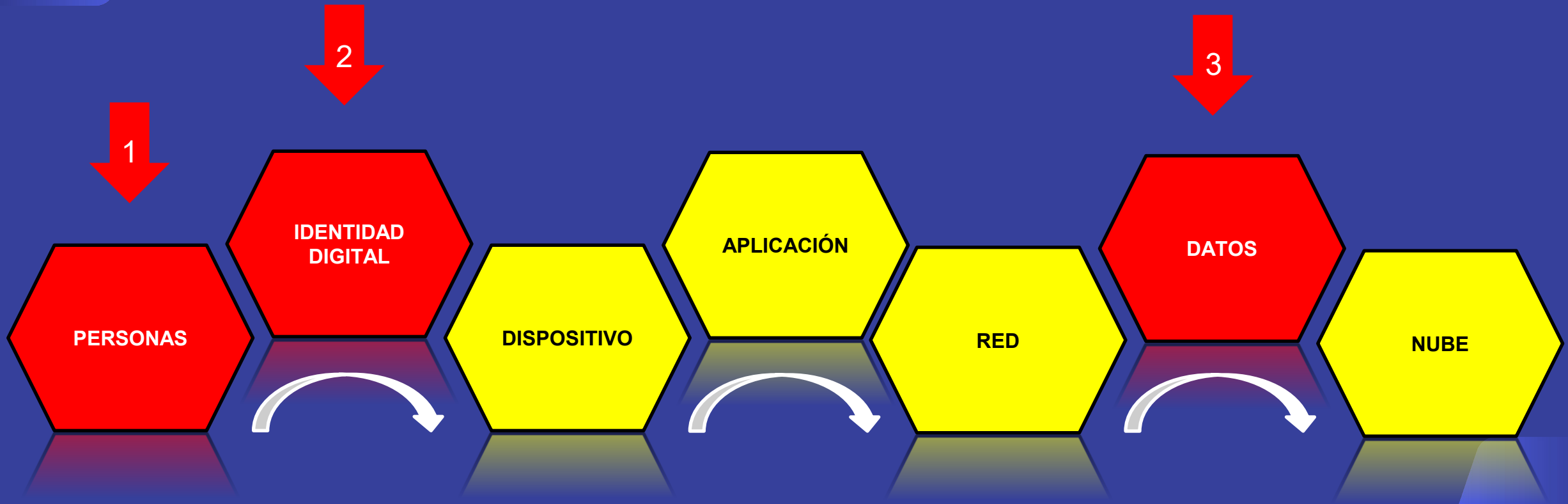
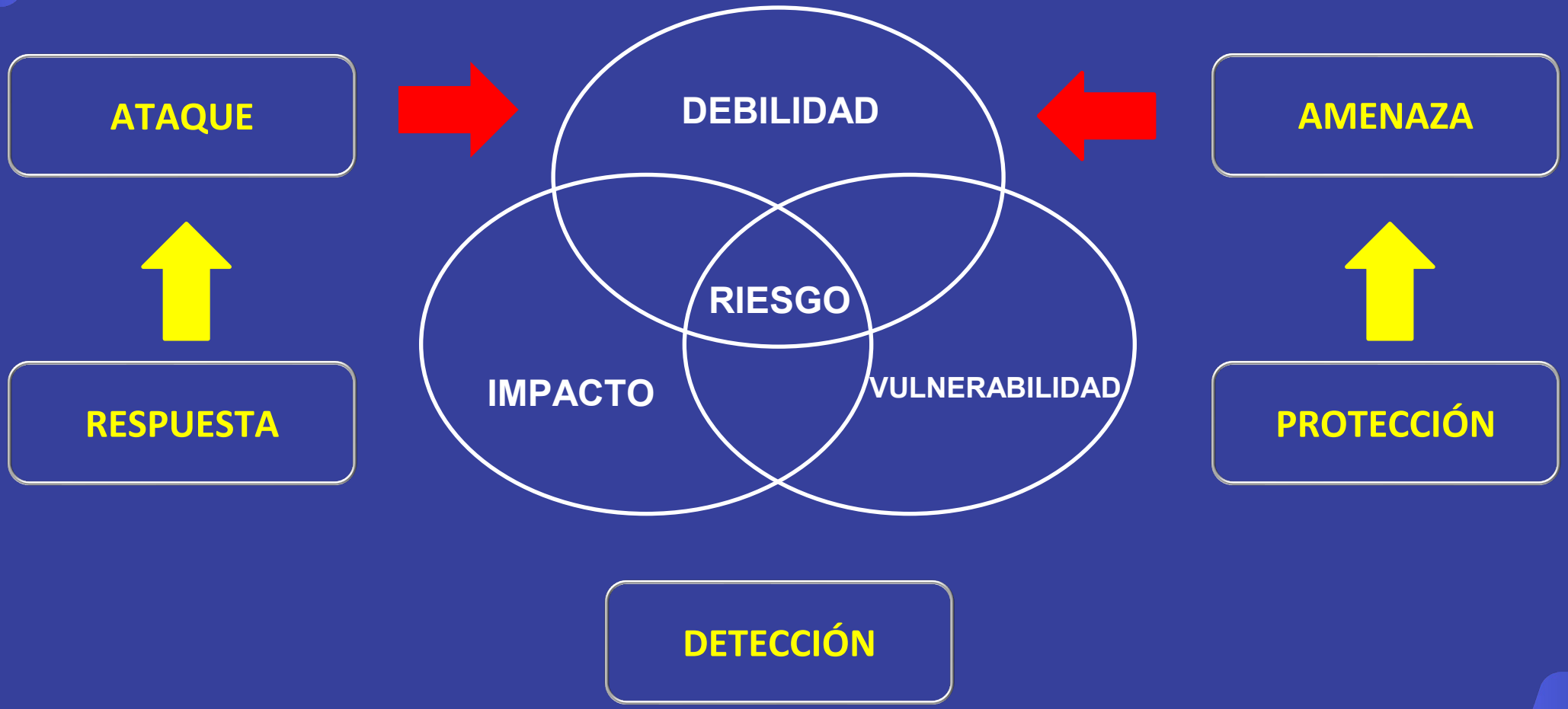
# Ingeniería Social

