C-Cyber-Security Framework

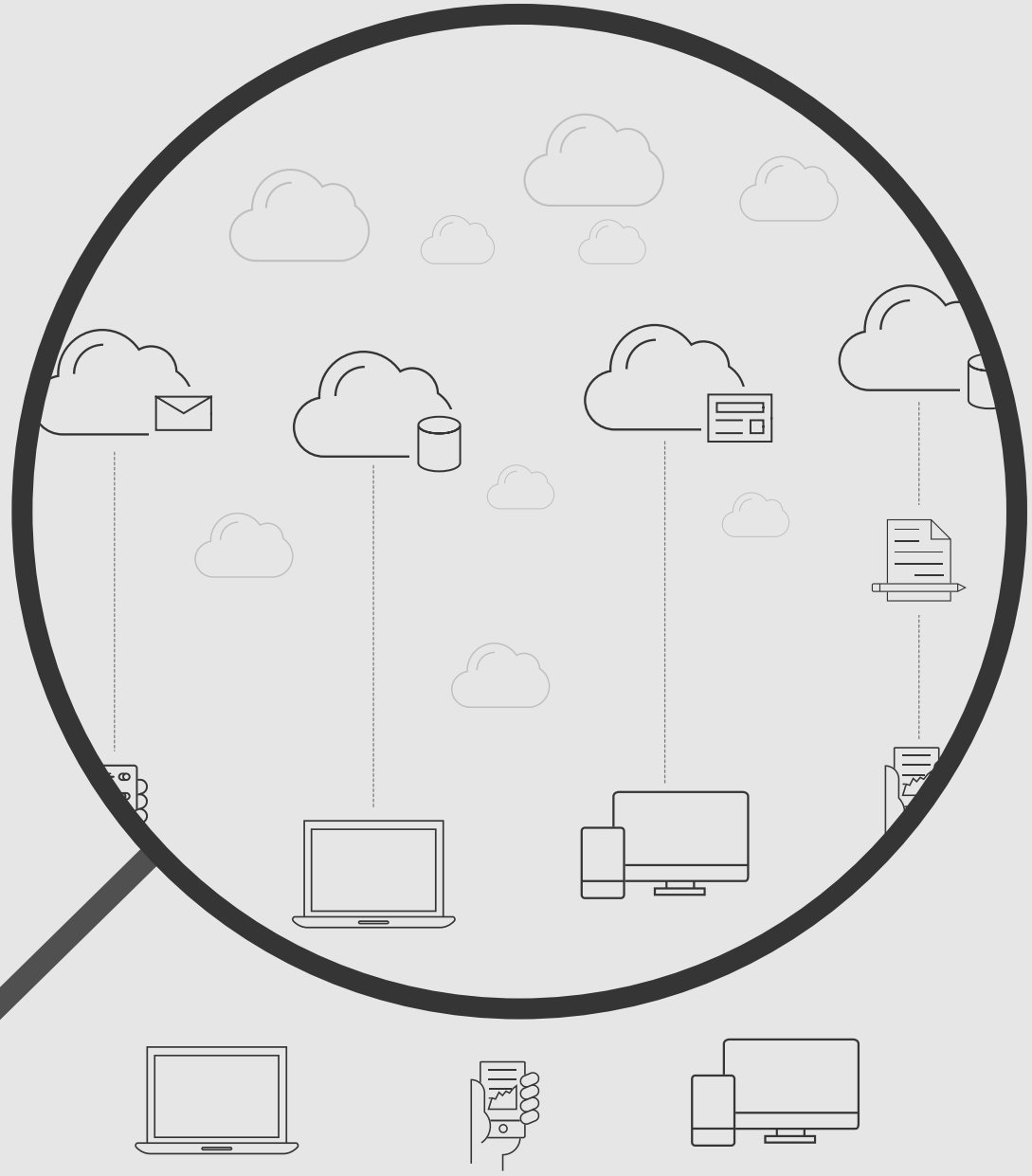
Criticidad Contextual

Relaciones de Seguridad

Adrian Cepero Corcho

Sigestic ‘2023

adrianceperocorcho@gmail.com



CC001

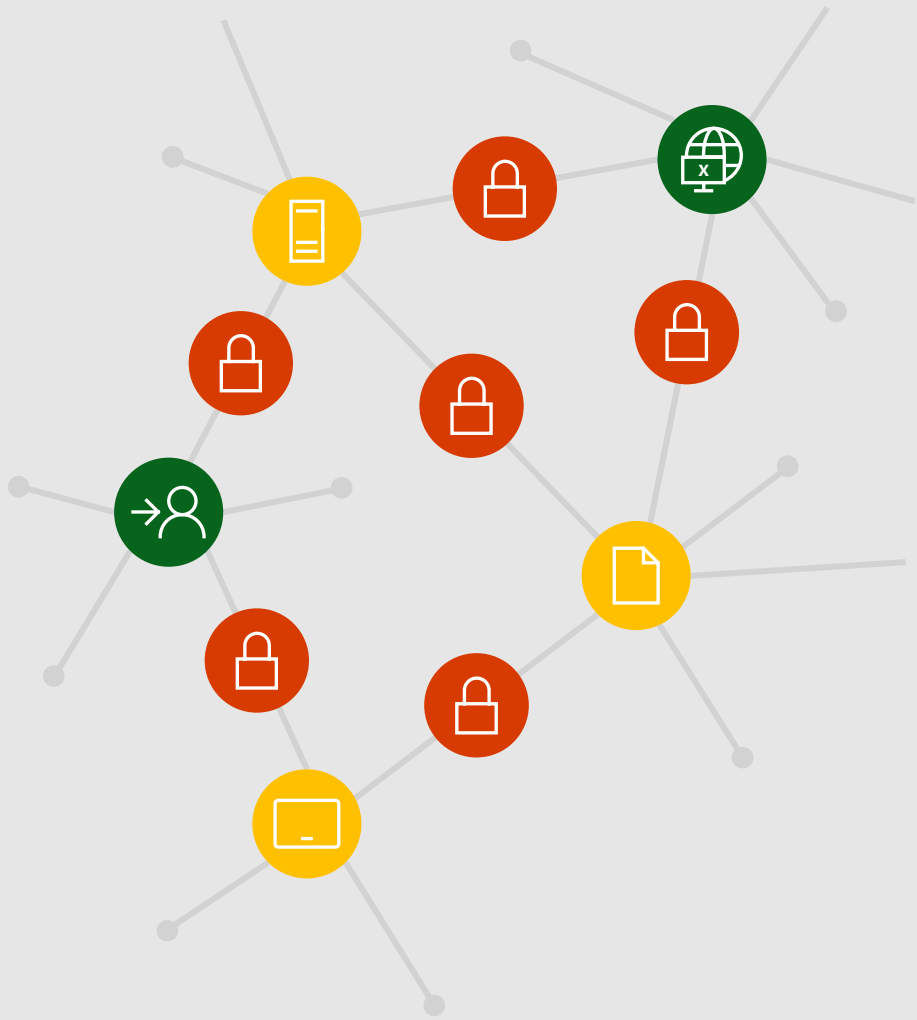
Agenda

Teoría	Práctica
Ciber-Seguridad	Acceso Inicial Demo 1
Criticidad Contextual	Contenido Extra
Relaciones de Seguridad	
Historia	

