

CIBERSEGURIDAD

ASEGURA TU EMPRESA

ASEMPAL 20 de septiembre de 2024



Financiado por:



CIBERSEGURIDAD

UNA MIRADA A LA PROTECCIÓN EN EL MUNDO DIGITAL

Ponente: Juan Carlos González
Consultor IT
Responsable Dpto. IT de CSM



Financiado por:





Uso
intensivo



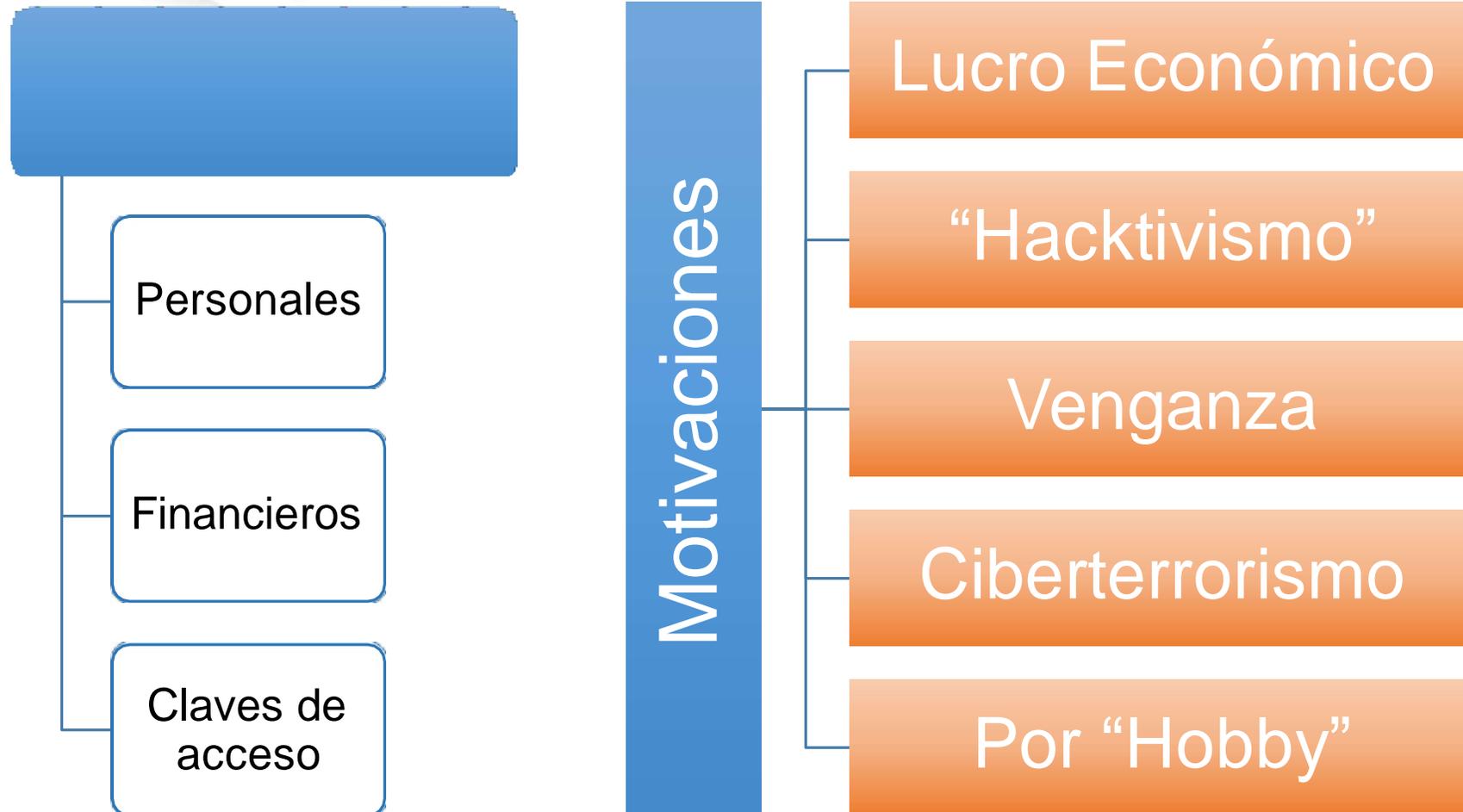
Robo de datos
Extorsión
Estafa



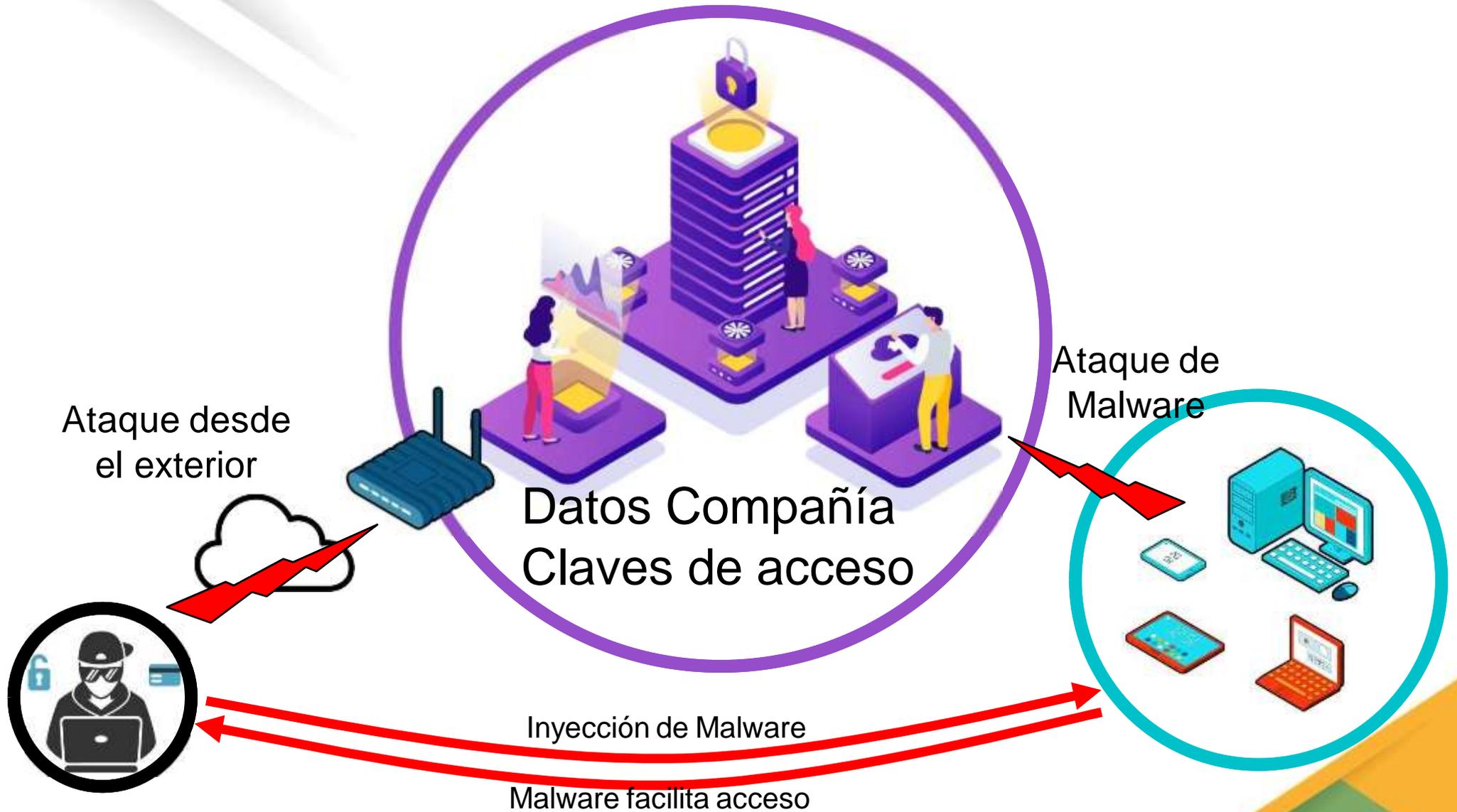
CIBERSEGURIDAD

- Medios físicos
- Herramientas
- Actitudes y acciones

¿Cuál es el OBJETIVO de los Cibercriminales?