# CAPAS DE CIBERSEGURIDAD

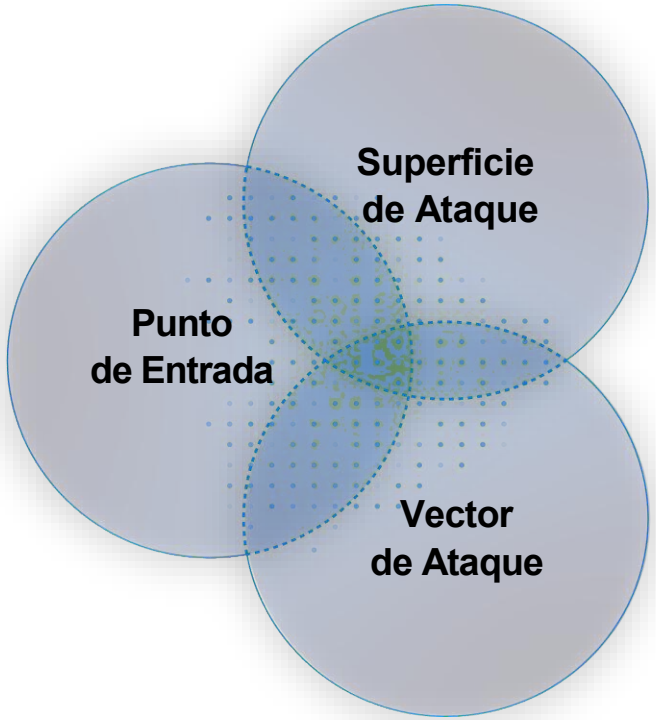
SEGURIDAD AMÉRICA.COM



# FACTORES DE CIBERSEGURIDAD



## ¿qué tan seguros están nuestros datos?




Qué datos son sensibles - Confidencialidad
Quién accede a los datos - Privilegios
Cómo se usan los datos - Disponibilidad y Actividad

