La Ciberseguridad desde las personas

Miguel Angel Aranguren Romero

CISA, CISM, CGEIT, CRISC, CISSP, ITIL, COBIT, OSCP, CDPSE, DATA SCIENCE SP
APMG Certified Trainer CISA, CISM, CGEIT, CRIS, CDPSE

PRESIDENTE ISACA BOGOTA

GIT
Governance | Risk | Compliance | Audit

A PESAR DE TODOS LOS CAMBIOS, UNA CONSTANTE EN CIBERSEGURIDAD

	2012	2017	2022
MEGATENDENCIA	Movilidad/BYOD	Nube	Trabaja desde cualquier lugar
RIESGOS CIBERNÉTICOS DOMINANTES	Violaciones de datos, robo de tarjetas de pago, espionaje, cumplimiento	Ransomware automatizado, troyanos bancarios	Big game ransomware, BEC, renuncias que se llevan datos
MAYOR RIESGO	**PERSONAS** "La mayoría de los principales ciberataques a corporaciones estadounidenses utilizan ingeniería social" The Washington Post	**PERSONAS** El 94 % del malware llega a través del correo electrónico y el phishing está involucrado en la mayoría de las infracciones. verizon DBIR	**PERSONAS** El 85% involucró un elemento humano, solo el 3% involucró una vulnerabilidad técnica verizon DBIR

LOS 3 PRINCIPALES RIESGOS DE CIBERSEGURIDAD: CENTRADOS EN TODAS LAS PERSONAS

85%

INVOLUCRA UN ELEMENTO HUMANO

La gran mayoría de los ataques de ransomware comienzan con el correo electrónico

- investiga paloalto NETWORKS

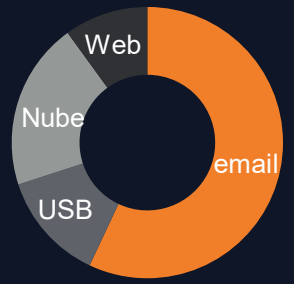
Las pérdidas de BEC superan todas las demás pérdidas de ciberseguridad combinadas