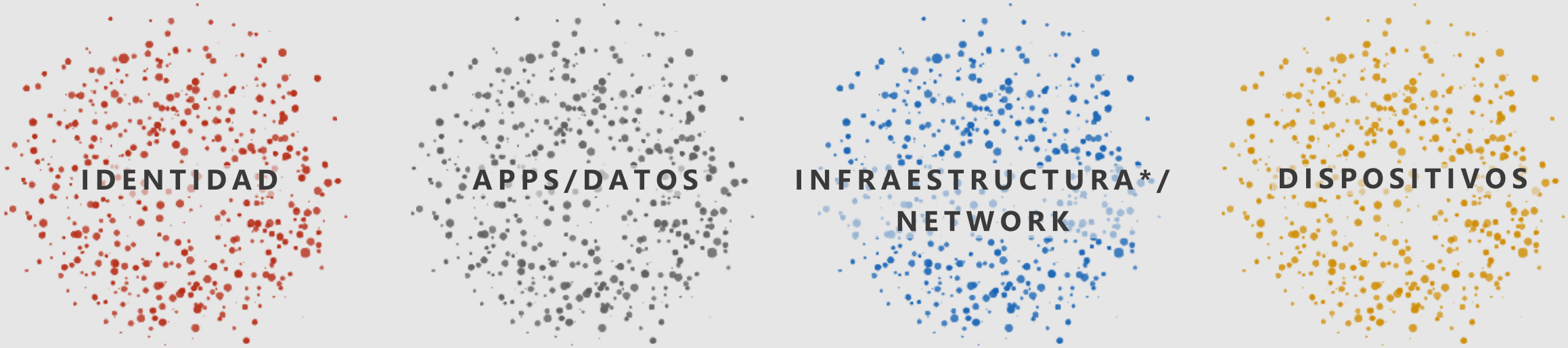
Ciber-Seguridad

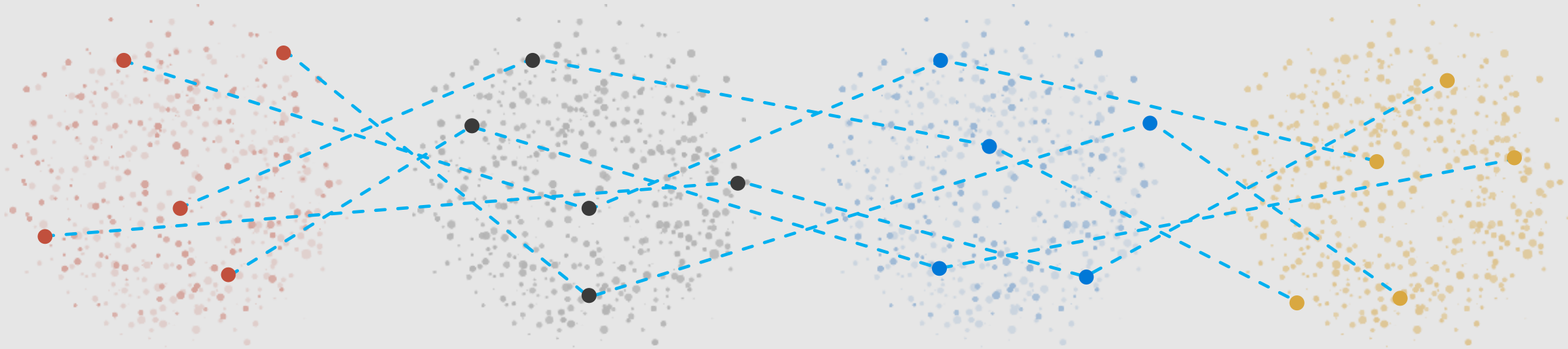
Definición

La Ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos



Origen: Microsoft Bing Chat


IDENTIDAD
APPS/DATOS
INFRAESTRUCTURA*/
NETWORK
DISPOSITIVOS



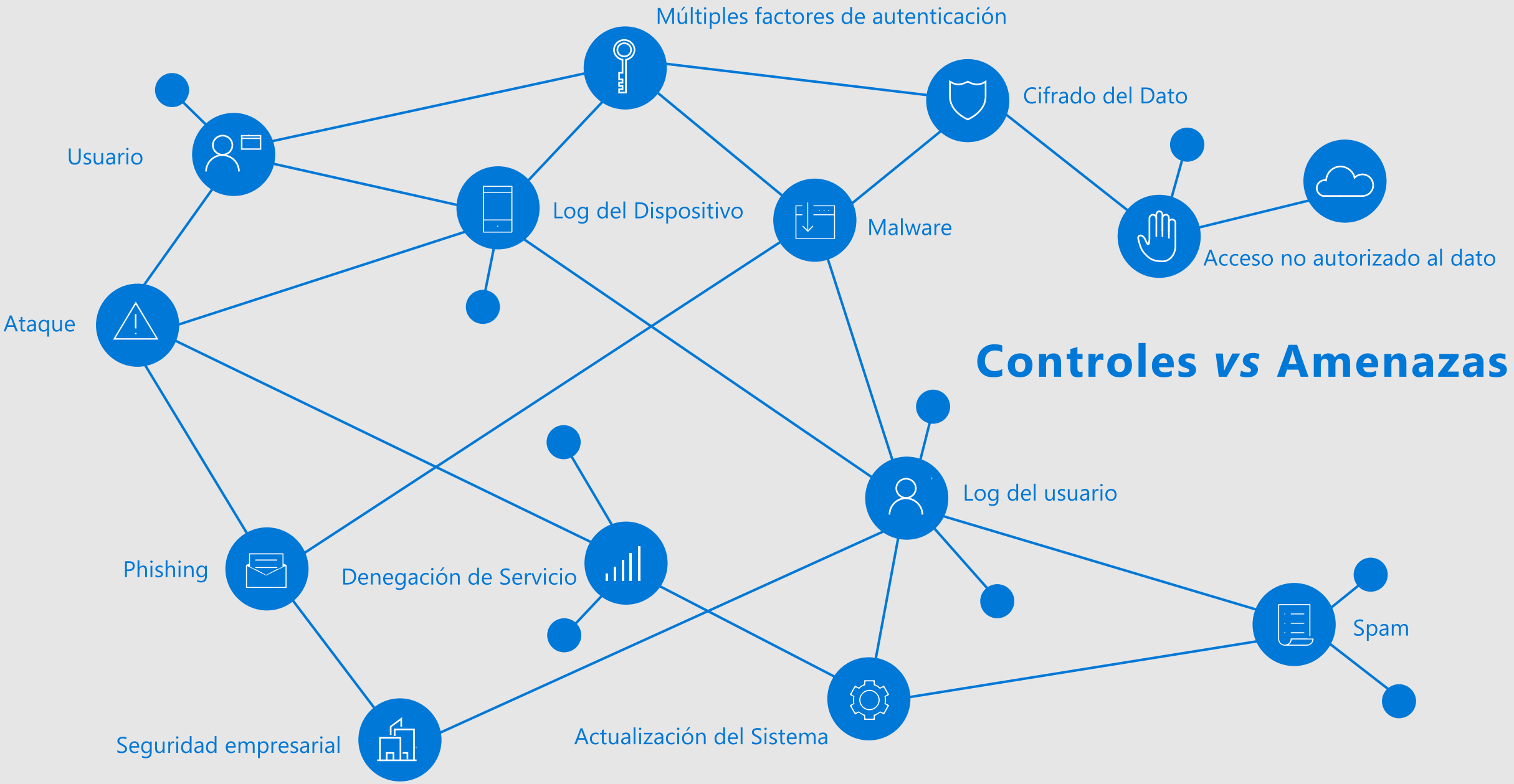
IDENTIDAD

APPS/DATOS

INFRAESTRUCTURA*/
NETWORK*

DISPOSITIVOS

Visibilidad • Control • Relaciones • Inteligencia • Guías de Operación*


Múltiples factores de autenticación
Cifrado del Dato
Usuario
Log del Dispositivo
Malware
Acceso no autorizado al dato
Ataque
Controles vs Amenazas
Log del usuario
Phishing
Denegación de Servicio
Spam
Seguridad empresarial
Actualización del Sistema

Ataques Comunes

PLAN

ENTRADA

MOVIMIENTO

EJECUTAR

A. Accede y Navega

Cualquier empleado abre un correo electrónico con URL del Atacante → **El Atacante accede a la misma información del usuario**

2a

La estación de trabajo es comprometida y el atacante obtiene credenciales

3a

El Atacante utiliza las credenciales robadas para moverse lateralmente

1

El Atacante compromete a empleados mediante una campaña de Phishing

4

El Atacante extrae de la Organización propiedad intelectual entre otras informaciones sensibles

B. Dispositivo Comprometido

El empleado seleccionado por el Atacante abre un correo dirigido → **El Atacante accede a la misma información del usuario**

2b

El empleado B abre el mensaje infectado (Móvil o PC). El Atacante deshabilita el Antivirus

3bc

Las Credenciales comprometidas en el dispositivo por el Atacante son empleadas para acceder a recursos en Cloud o la organización

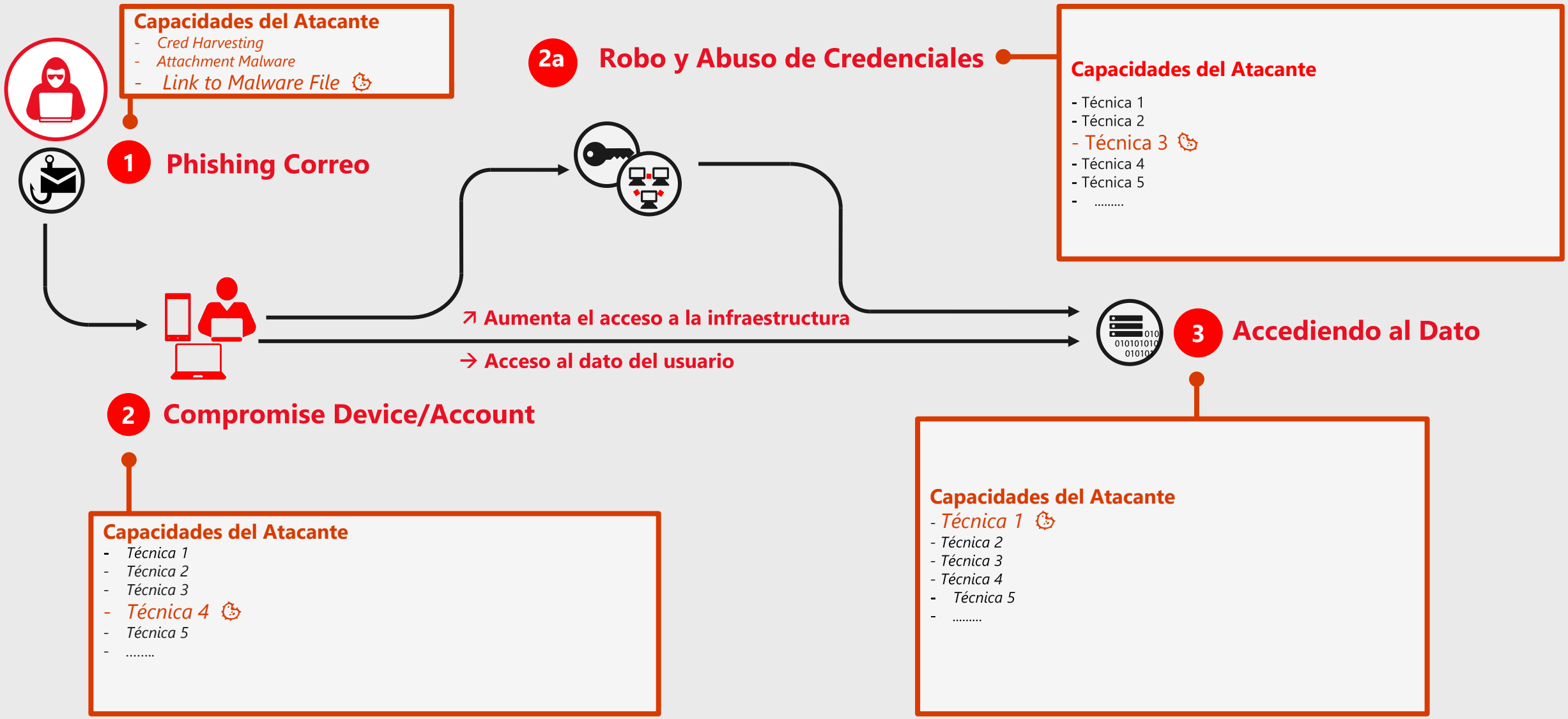
C. Recolectar Credenciales Remotas

El empleado introduce sus credenciales en una página Web falsa → **El Atacante accede a la misma información del usuario**

2c

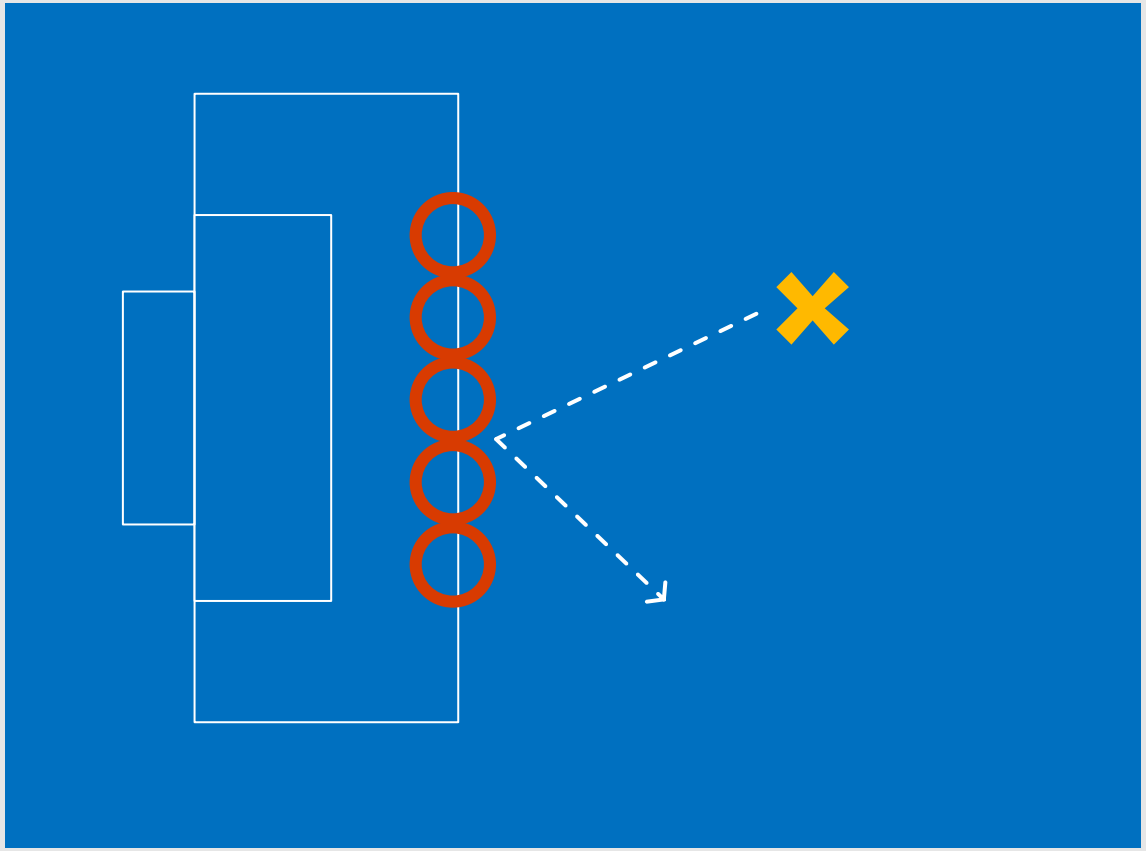
Las credenciales son obtenidas cuando el empleado se autentica en un sitio falso