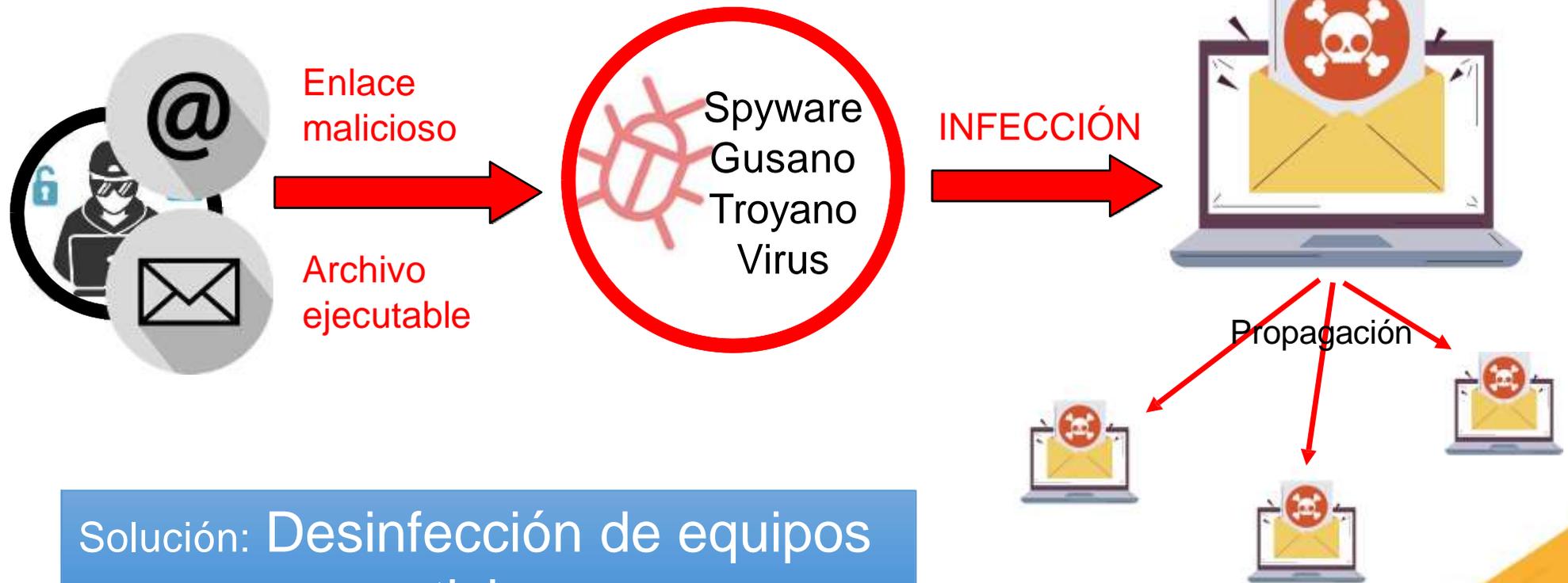


¿Qué atacan los Ciberdelincuentes?



Ataques cibernéticos (I)

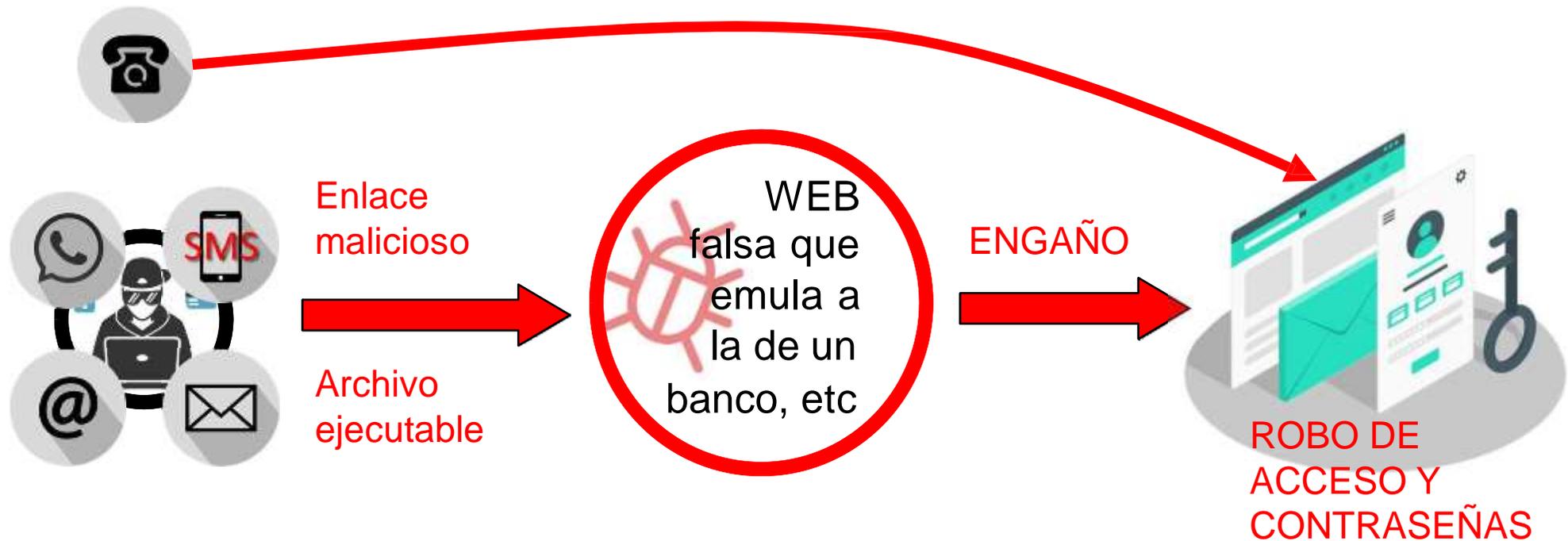
MALWARE



Solución: Desinfección de equipos con antivirus.