— datos de 791.790 incidentes

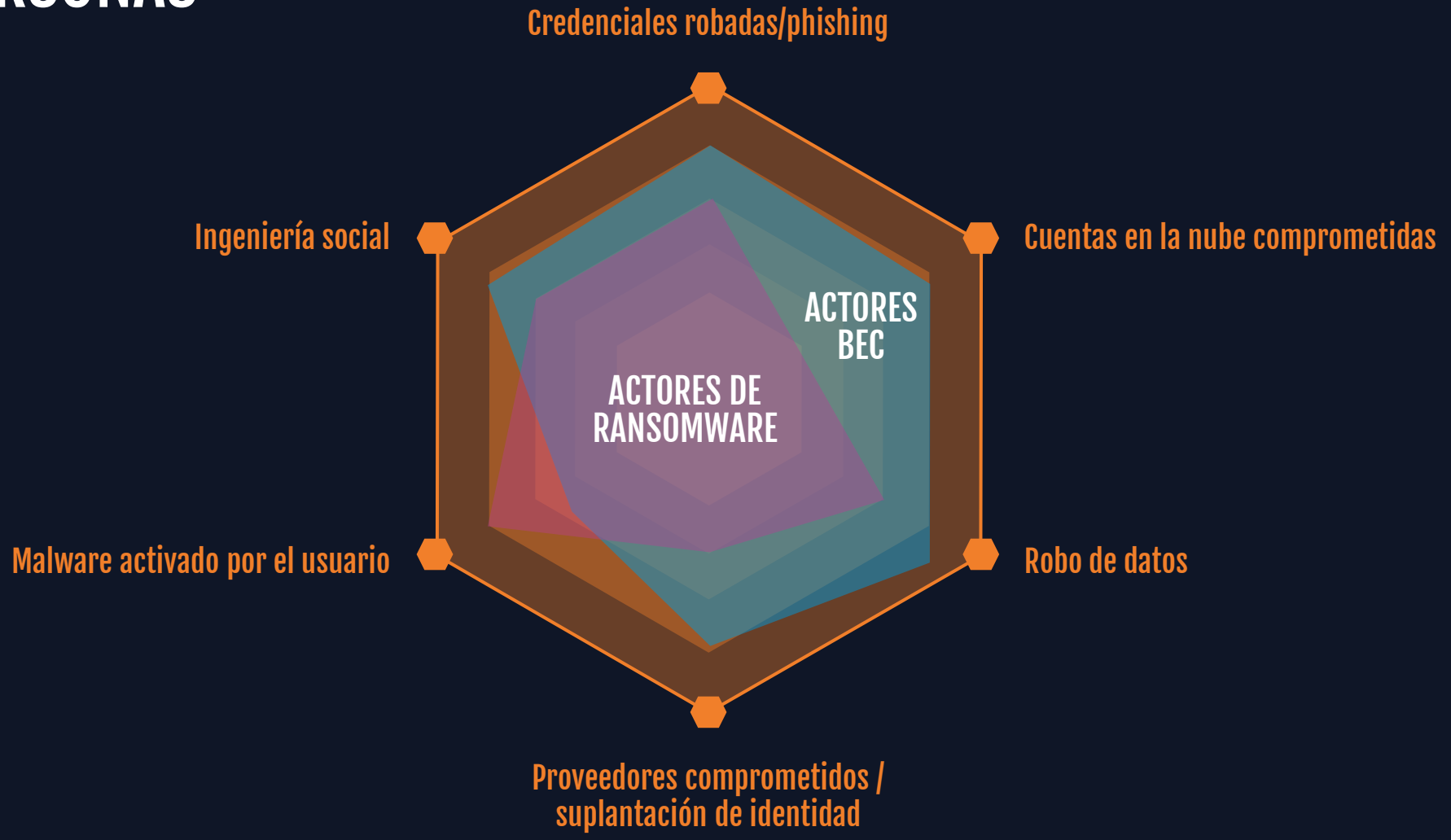
El 99% de los incidentes de pérdida de datos son provocados por humanos

— datos de **puntos de prueba** en 3000 organizaciones

proofpoint.