TTPs Atacantes

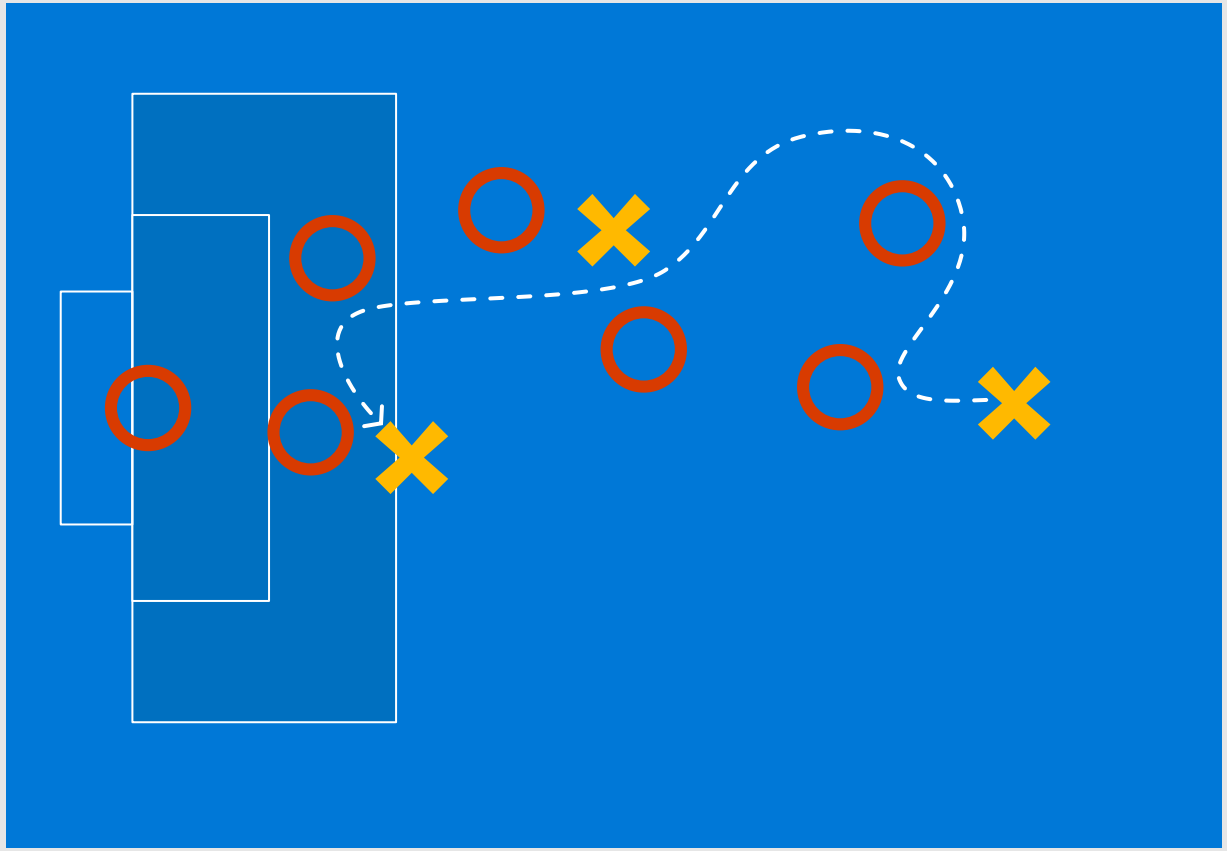


El Defensor piensa en lista.

Cómo construimos nuestras defensas



Qué pasa realmente



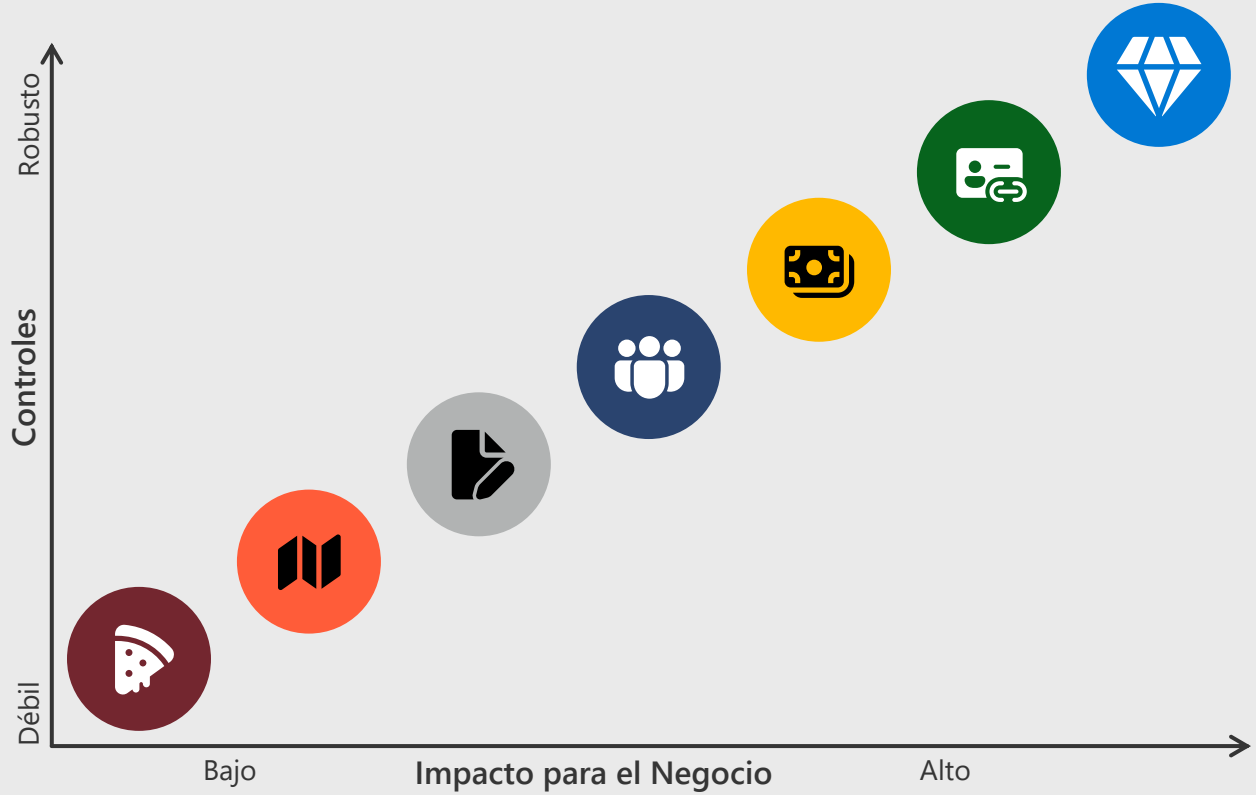
Leyenda

Atacante

Defensor

Criticidad Tradicional

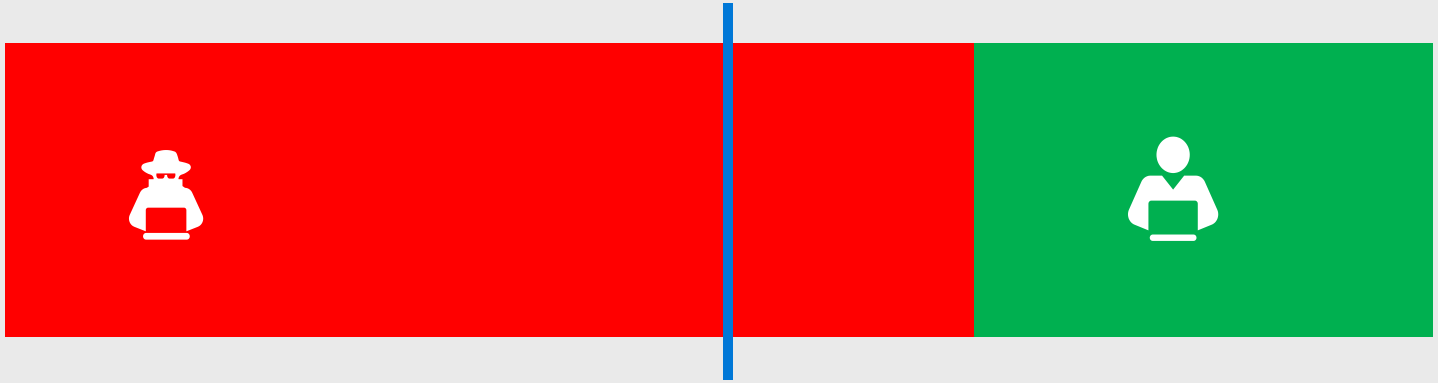
Riesgo Potencial (Incertidumbre)



Criticidad Dinámica

Riesgo Real (Certeza)

La criticidad se calcula dinámicamente en base al riesgo que representa la **acción** para la organización.



Criticidad Dinámica
& Criticidad Contextual

La misma acción produce diferentes resultados

Contexto Interrelacionado*

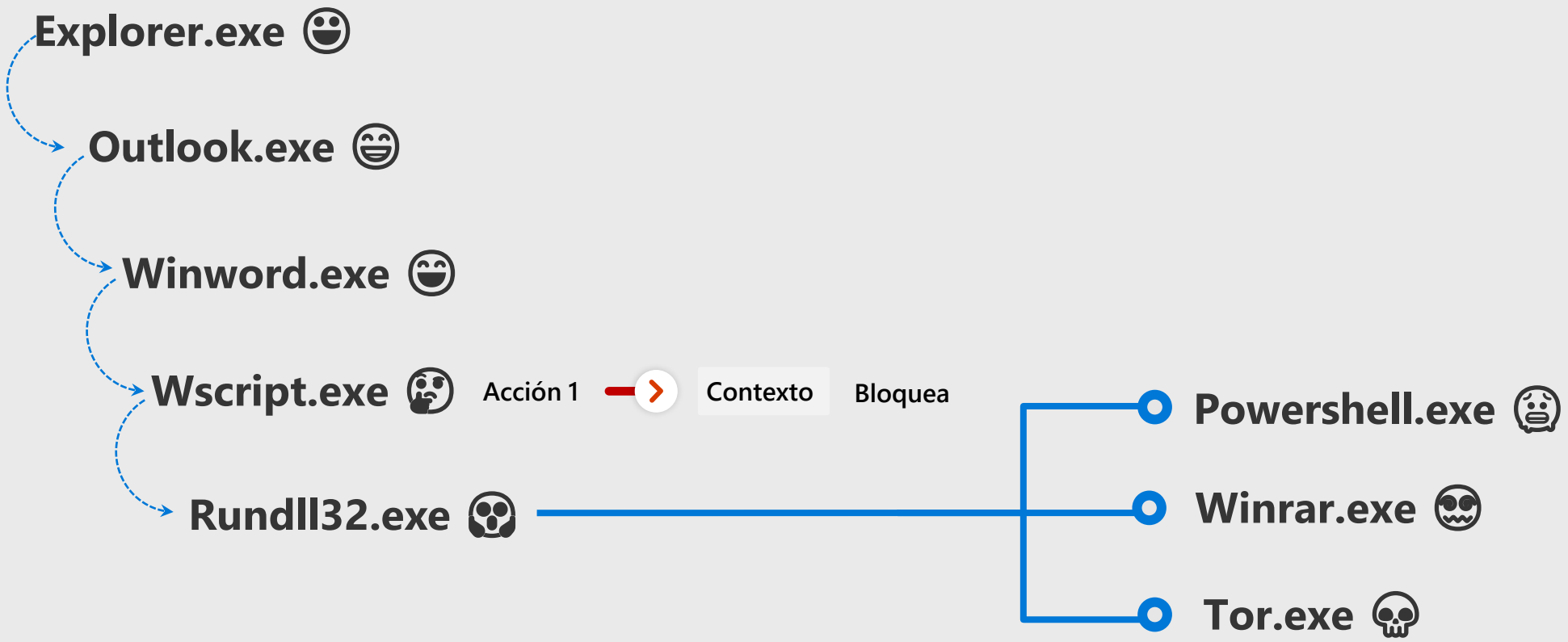
Prevención y Detección (Conscientes del Contexto)

Mitigación Automática

Ejecución dinámica de Controles (A partir del Contexto)