Ataques cibernéticos (II)

PHISHING



Solución: Comunicación a la entidad afectada.
Cambio de claves de acceso.

Ataques cibernéticos (III) RAMSONWARE



Solución: Recuperación de datos desde copia de seguridad.

Ataques cibernéticos (IV)

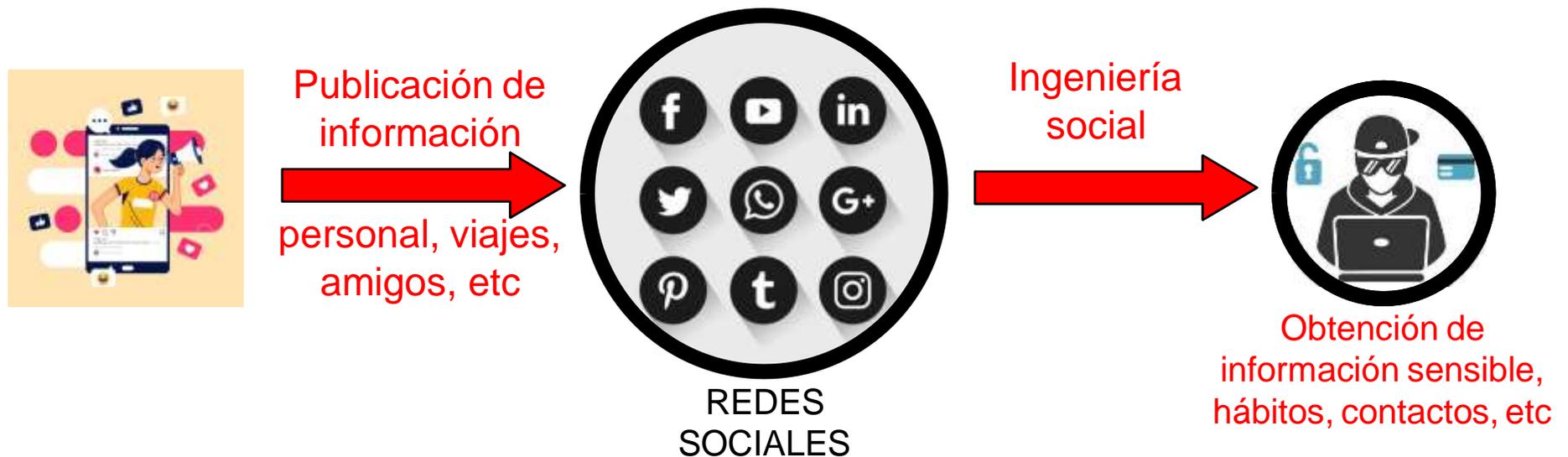
ATAQUE DE INTERMEDIARIO



Solución: No intercambiar información sensible a través de redes WiFi públicas o no securizadas.

Ataques cibernéticos (V)

ATAQUE DE INGENIERÍA SOCIAL



Solución: No intercambiar información sensible a través de redes WiFi públicas o no securizadas.

Ataques cibernéticos (VI)

OTROS ATAQUES

FRAUDE DEL CEO

- Suplantación de identidad del CEO.
- Víctimas: trabajadores de la empresa.
- Solución: aplicar el sentido común.

AMENAZA INTERNA

- Empleado descontento roba información o infecta el sistema informático.
- Solución: limitar acceso a la información sensible y la instalación de aplicaciones.

ATAQUES POR FUERZA BRUTA

- El ciberdelincuente trata de romper la contraseña de un sistema mediante algoritmos criptográficos.
- Solución: uso de contraseñas complejas y cambio periódico.

ATAQUE DE DENEGACIÓN DE SERVICIO

- Colapso del sistema atacado por una avalancha de peticiones de servicio.
- Solución: refuerzo de los accesos a los sistemas.

Ataques cibernéticos (VII)

OTROS ATAQUES

ATAQUE DE DÍA CERO

- Ataque aprovechando vulnerabilidad del sistema operativo en el instante entre la publicación de una actualización y su aplicación.
- Solución: aplicar actualizaciones de forma inmediata.