SEGURIDAD AMÉRICA.COM

# Percepción de Riesgo

## Ejemplo de Industria

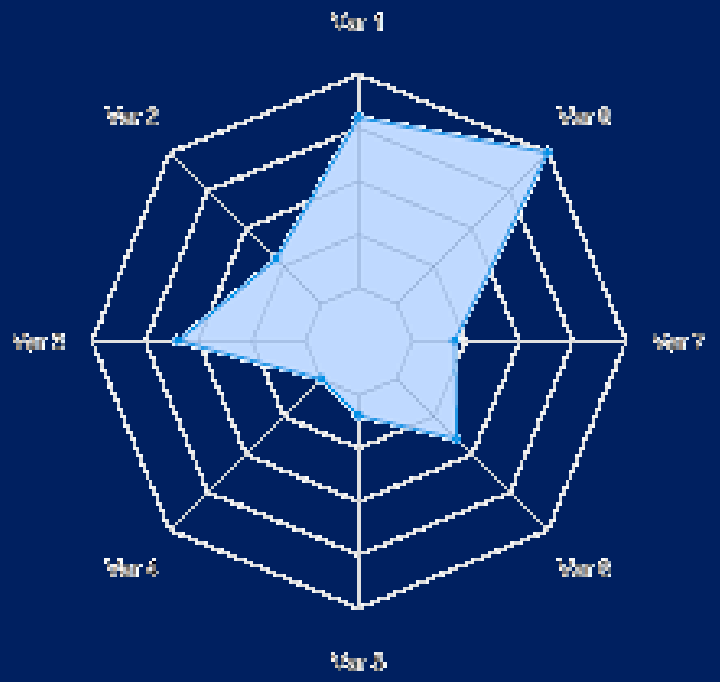
| | |
|---|---|
| PERSONAS | 4,8 |
| IDENTIDAD | 4,4 |
| DISPOSITIVOS | 2,3 |
| APPs & APIs | 3,4 |
| RED | 1,1 |
| DATOS | 4,0 |
| NUBE | 2,8 |

SOPORTE A USUARIOS / SOPORTE ARQUITECTURA

1 — 5

SEGURIDAD AMÉRICA.COM

SUPERFICIE DE ATAQUE (e.g.,)



| | | |
|---|---|---|
| PERSONAS | IDENTIDAD | DISPOSITIVOS |
| APPs y APIs | RED | DATOS |
| NUBE | | |

# CAPAS DE CIBERSEGURIDAD

SEGURIDAD AMÉRICA.COM

| CAPA | PERSONAS | IDENTIDAD DIGITAL | RED | DISPOSITIVOS | APLICACIONES | DATOS | ACTIVOS CRÍTICOS |
|---|---|---|---|---|---|---|---|
| OBJETIVO | Capacitar y sensibilizar a los usuarios en medidas contra la Ingeniería Social | Proteger red interna de amenazas del perímetro (internet). | Resguardar la infraestructura de la red interna. | Proteger dispositivos (equipos) individuales. | Asegurar que aplicaciones y APIs usadas estén libres de vulnerabilidades . | Proteger datos críticos donde sea que estén almacenados o transmitidos. | Priorizar la seguridad de acceso a dispositivos, redes y servidores. |
| | USER AWARENESS | IAM / THREAT PREVENTION | | | | DATA SECURITY | |

# CAPAS DE CIBERSEGURIDAD

SEGURIDAD AMÉRICA.COM

PUNTO ENTRADA

PERSONAS

IDENTIDAD DIGITAL

DATOS

| CAPA | Human Layer (User Attack Surface) | Identity & Access Layer | Data Layer |
|---|---|---|---|
| Goal | Reduce human-based entry points (social engineering). | Reduce identity-based attack surface | Reduce exposure of sensitive data |
| Risk | Phishing<br>Credential Theft<br>Social Engineering Attacks | Credential stuffing<br>Privilege escalation<br>Account takeover | Data exfiltration<br>Unauthorized access<br>Leakage |
| ASR Controls | Security Awareness Training<br>Phishing Simulations<br>Least Privilege Access<br>Restrict Macro Usage | Multi-Factor Authentication (MFA)<br>Least Privilege (RBAC)<br>Password Policies<br>Identity Monitoring | Data Classification<br>Encryption (at rest /in transit /in use)<br>Access Control Policies<br>Data Loss Prevention (DLP) |
| Outcome | Reduces human error as an entry-point | Protects most targeted entry point: credentials | Limits impact even if breach occurs |

# Ingeniería Social*

La ingeniería social es el proceso psicológico y conductual mediante el cual un atacante manipula, induce, influye, o engaña a individuos para que revelen datos confidenciales, otorguen acceso no autorizado o realicen acciones que comprometan la seguridad de sistemas, datos, personas y organizaciones.

Se basa en principios de persuasión, sesgos cognitivos, explotación de la confianza y manipulación del comportamiento humano, más que en vulnerabilidades técnicas.

*** Primer uso registrado del término "social engineering"**: **1894**, en un ensayo de J.C. van Marken.

SEGURIDAD AMÉRICA.COM

# En ciberseguridad

La ingeniería social es el conjunto de técnicas empleadas para inducir o influir en comportamientos o decisiones que permitan eludir mecanismos de seguridad, aprovechando la confianza, el error humano o la falta de conciencia del usuario.