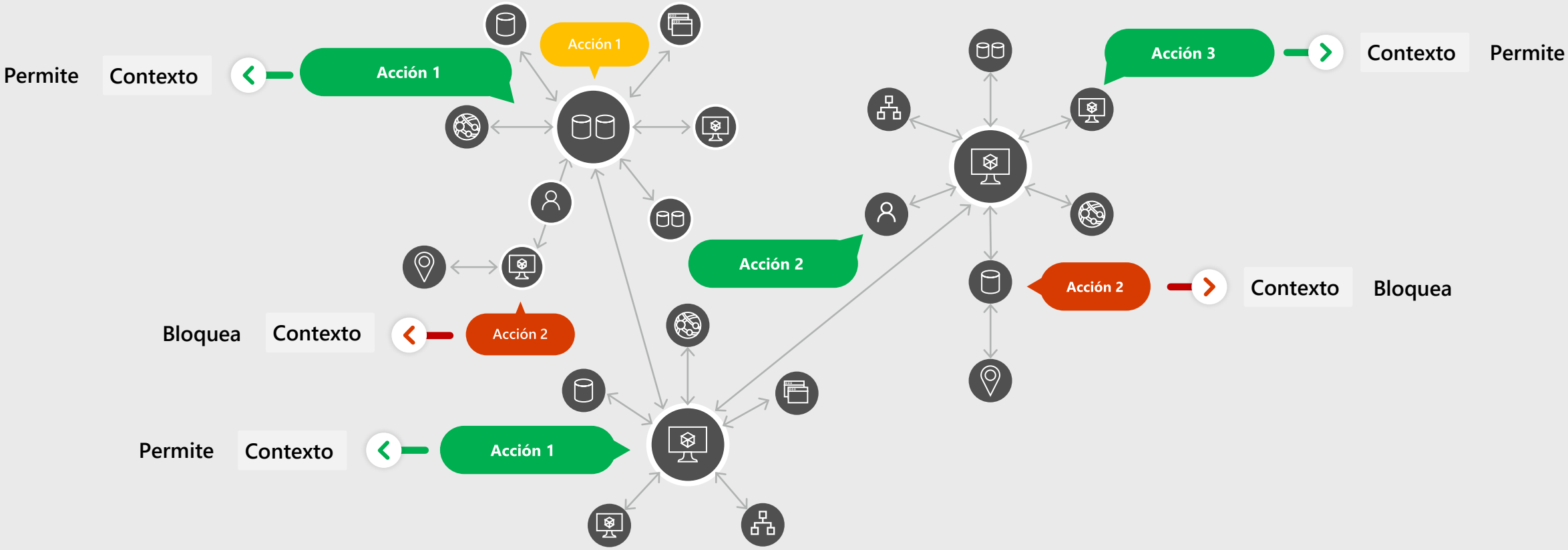
Criticidad Contextual (Micro)

Menos Malware en el ataque



Criticidad Dinámica & Criticidad Contextual

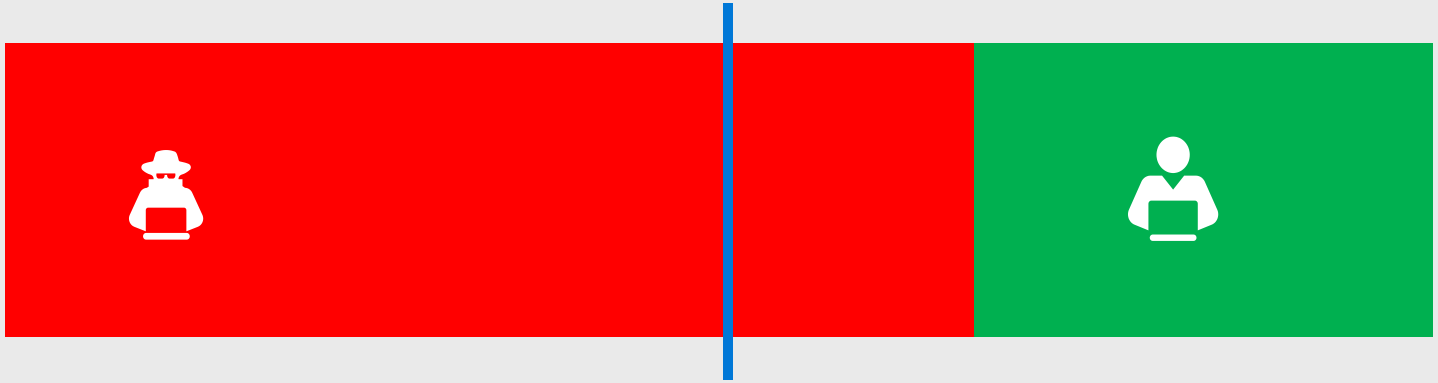
El Defensor piensa en Gráfico



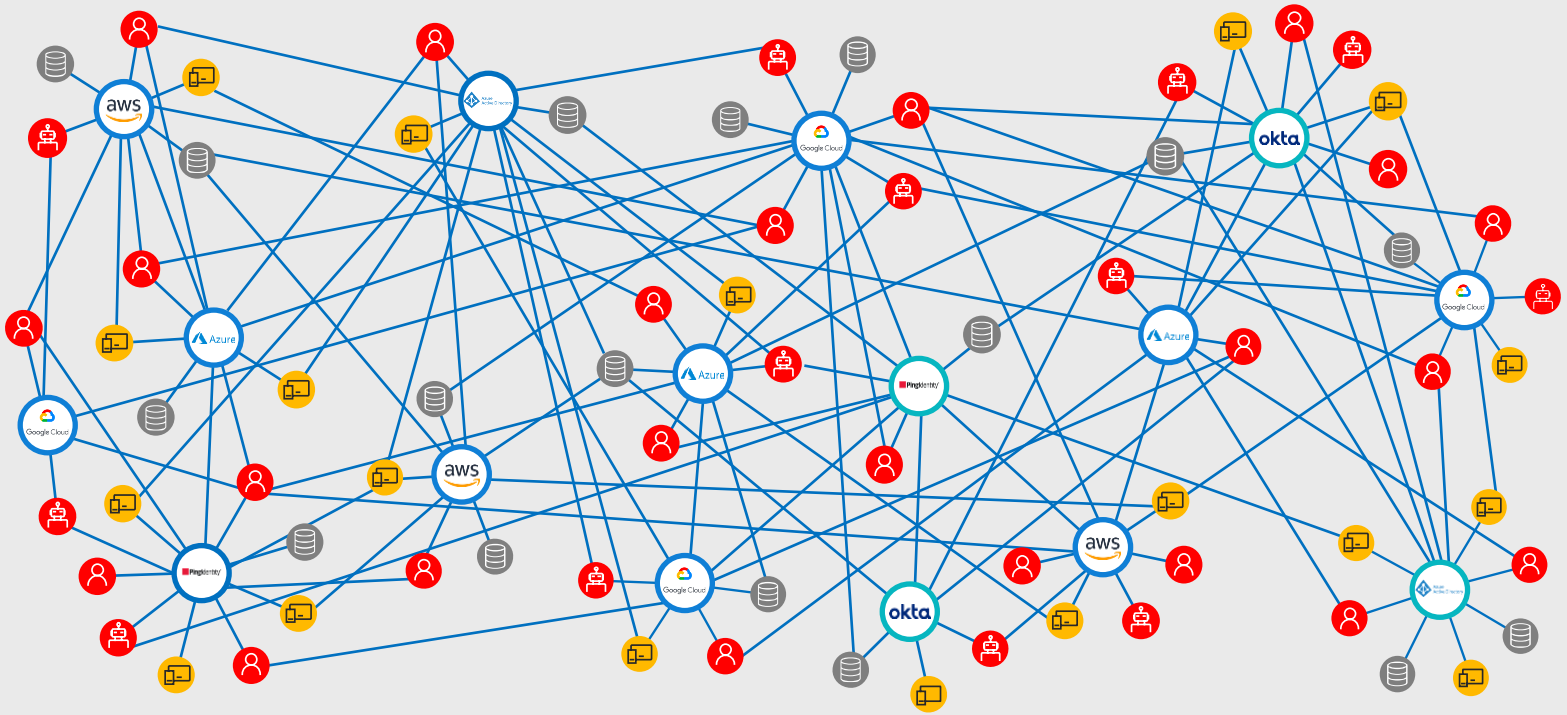
Relaciones de Seguridad

Contexto Local y Distribuido

Incorporar contexto local y distribuido e identificar relaciones perniciosas.

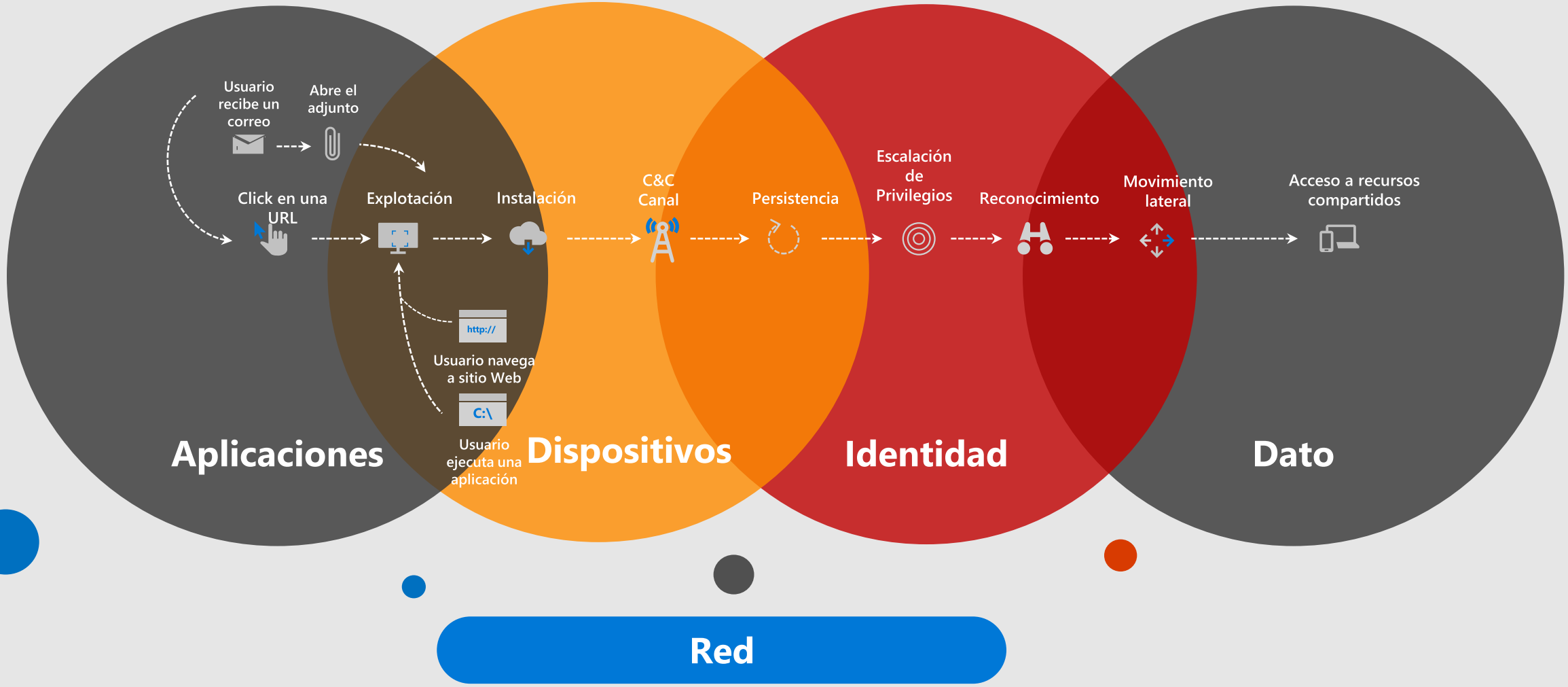


Relaciones de Seguridad (Macro)



Los Activos operan a partir de Relaciones de Seguridad

Relaciones de Seguridad (Micro)



Relaciones de Seguridad (Categorías Macro)