ATAQUES A SQL

- El ciberdelincuente inyecta un programa malicioso aprovechando vulnerabilidades de las bases de datos.
- Solución: limitación de ejecución de instrucciones SQL.

ATAQUES A IOT

- Aprovechamiento de las vulnerabilidades de los elementos integrantes de soluciones de domótica, automatismos industriales, conducción autónoma, etc.
- Solución: implementar soluciones IOT de marcas de confianza y reconocidas.

¿Cómo proteger nuestros sistemas?

Prevención Organizativa



Creación de una cultura de ciberseguridad en la organización.

- 
- Creación de roles y permisos claros.

- 
- Control de acceso a las instalaciones y equipos.

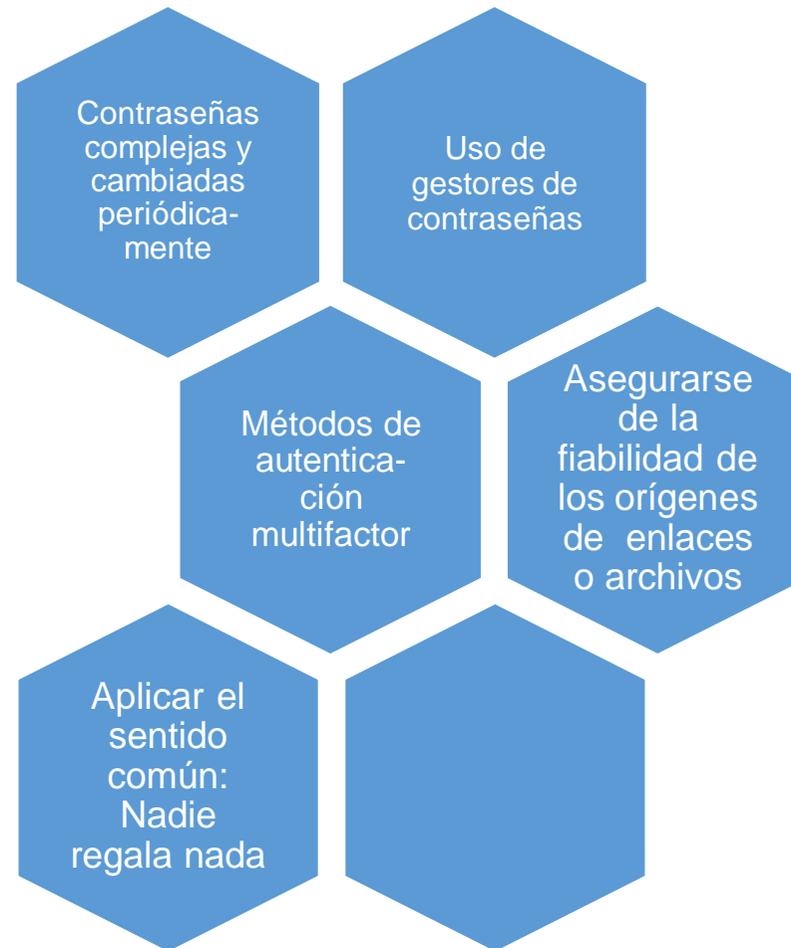
- 
- Creación de un Plan de Seguridad.

¿Cómo proteger nuestros sistemas?

Prevención Tecnológica

- Instalación de Antivirus en todos los dispositivos
- Control de instalación de aplicaciones
- Instalación inmediata de actualizaciones de seguridad
- Uso de las últimas versiones de sistemas operativos
- Actualización de los componentes de los sitios web
- Creación de copias de seguridad internas y externas
- Uso de VPN para acceso desde el exterior
- Uso de firewall avanzados en la red
-

¿Cómo proteger nuestros sistemas? Prevención a nivel de Usuario



¿Cómo proteger nuestros sistemas? Prevención Financiera



Contratación de un
CIBERSEGURO

Sitios de interés

Instituto Nacional de Ciberseguridad (INCIBE)

La página para Particulares (Ciudadanía/Herramientas) contiene herramientas muy útiles y gratuitas. La página de Empresa contiene recursos y herramientas muy interesantes.

<https://www.incibe.es/>

VirusTotal

Sitio que permite averiguar si una web o un enlace están en la lista de no confiables o peligrosos.

<https://www.virustotal.com/>

ESET Online Scanner

Antivirus gratuito para análisis "online". Permite realizar un escaneo completo del ordenador cada mes.

<https://www.eset.com/es/hogar/online-scanner/>

AV Test

Sitio que presenta comparativas independientes de los antivirus del mercado. Muy útil para elegir un antivirus.