Un artículo de 1995 titulado *"Cracking a Social Engineer"* en la revista **LAN Times** ya empleaba este término en ese sentido.

**Identidad Digital** (propósito)

Verificar quien eres.

Verifica quien eres en el mundo digital buscándote en alguna fuente de verdad.

**Autenticación** (propósito)

Confirma que realmente eres quien dices ser.

Confirma quien eres con algo que:

- Sabes
- Tienes
- Eres
- Haces
- o lugar donde estás

# Incidentes de Seguridad

Nueve de cada diez (9/10) incidentes de seguridad relacionados con la **Identidad Digital** y **Autenticación** de un usuario tienen su origen en un intento exitoso de ataque o fraude mediante Ingeniería Social.

## Ataque Emocional

| + | − |
|---|---|
| Alegría | Tristeza |
| Confianza | Asco |
| Miedo | Ira |
| Sorpresa | Expectación |

Miedo + Sorpresa = Alarma

# Malware *

(Malicious Software)

Malware es la categoría general de cualquier software malicioso diseñado para causar daño, infiltrar, o comprometer sistemas.

Como ejemplo se puede citar el **Ransomware** como un tipo de malware extorsivo diseñado para denegar el acceso a datos, sistemas o dispositivos generalmente mediante cifrado o bloqueo.

* The Evolution of Malicious Code by **Yisrael Radai y Yitzhak Ben-Israel** en 1990 - Universidad Hebrea de Jerusalén

## Ejemplos de Malware

- Phishing
- Ransomware
- Virus
- Gusanos
- Troyanos
- Spyware
- Rootkits

# Ataques de Ingeniería Social - Correos de Phishing -

El phishing como malware es exitoso porque explota emociones humanas en lugar de debilidades técnicas de un sistema.

Utiliza la ingeniería social para manipular a las personas mediante el miedo, curiosidad, urgencia, o confianza.

El de costo de implementar correos de phishing es prácticamente cero.

SEGURIDAD AMÉRICA.COM

## Razones de su efectividad

- **Urgencia y miedo:** Los atacantes presionan a las víctimas con mensajes de cuentas bloqueadas, multas inminentes o encomiendas retenidas. Esto anula el pensamiento crítico e induce a una acción rápida.

- **Personalización extrema:** A través del *spearphishing*, los estafadores investigan a sus objetivos en redes sociales (como LinkedIn o Instagram) para crear mensajes altamente creíbles que parecen provenir de jefes, bancos o entidades oficiales.

- **Tecnología e Inteligencia Artificial:** La IA generativa permite a los cibercriminales redactar correos electrónicos impecables sin faltas de ortografía, automatizar el envío de mensajes y clonar voces reales para estafas telefónicas.

- **Diversificación de plataformas:** Ya no se limita solo al correo electrónico. Los ataques se despliegan de forma masiva en SMS, WhatsApp, redes sociales e incluso aplicaciones de mensajería corporativa.

- **Falsificación visual:** Crean páginas web o aplicaciones falsas que son copias exactas de las originales, engañando incluso a usuarios experimentados.

# Ingeniería Social Señales de Alerta

## DE

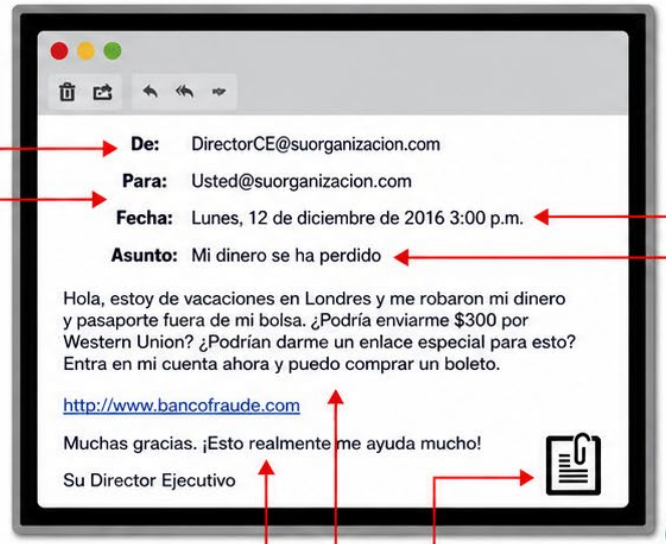
- No reconozco la dirección de correo electrónico del **remitente como alguien** con quien normalmente me comunico.
- Este correo es de alguien **fuera de mi organización y** no está **relacionado con** mi trabajo.
- Este correo fue enviado desde **dentro** de mi organización, pero de un cliente, proveedor **o socio, y es muy inusual o fuera de carácter.**
- La dirección de correo del remitente **proviene de un dominio sospechoso** (como **microsoft-support.com**)?
- **No conozco personalmente al remitente** y no fui presentado por alguien de confianza.
- **No tengo una relación comercial real** ni comunicaciones anteriores con el remitente.
- Este es un correo **inesperado o inusual con un hipervínculo incrustado o un archivo adjunto de alguien con quien no he comunicado recientemente.**