Interacciones Perniciosas

Por Privilegios

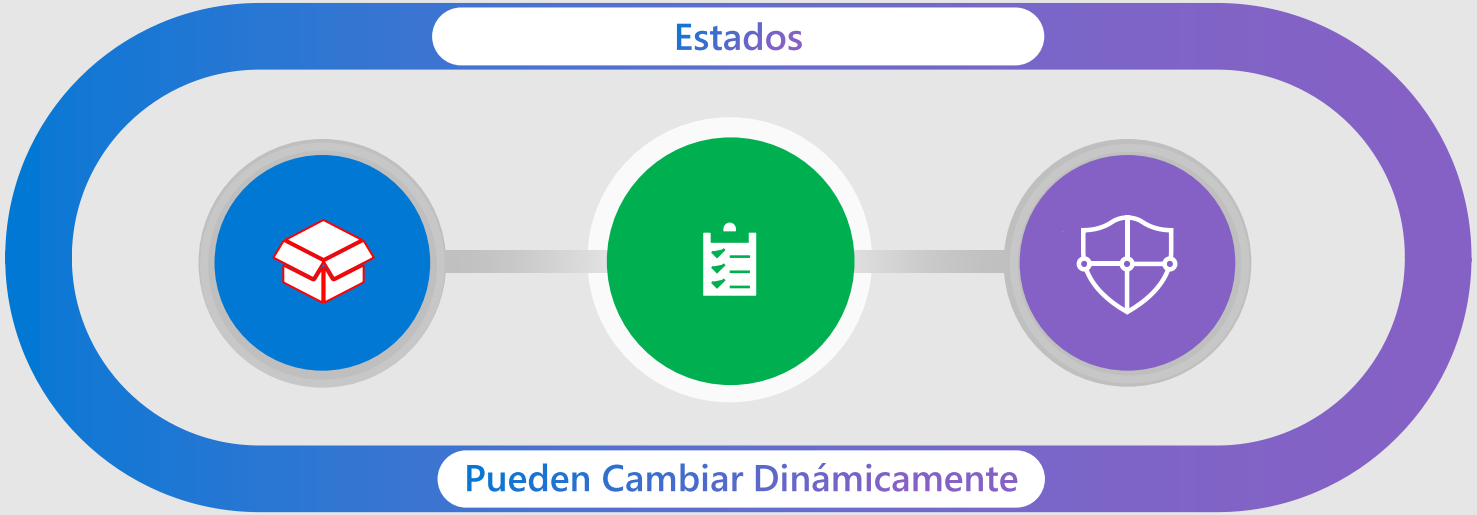
Por Dependencia

Por Similitud

Por Influencia

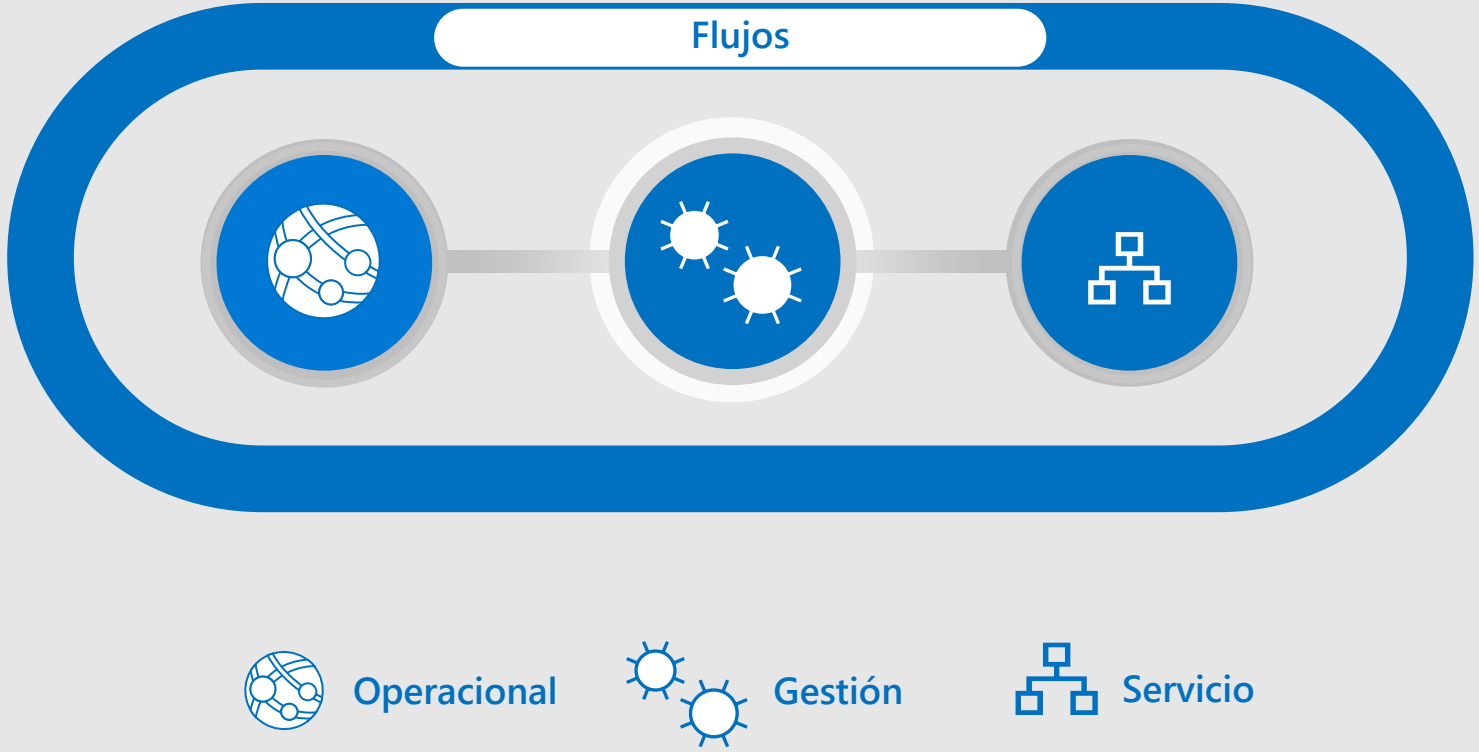
Relaciones de Seguridad (Estados)

Niveles de Reputación

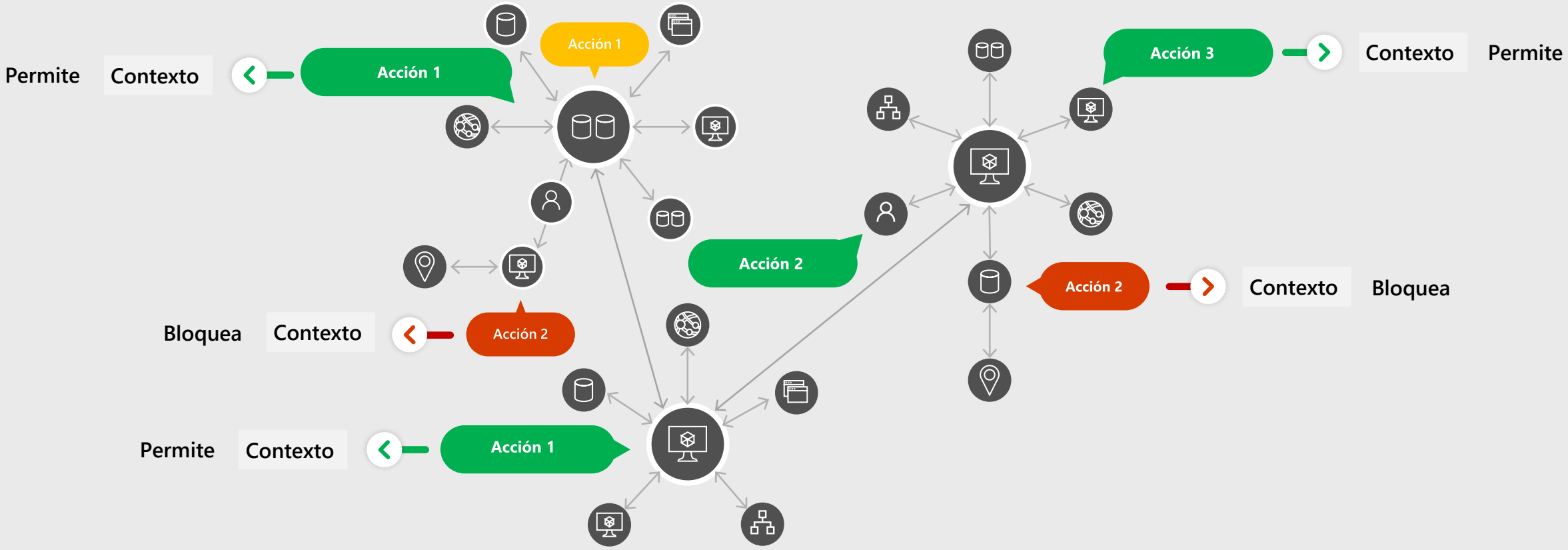


No Controlable Controlable Controlado

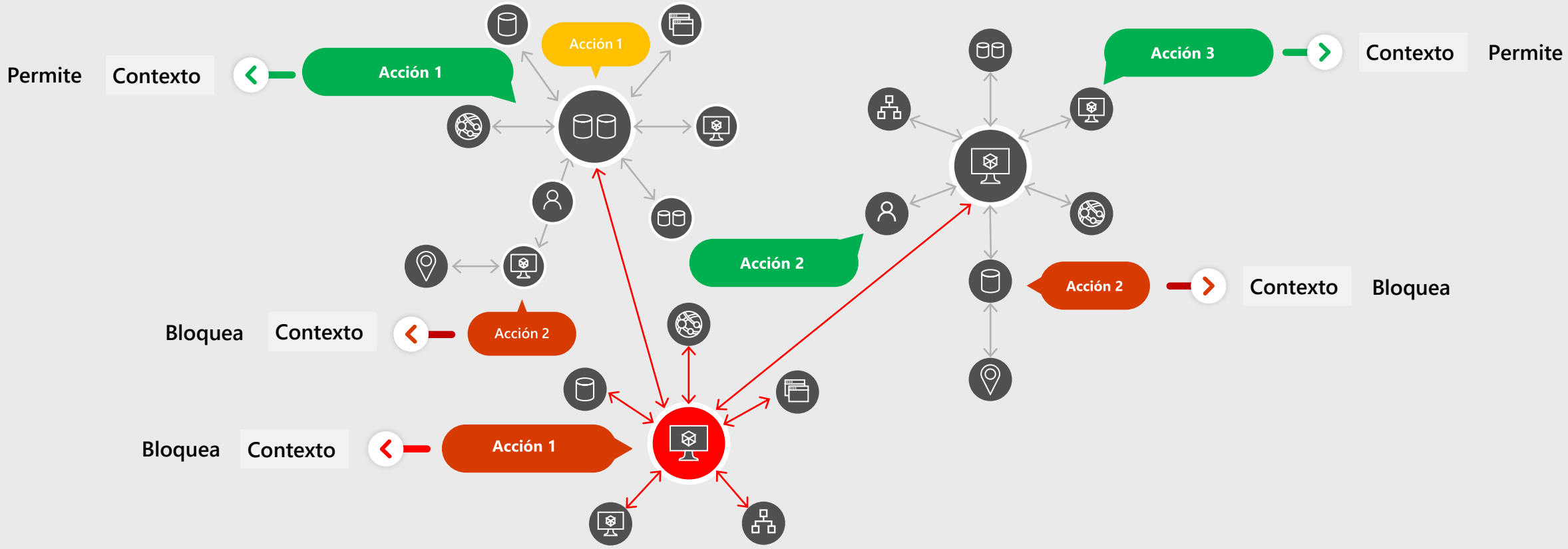
Relaciones de Seguridad (Flujos)