<https://www.av-test.org/es/>

Fuentes

Instituto Nacional de Ciberseguridad (INCIBE)

<https://www.incibe.es/>

Microsoft

<https://www.microsoft.com/es-es/>

ACELERA PYME

<https://www.acelerapyme.es/>

Universitat Oberta de Catalunya

<https://www.uoc.edu/es>

IBM

<https://www.ibm.com/es-es/topics/cybersecurity>

CISCO

https://www.cisco.com/c/es_es/

10H Informática y Telefonía

<https://www.10h.es/>

EL CIBERSEGURO

PREVENCIÓN DEL IMPACTO DE LA CIBERDELINCUENCIA

Ponente: **Ricardo Montoya**
Responsable Comercial de
CSM para la Zona Sur



Financiado por:



El Ciberseguro

¿Qué es y para qué sirve?

A pesar de tomar todas las medidas de prevención y de protección de nuestros sistemas informáticos, los ataques cibernéticos no pueden evitarse al 100%.

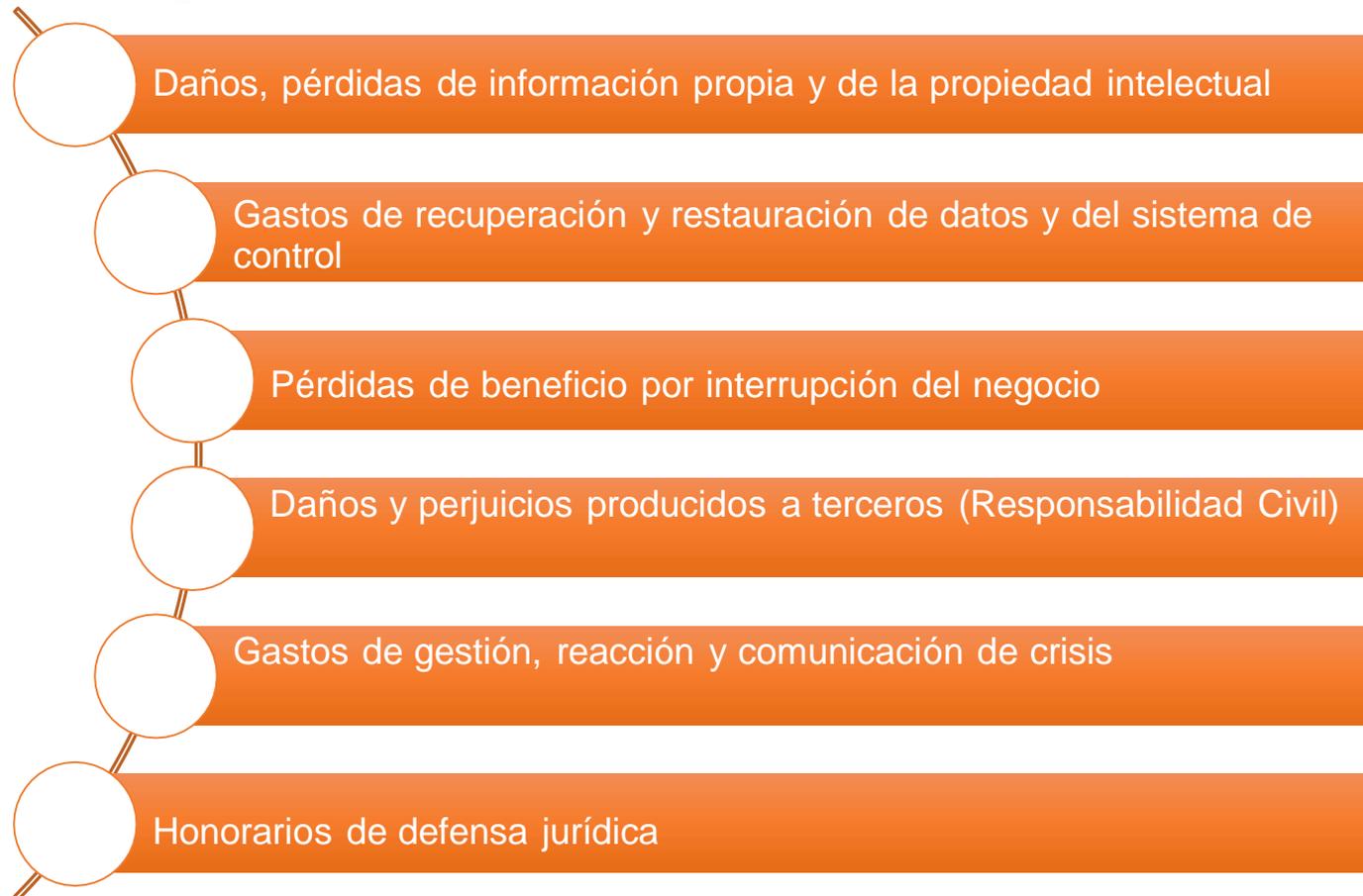
El CIBERSEGURO ayuda a intentar resolver y paliar los efectos de un ataque a nuestros sistemas, asistiendo a la recuperación y reactivación de nuestra actividad.