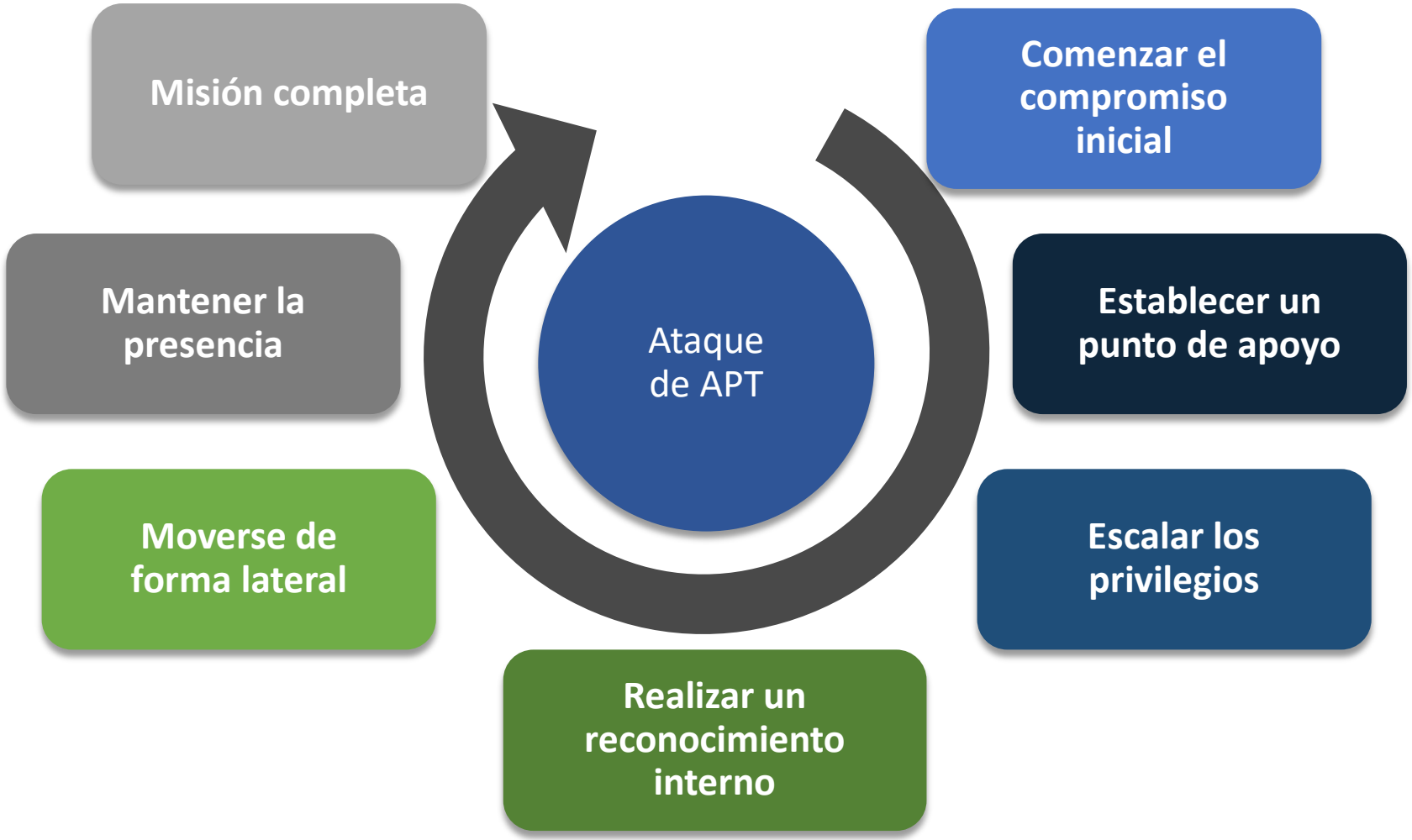


LA PLATAFORMA DEL ATACANTE PARA LA EXPLOTACIÓN CENTRADA EN LAS PERSONAS



Amenazas persistentes avanzadas (APT)

Atacantes muy capacitados y avanzados que intentan explotar sistemas y redes.



Abordar las amenazas

Externas

Documentar todas las amenazas que pueden aplicarse a los sistemas y los procesos de negocio en revisión.