Criticidad Dinámica & Criticidad Contextual

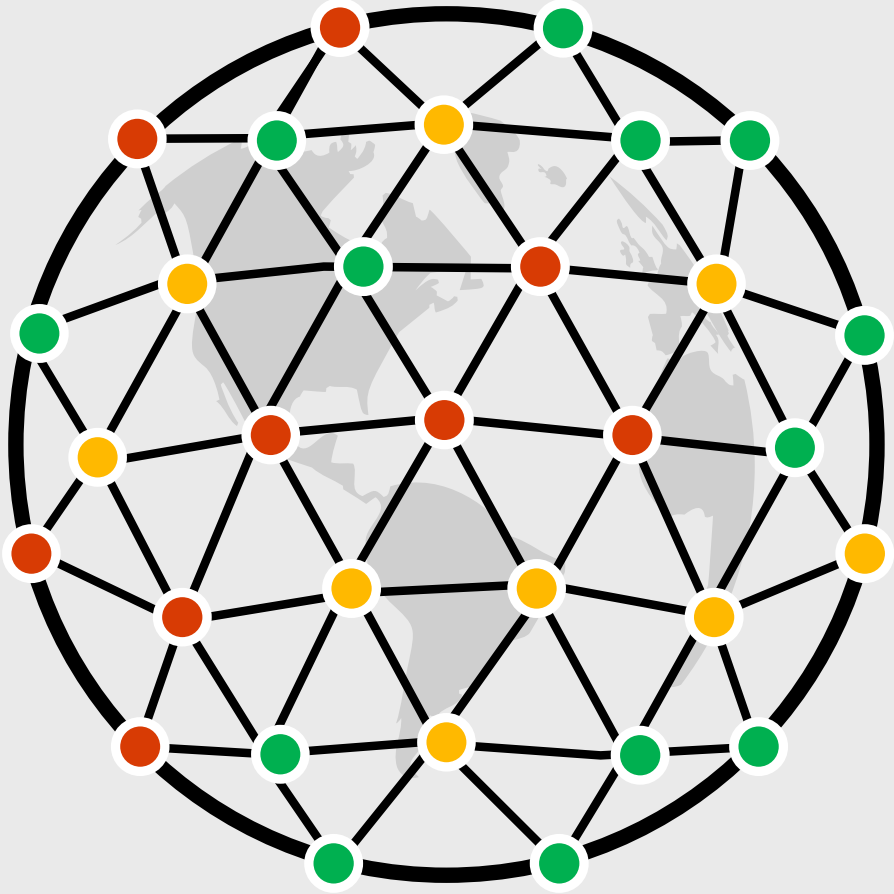


Criticidad Dinámica & Criticidad Contextual & Relaciones de Seguridad

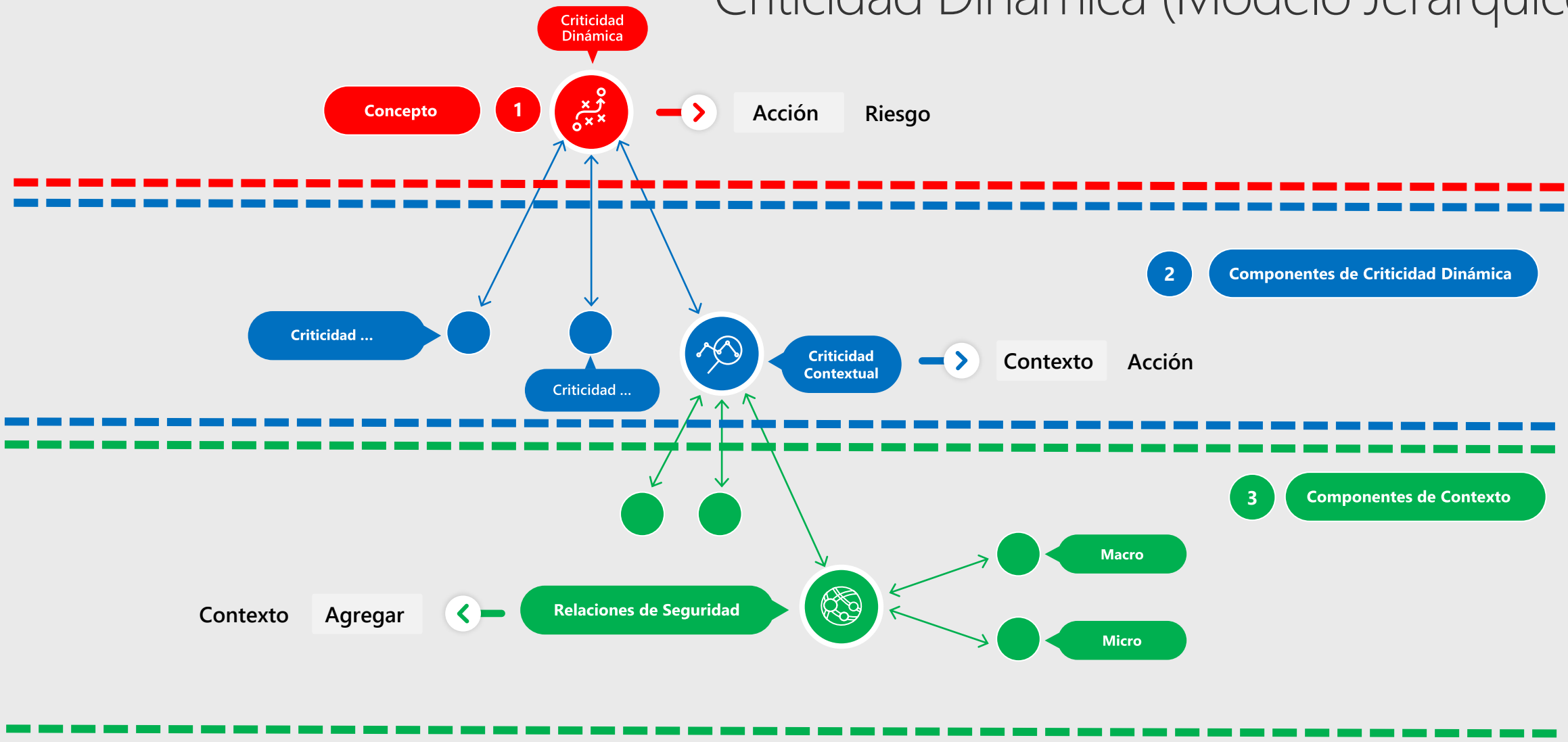


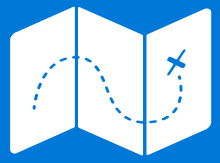
El Defensor piensa en Gráfico Interrelacionado

Criticidad Dinámica & Criticidad Contextual & Relaciones de Seguridad



Criticidad Dinámica (Modelo Jerárquico)



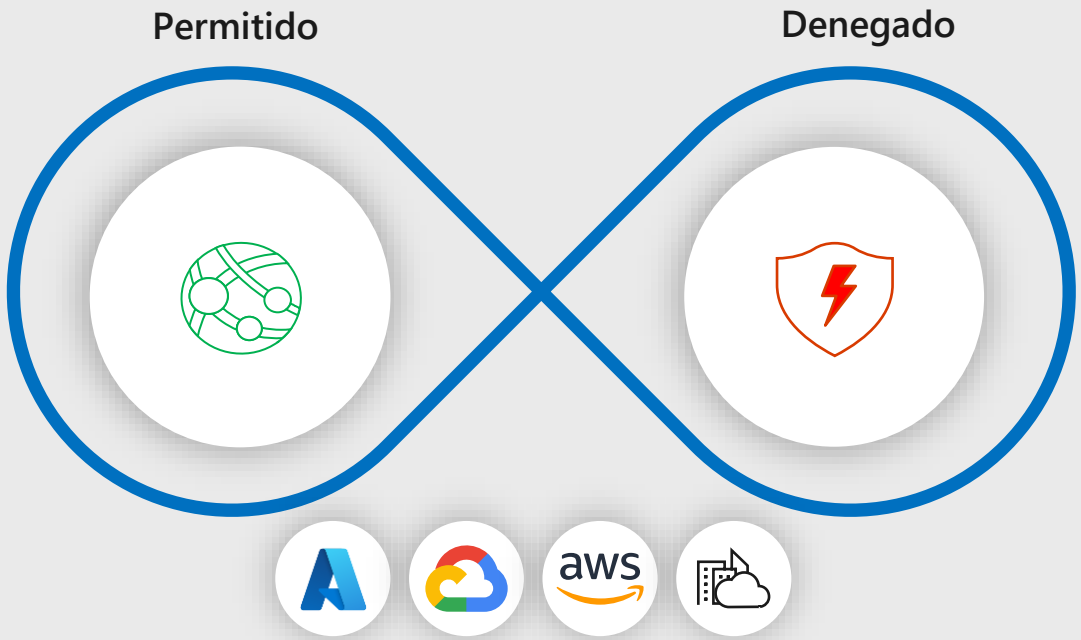


Historia X y ABCD OneNote

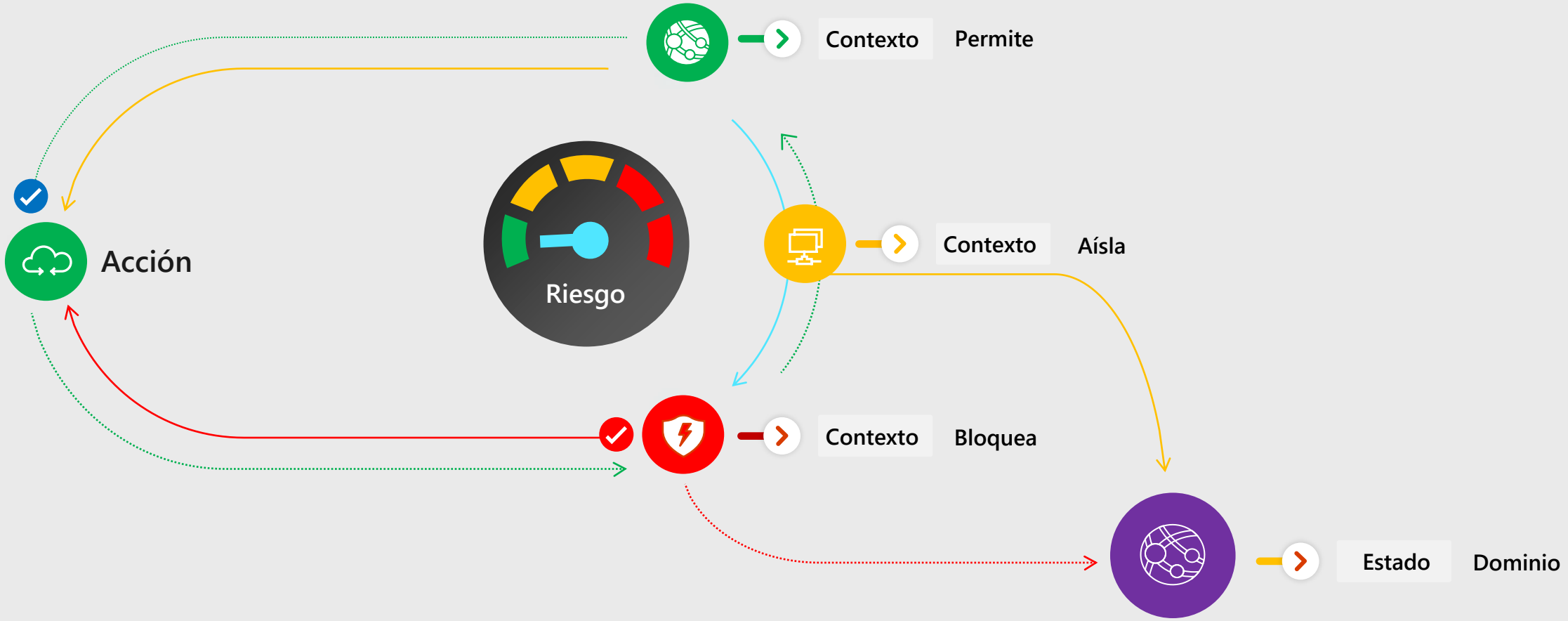
Historia de un Ataque

Lista Blanca (Problemas)

