Universidad de Costa Rica
Centro de Informática
Jornadas de Investigación **PROSIC** 2025

De amenazas invisibles a responsabilidad de todos

Estamos bajo asedio constante

Luis Loría Chavarría

¿Qué es ciberseguridad?

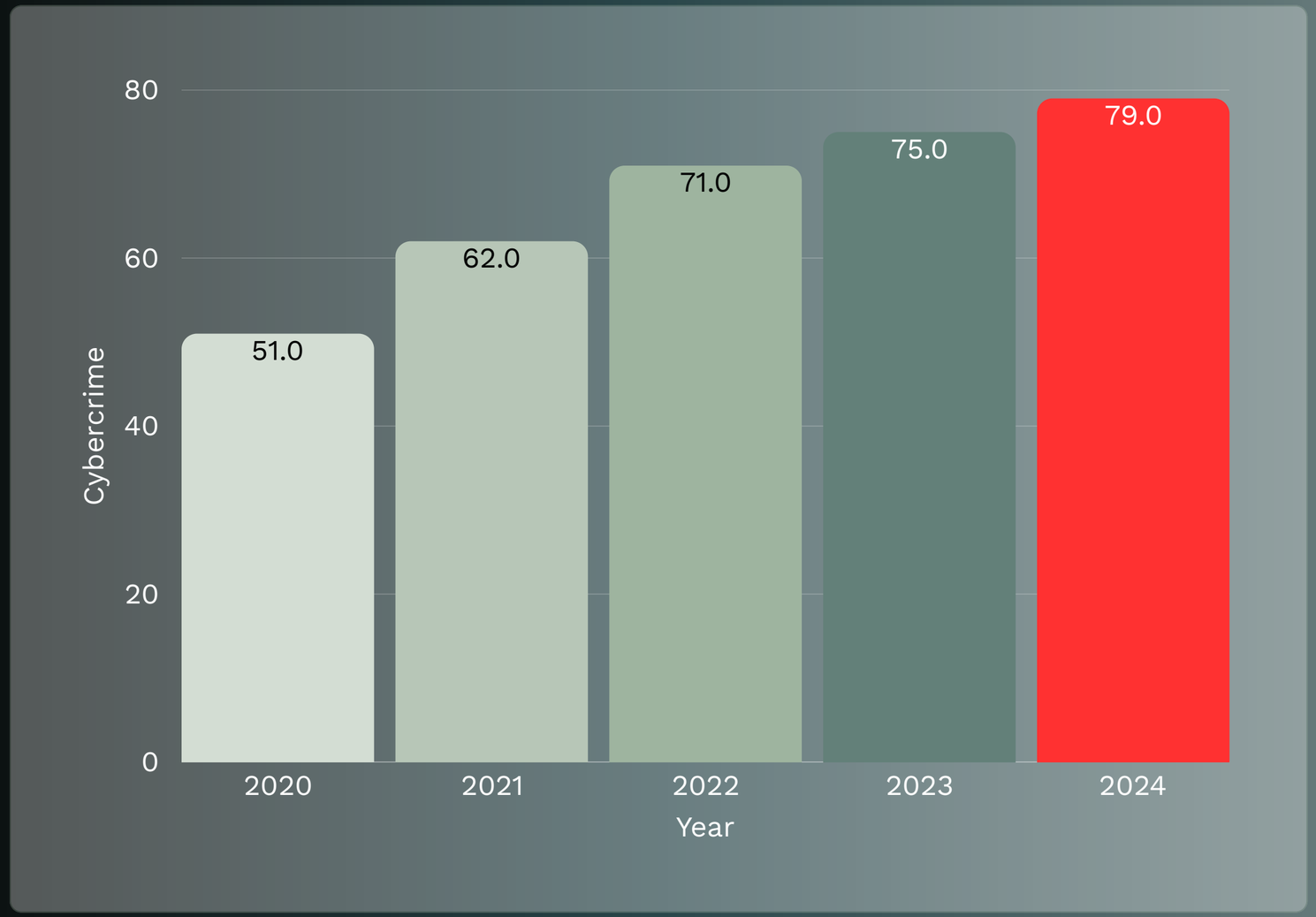
La ciberseguridad se refiere a las tecnologías, recursos humanos y prácticas utilizadas para mantener seguros los **sistemas informáticos, datos electrónicos y a las personas.**

« No somos un objetivo secundario.