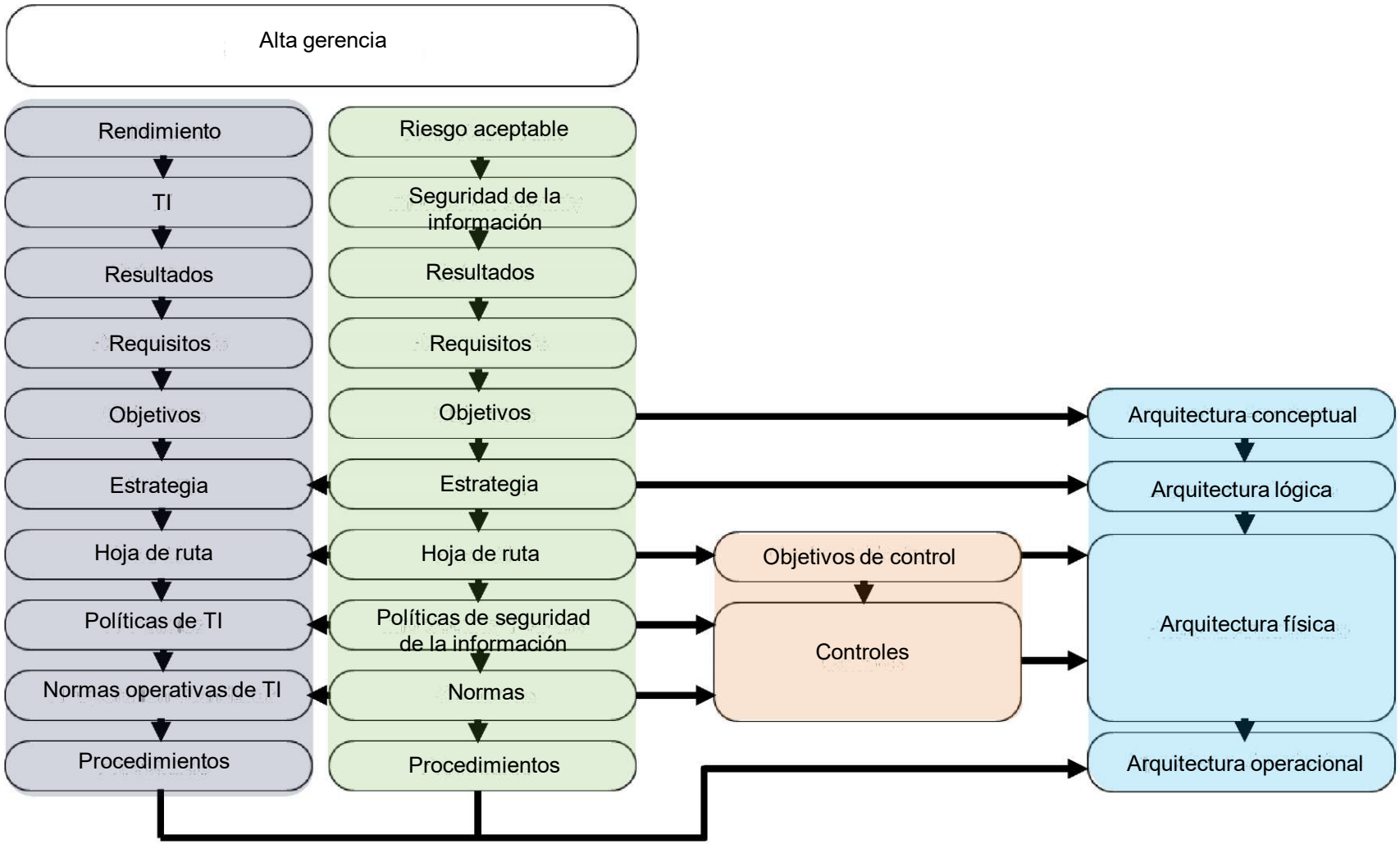
Examinar:

- Causas de fallos anteriores
- Informes de auditoría y de los medios de comunicación
- Información de los equipos de respuesta a emergencias informáticas (CERT)
- Datos de proveedores de seguridad
- Comunicación con grupos internos o de homólogos

Internas

- Aplicar de acuerdo con las funciones, privilegio mínimo y segregación de funciones
- Ser consciente de las personas internas de confianza
- Implementar una supervisión continua de todos los sistemas del negocio.
- Señalar comportamientos anómalos con la inteligencia artificial y aprendizaje automático

Relación de los elementos de gobierno



Participantes en el desarrollo de la estrategia de SI

Estado deseado

Denota una imagen completa de todas las condiciones relevantes en un momento futuro

- Principios, políticas y marcos
- Estructuras organizativas
- Cultura, ética y conducta
- Información
- Procesos
- Servicios, infraestructura y aplicaciones
- Personas, habilidades y competencias