Control de Seguridad



Control & Criticidad Contextual & Relaciones de Seguridad



Clasificación de Estados

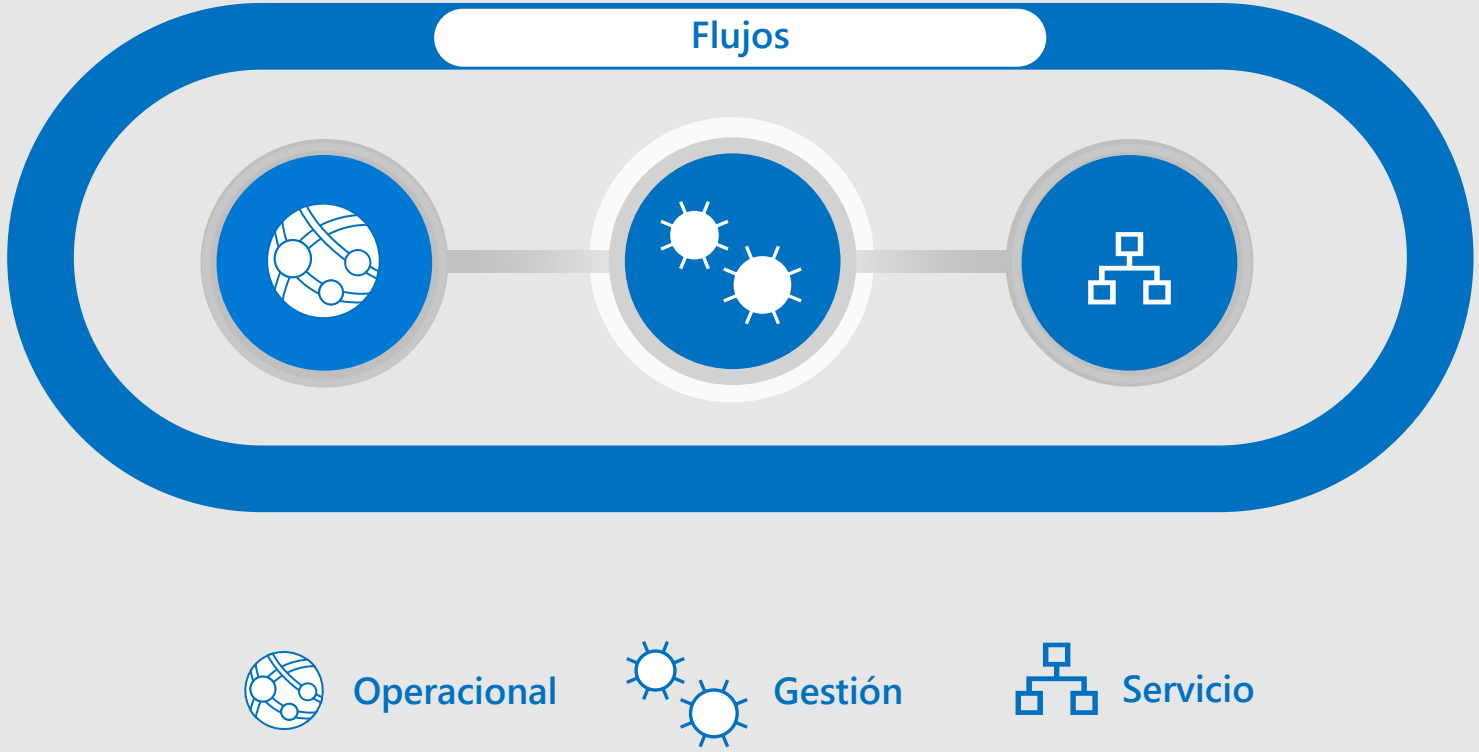
Niveles de Reputación

No Controlable

Controlable

Controlado

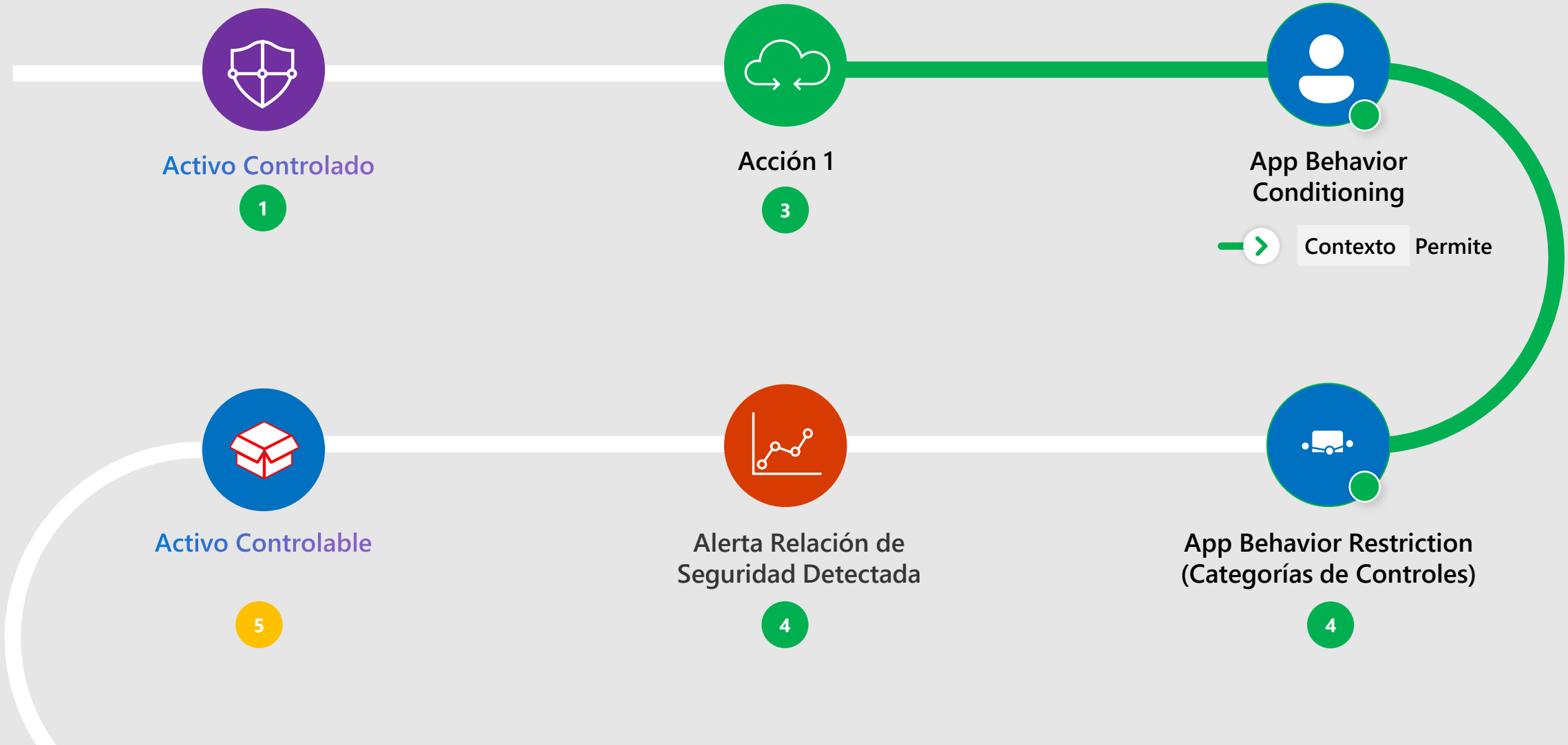
Relaciones de Seguridad (Flujos)