Somos un objetivo primario y rentable. »

Tipos más comunes de ciberataques

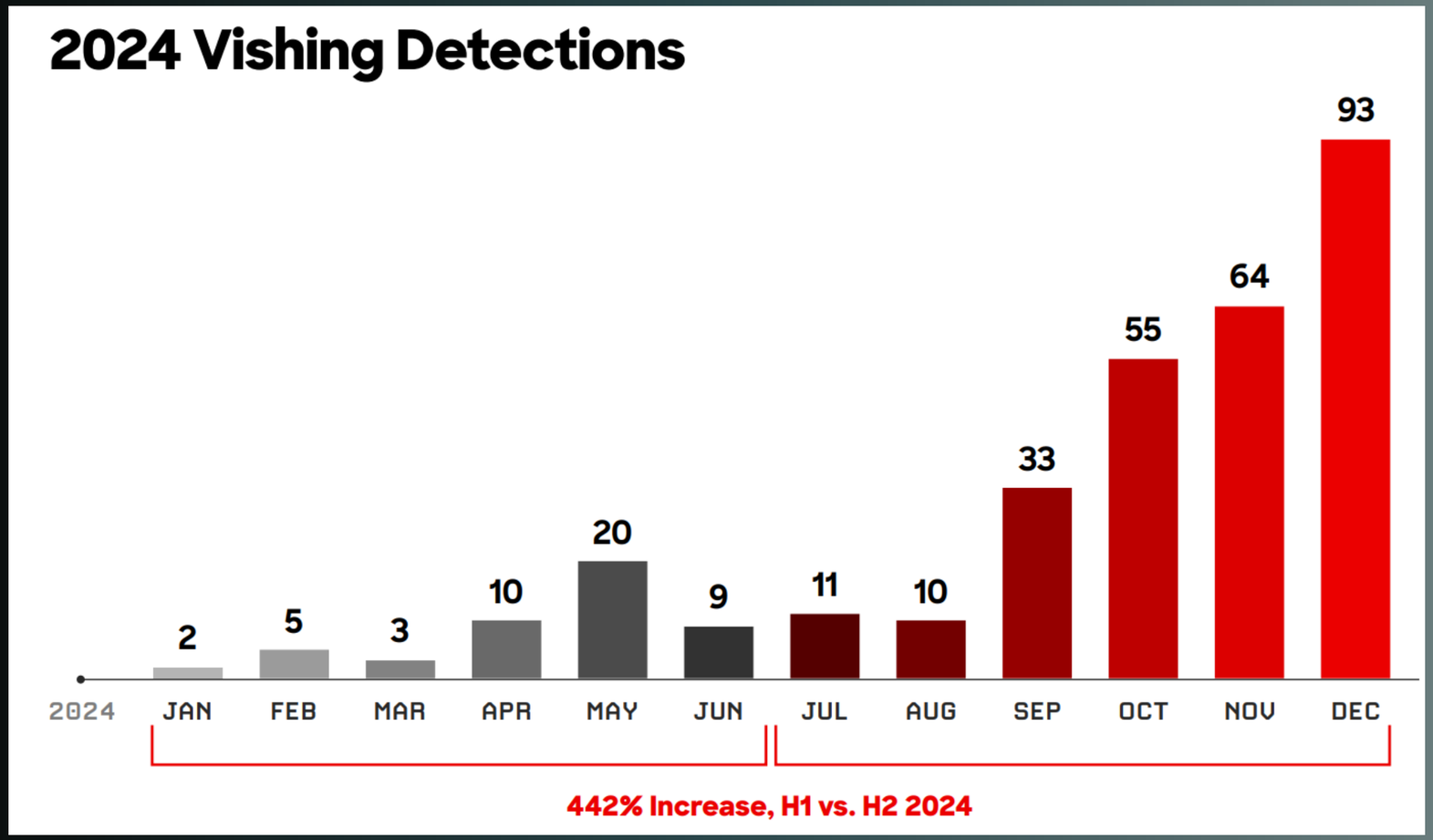
Tipo	Descripción
Ingeniería Social	Utiliza diversas técnicas como la suplantación de identidad para manipular a las personas y conseguir que compartan información confidencial o accedan a ella.
Phishing	Engaña a los usuarios para que revelen información personal o confidencial mediante (enlaces falsos.)
Ransomware	Bloquea o encripta los datos y exige un pago para desbloquearlos.