Alinear la estrategia de seguridad con los requisitos del negocio

Mínimos necesarios

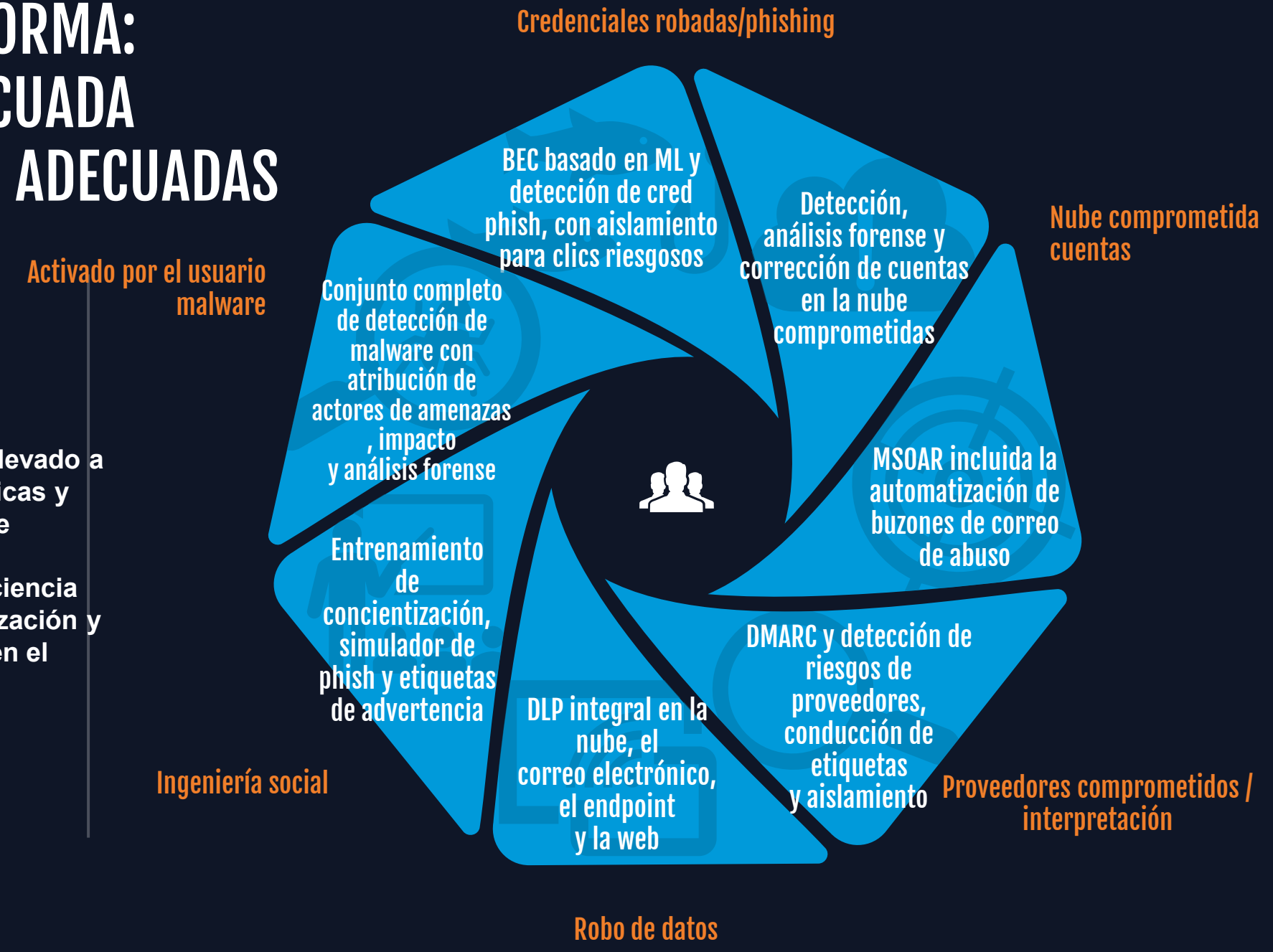
Para reducir el impacto de las interrupciones en la empresa, las organizaciones deben contar con estrategias y planes para garantizar lo siguiente:

- La protección y conexión de su fuerza laboral dinámica
- La eficacia de las comunicaciones
- La compresión de los impactos en el negocio
- La continuidad de las partes más importantes de la empresa
- La rápida recuperación de las áreas que se interrumpen

ENFOQUE DE PLATAFORMA: LA PROTECCIÓN ADECUADA PARA LAS PERSONAS ADECUADAS

"La evolución de las amenazas ha llevado a una mayor demanda de otras técnicas y servicios, como DMARC, agente de seguridad de acceso a la nube (CASB)/integraciones de API, conciencia continua y orquestación, automatización y respuesta de seguridad centrada en el correo (MSOAR)".