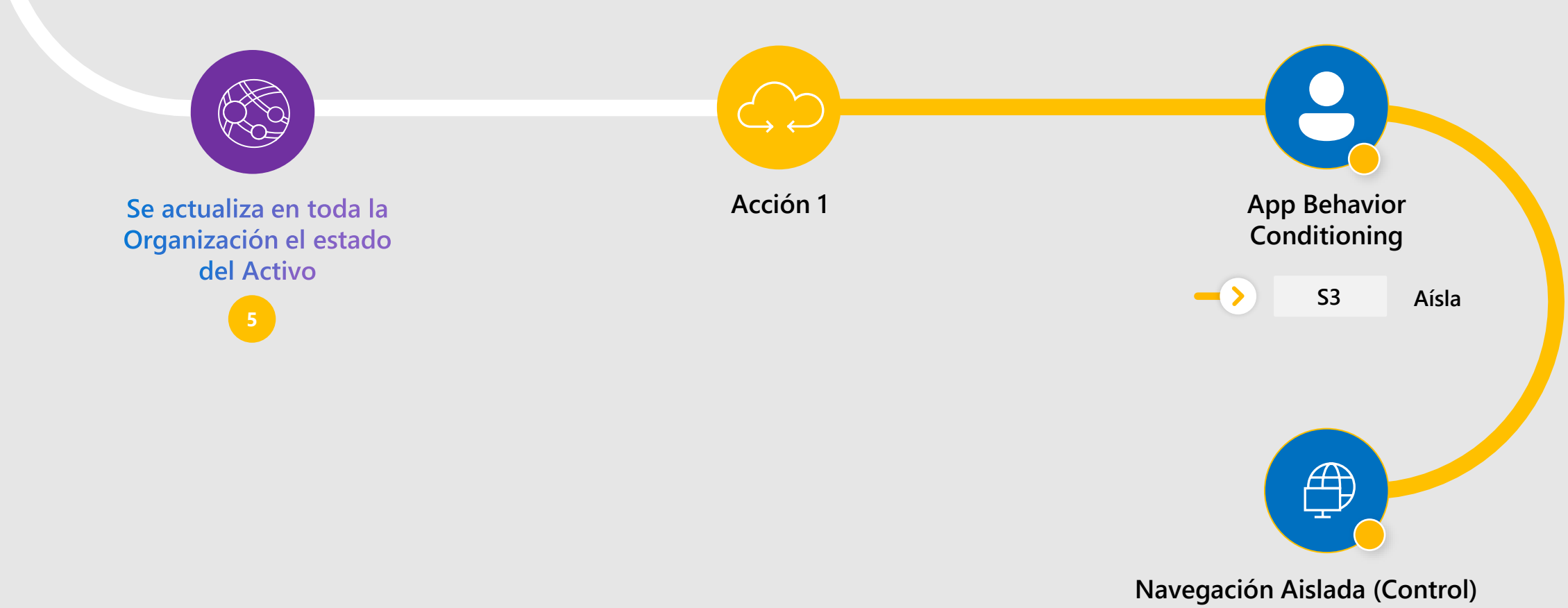
Flujo de la Demo

Relación de Seguridad – Por Influencia

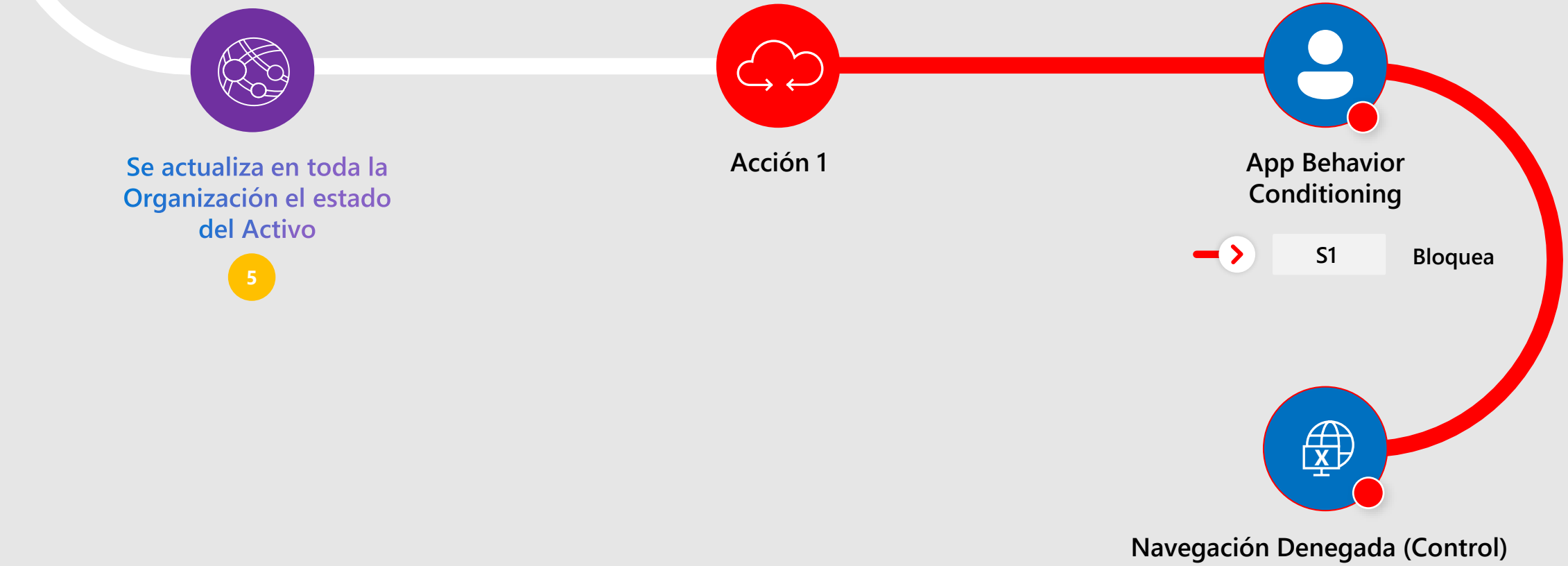
Flujo de la Demo



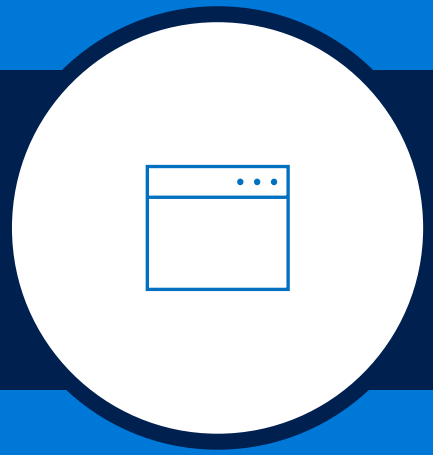
Flujo de la Demo



Flujo de la Demo



Acceso Inicial Demo 1

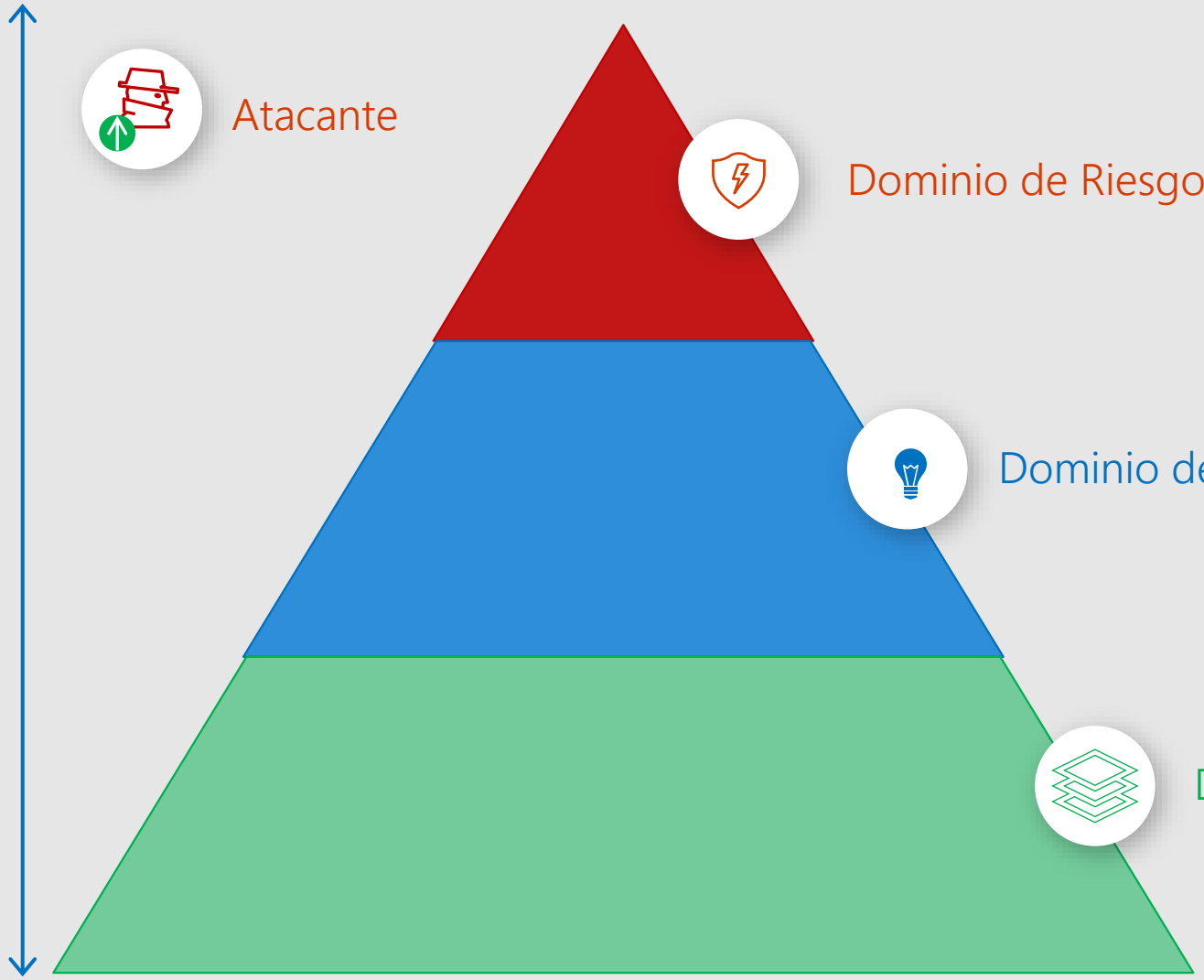


Relación de Seguridad – Por Influencia

Administrator: PowerShell

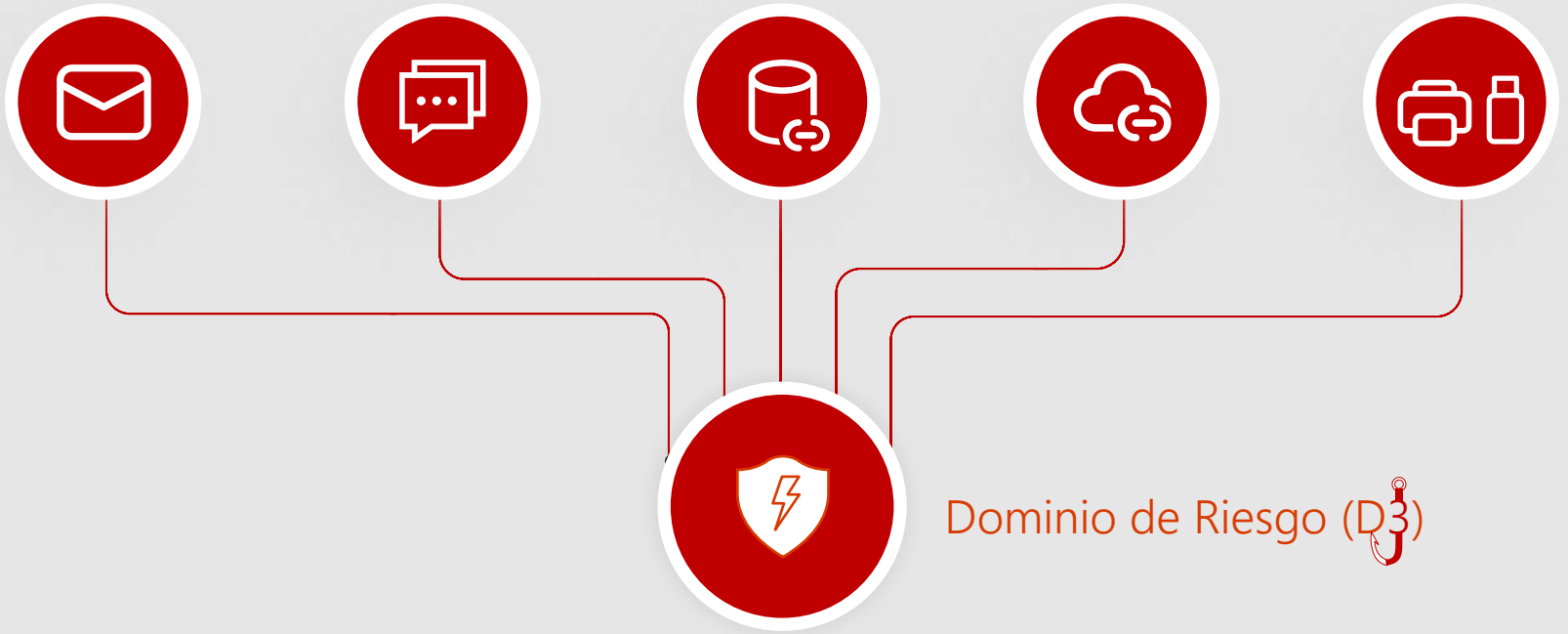
==========💿 📅 S🪢GESTIC 2 3 Demo 1 🕸️Relación de Seguridad - Por Influencia
👨‍💻 Acceso Inicial Drive-by Compromise 💉T1189 💿==========
👍 1: Mostrar Url Permitidas (Recursos Seguros 🛡️Activos Controlados).
💎 2: Listar Variable de Entorno de Nivel de Sensibilidad.
💣 3: Ejecutar la Url Maliciosa https://cyber-kill-chain.ch/techniques/T1189/?lang=.
(🗣️Relación de Seguridad - Por Influencia)
🦹‍♀️ 4: Mostrar el Evento Generado por la Acción (📝Activo Controlable).
👍 5: Mostrar Url Permitidas (Recursos Seguros 🛡️Activos Controlados).
⏳ 6: Recrear la Demostración.
🕰️ Q: Salir.
Por favor, elija una opción:

Contenido Extra



MODELO DE AISLAMIENTO DE APLICACIONES CLIENTES

Contenido Extra



Modelado (Técnicas)*

Contenido Extra

Aísla Contexto Acción 1

Web Confiable

Drive-by Compromise T1189 +

App

Drive-by Compromise T1189 +

Phishing (3) T1566 +

Supply Chain Compromise (2) T1195 +

Dispositivo

Hardware Additions T1200

Replication Through Removable Media T1091

Supply Chain Compromise (1) T1195 +

Identidad

Trusted Relationship T1199

Valid Accounts (4) T1078

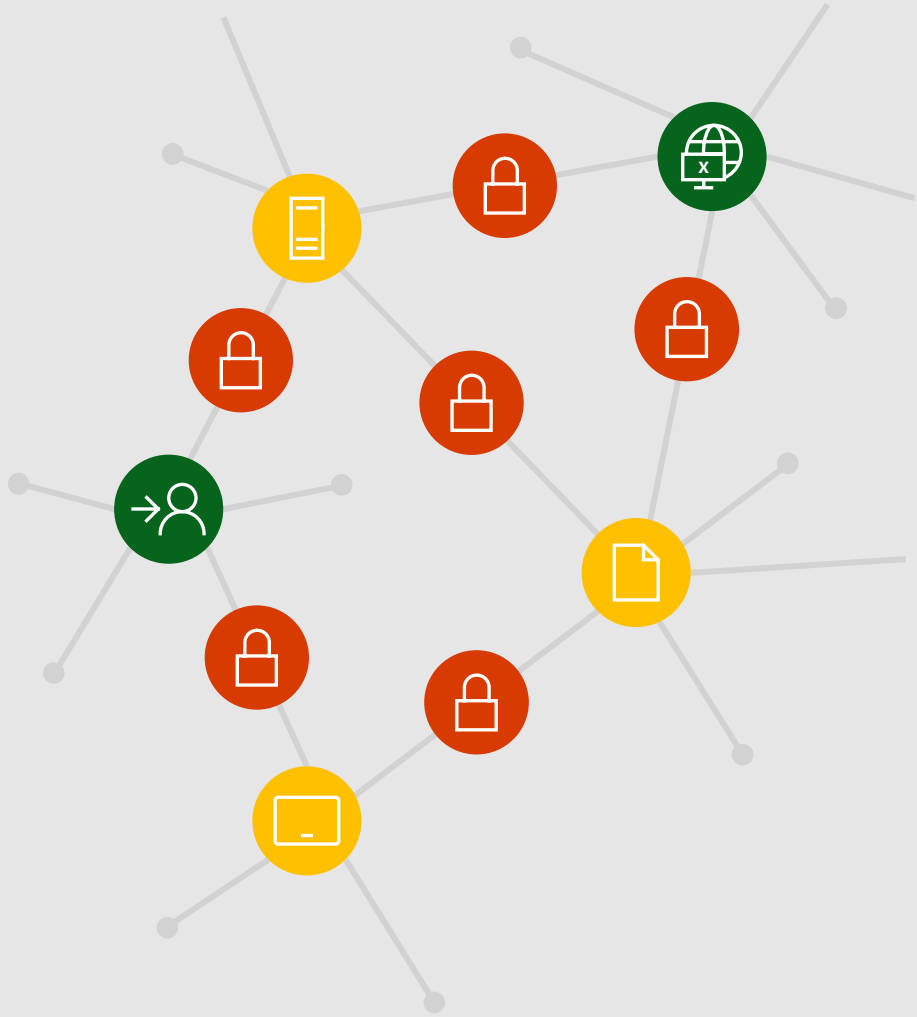
Dato

Acceso Inicial

Recapitulando

Criticidad Contextual

Relaciones de Seguridad



C-Cyber-Security Framework