Fuente: CrowdStrike Global Threat Report 2025, CrowdStrike
Cost of a Data Breach Report 2025, The AI Oversight Gap. IBM

Volumen de ataques en aumento

Por segundo año consecutivo, los ataques internos maliciosos
generaron los costos promedio más altos por brechas de seguridad entre los vectores de amenaza iniciales: **USD 4,92 millones**. La vulneración de proveedores externos y la cadena de suministro
le siguieron de cerca con USD 4,91 millones. Otros vectores de ataque costosos incluyeron la explotación de vulnerabilidades y el phishing. **Sin embargo, el tipo de vector de ataque más frecuente en las organizaciones fue el phishing, con un 16%, con un costo promedio de USD 4,8 millones.**



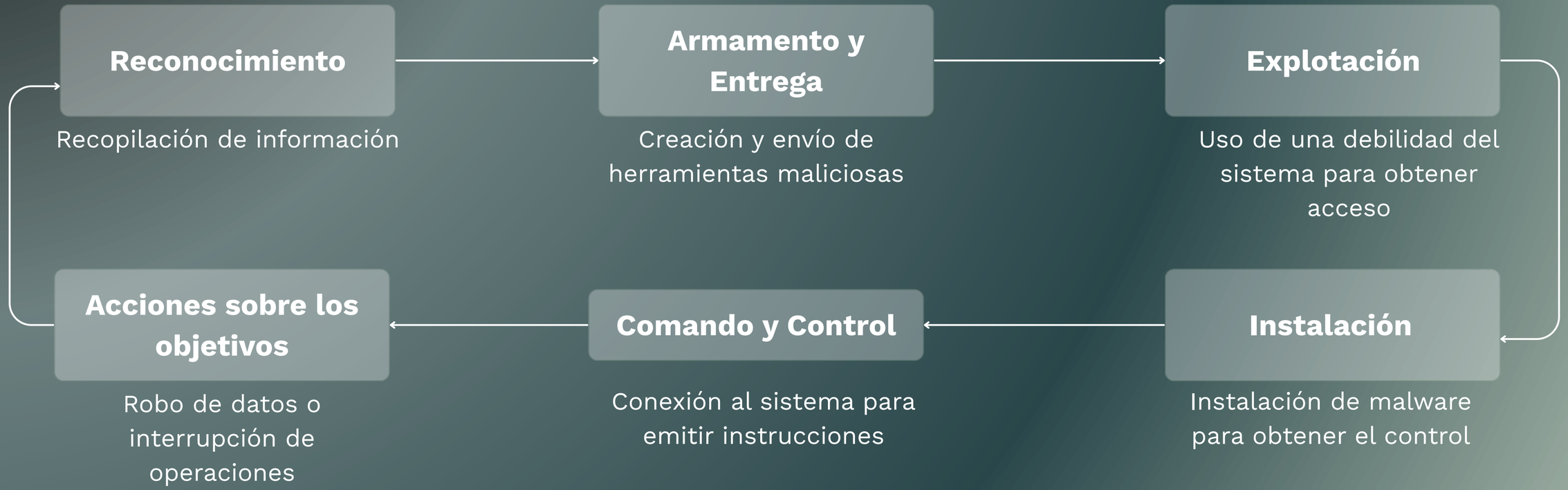
Volumen de ataques en aumento

En las campañas de vishing, los ciberdelincuentes llaman a los usuarios objetivo e intentan persuadirlos para que descarguen archivos maliciosos, establezcan sesiones de soporte remoto o introduzcan sus credenciales en páginas de phishing de tipo adversario en el medio (AITM).

Fuente: CrowdStrike Global Threat Report 2025, CrowdStrike

Ciclo de vida del ciberataque

Los ciberataques usualmente siguen las siguientes etapas:



Top 5

Phishing

(y sus variantes de Ingeniería Social)

Ataques a la Cadena de Suministro

(Terceros)

Amenazas Internas Maliciosas

Insiders

Compromiso de Credenciales Válidas

Abuso de Cuentas

Ataques Potenciados por IA

Deepfakes y Phishing Avanzado

Reforzar la Identidad como el Nuevo Perímetro:
MFA robusta y resistente al phishing

Adoptar una Defensa Proactiva contra la Ingeniería Social:
entrenar al personal para reconocer

Usar IA en Defensa:
herramientas de seguridad y automatizción

Cultura de "TI Saludable":
transformar la TI hacia una educación y discusión continua y activa.

¿Cómo nos defendemos?

De lo que no vemos...

Universidad de Costa Rica
Centro de Informática
Jornadas de Investigación **PROSIC** 2025

De amenazas invisibles a responsabilidad de todos

Estamos bajo asedio constante

Luis Loría Chavarría