Gartner®



¿POR QUÉ PRIORIZAR LA PROTECCIÓN DE LAS PERSONAS?

EFICACIA

Se implementa rápidamente, cubre el 100 % de su organización dondequiera que trabajen y detiene las amenazas y la pérdida de datos **antes** de que comprometan lo que le importa

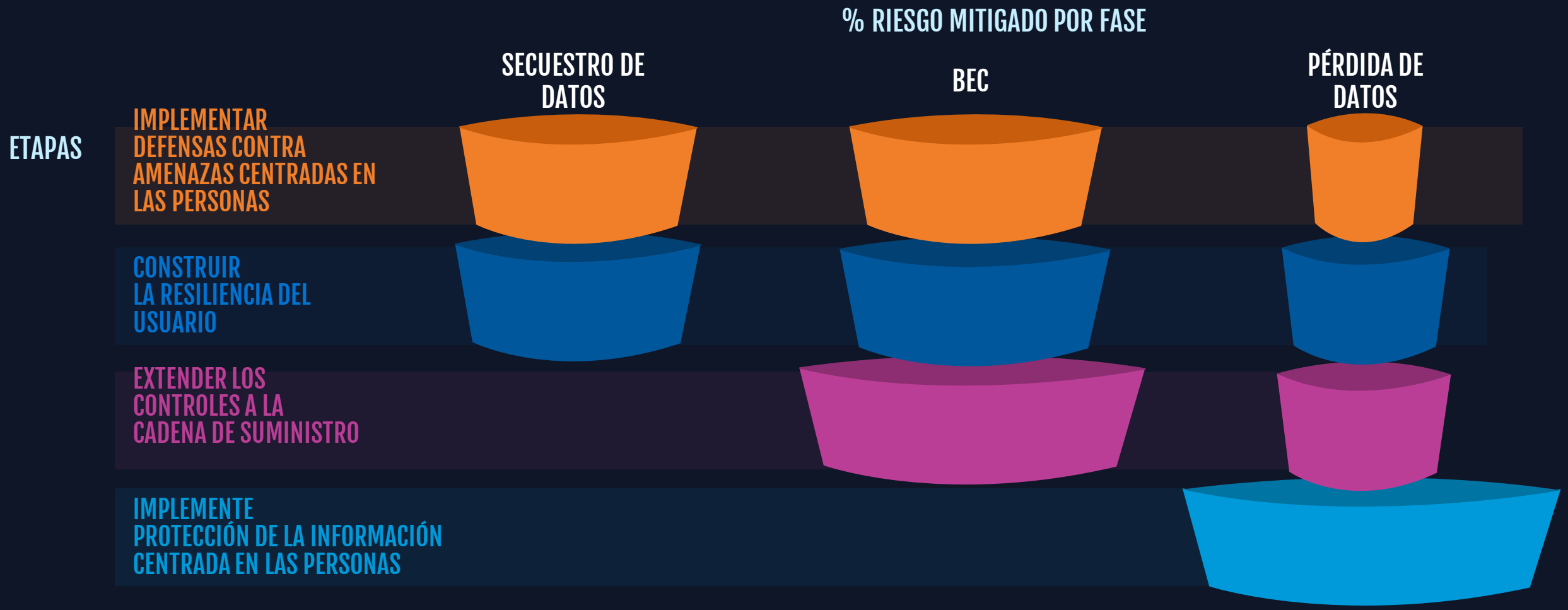
VISIBILIDAD

Ver quién está siendo atacado, quién está creando riesgo y quién está atacando es indispensable para comprender el riesgo.

EFICIENCIA OPERACIONAL

Una plataforma de seguridad centrada en las personas elimina
la carga de sus usuarios, su equipo y
sus controles posteriores

UN ENFOQUE POR FASES PARA OBTENER RESULTADOS EXITOSOS



Descripción general de la respuesta al riesgo