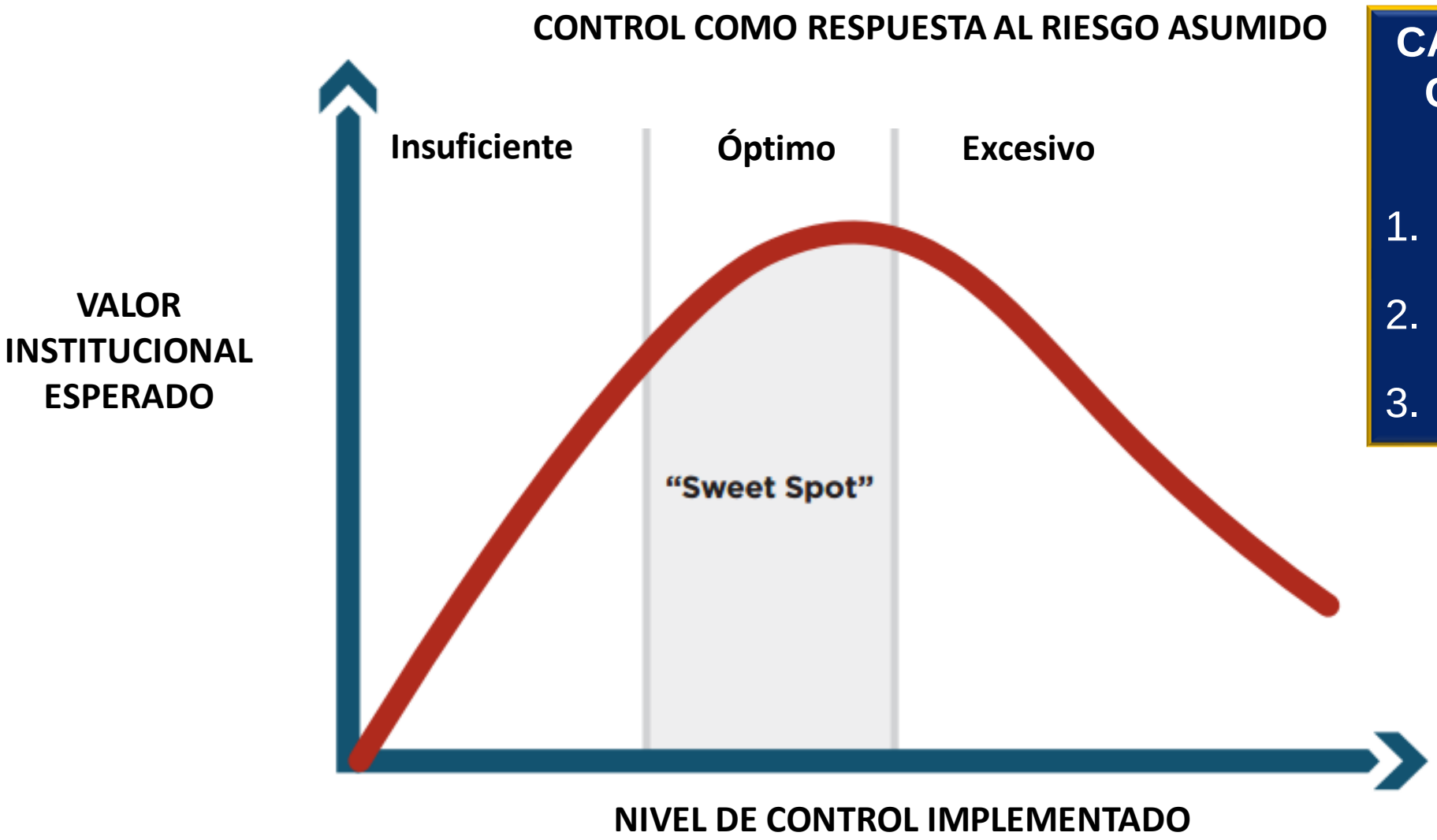
TIPOS Y UBICACIONES DE LOS CONTROLES

TIPOS DE CONTROLES

- Disuasivos
- Preventivos
- Detectivos
- Correctivos

MUESTRA DE UN CONTROL DISUASIVO

CAPACIDAD DEL CONTROL PARA GENERAR VALOR



CARACTERÍSTICAS DE LOS CONTROLES EFECTIVOS

1. Pertinentes
2. Maduros
3. Aplicados a todos

LECCIONES APRENDIDAS

1. Es nuestra responsabilidad el implementar los controles suficientes para responder a los riesgos directos que enfrentemos en nuestro trabajo;
2. La ingeniería social se puede generar aunque no nos percatemos de ello;
3. El entorno en el que efectuemos teletrabajo debe ofrecer la ciber seguridad definida por la entidad;
4. El respeto por las clasificaciones de la información es fundamental para mantener la confianza y el prestigio institucional;
5. Aprenda, participe y aplique las iniciativas de ciber seguridad implementadas por la entidad.

CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

BC CR BANCO CENTRAL DE COSTA RICA

BANCO DE ESPAÑA
Eurosistema

SEMINARIO SOBRE GESTIÓN DOCUMENTAL Y DE ARCHIVOS EN LOS BANCOS CENTRALES

Ciberseguridad y protección de la información

Álvaro G. Jaikel ajaikel@smartgovern.cr
Cel +506 8390-6397

22-11-04, Sesión 9