“Es un seguro a ‘posteriori’, indemnizatorio más que preventivo, centrado en paliar los posibles daños provocados por un ciberataque y en la reactivación de negocio”

El Ciberseguro

COBERTURAS



El Ciberseguro

VENTAJAS Y REQUISITOS

Ventajas

Aporta
tranquilidad al
trabajo diario

Facilita medios de
Prevención contra
ciberataques

Protección de las
consecuencias de
un ciberataque

Requisitos

Antivirus actualizado

Creación regular de
copias de seguridad

Cumplimiento de
LOPD / RGPD

Disponer de
departamento IT
(interno o externo)

El Ciberseguro

DERECHOS Y OBLIGACIONES

Obligaciones

Pago de la prima íntegra del seguro

Comunicación del ciberataque en un máximo de 7 días

Derechos

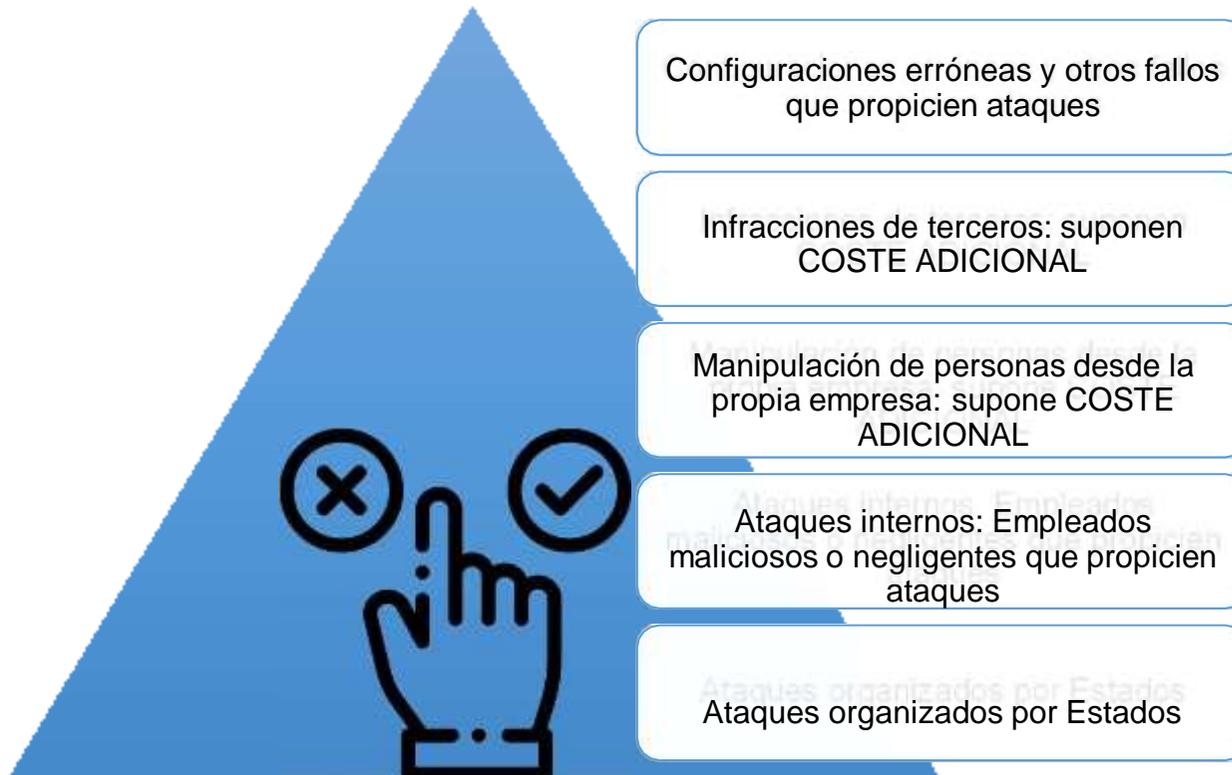
Obtener respuesta a sus consultas

Liquidación del siniestro

Pago de las indemnizaciones pertinentes

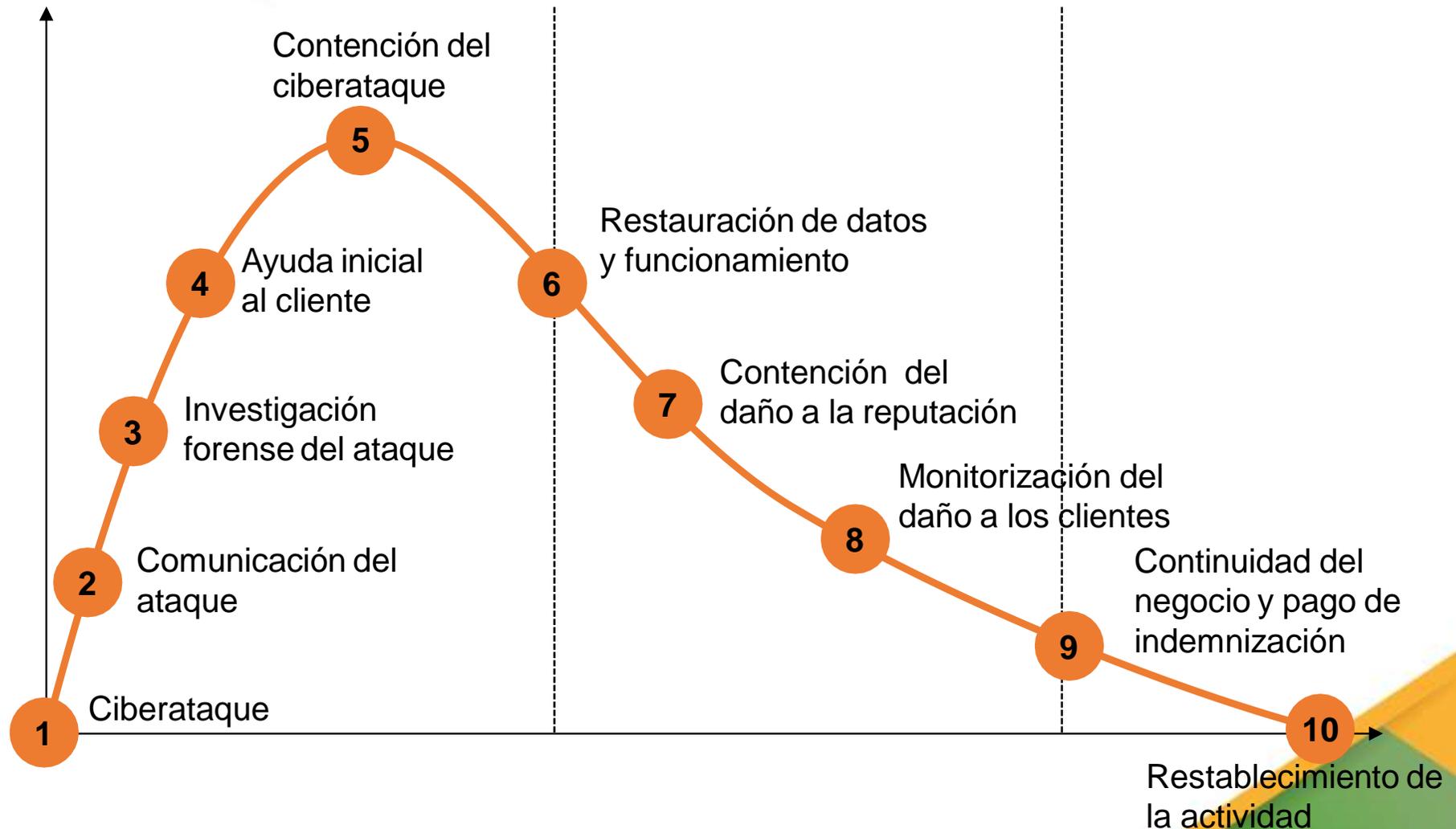
Acciones judiciales que contemplan la póliza

El Ciberseguro EXCLUSIONES



El Ciberseguro

PROCEDIMIENTO ANTE SINIESTROS



El Ciberseguro EJEMPLOS

Información y Consultas en
masempresas.cea.es



/CEA.es



@CEA.es_



/CEA.es



Ruegos y Preguntas

Financiado por:





/CEA.es



@CEA.es_



/CEA.es



Ricardo Montoya



rmontoya@csmcorreduria.es



670 866 756 / 950 502 922

Colaboran:



Confederación de
Empresarios de Andalucía

Financiado por:



Junta de Andalucía