## PARA

- Se me envió un correo a mí y a otras personas, pero no conozco personalmente a las otras personas a quienes se envió.
- Recibí un correo que también fue enviado **a una mezcla inusual de personas.** Por ejemplo, podría haberse enviado a un grupo aleatorio de personas de mi organización cuyos nombres comienzan con la misma letra, o a toda una lista de direcciones no relacionadas.

## HIPERVÍNCULOS

- Paso el mouse sobre un hipervínculo que aparece en el mensaje de **correo electrónico, pero el enlace me dirige a un sitio web diferente. (Esta es una gran señal de alerta roja).**
- Recibí un correo electrónico que solo tiene hipervínculos largos sin más información y el resto del correo está completamente en blanco.
- Recibí un correo con un **hipervínculo** que es **una mala escritura** de un sitio web conocido. Por ejemplo, **www.banKodarmerica.com** — la "m" son en realidad dos caracteres: — "r" y "n".




## FECHA

- ¿Recibí un correo electrónico que normalmente recibiría durante el horario laboral habitual, pero **fue enviado en un momento inusual** como a las 3:00 a.m.?

## ASUNTO

- ¿Recibí un correo electrónico con una línea **de asunto** que es **irrelevante o no coincide** con el contenido del mensaje?
- ¿Es el mensaje de correo electrónico una respuesta a algo que nunca envié ni solicité?

## ARCHIVOS ADJUNTOS

- El remitente incluyó un archivo adjunto de correo electrónico que no **esperaba o que no tiene sentido** en relación con el mensaje de correo electrónico. (Este remitente normalmente no envía este tipo de adjunto).
- Veo un archivo adjunto de un **tipo de archivo posiblemente peligroso.** El único tipo de archivo que siempre es seguro para hacer clic es **.txt.**

## CONTENIDO

- ¿El remitente me pide que **haga clic en un enlace o abra un archivo adjunto** para **evitar una consecuencia negativa o para obtener algo de valor?**
- ¿Está el correo lleno de **errores gramaticales u ortográficos?**
- ¿El remitente me pide **hacer clic en un enlace o abrir un archivo adjunto que me parece extraño o ilegal?**
- ¿Tengo una sensación **incómoda acerca** de la solicitud del remitente de abrir un archivo adjunto o hacer clic en un enlace?
- ¿El remitente me pide que **mire una imagen comprometida o vergonzosa** de mí mismo o de alguien que conozco?

# 20 FORMAS DE BLOQUEAR ATAQUES MÓVILES

**No bajes la guardia solo porque estás usando un dispositivo móvil. ¡Sé tan cuidadoso como lo serías en un computador de escritorio!**

## WiFi

- No permitas que tu dispositivo se conecte automáticamente a redes desconocidas.
- Apaga el WiFi cuando no lo estés utilizando o no lo necesites.
- Nunca envíes información sensible a través de WiFi, a menos que estés completamente seguro de que es una red segura.

## Aplicaciones

- Utiliza únicamente aplicaciones disponibles en la tienda oficial de tu dispositivo. **Nunca descargues aplicaciones desde el navegador.**
- Desconfía de aplicaciones de desarrolladores desconocidos o con pocas/malas reseñas.
- Mantén las aplicaciones actualizadas para garantizar que cuenten con las últimas medidas de seguridad.
- Si una aplicación ya no recibe soporte o actualizaciones, elimínala.
- No otorgues permisos de administrador ni privilegios excesivos a aplicaciones, a menos que realmente confíes en ellas.

## Navegador

- Ten cuidado con anuncios, sorteos y concursos que parezcan demasiado buenos para ser verdad. A menudo conducen a sitios de phishing que aparentan ser legítimos.
- Presta mucha atención a las URL. En pantallas móviles es más difícil verificarlas, pero vale la pena hacerlo.
- Nunca guardes tus credenciales de acceso cuando navegues desde un navegador web.


## Bluetooth

- Desactiva el emparejamiento automático por Bluetooth.
- Mantén Bluetooth apagado cuando no lo necesites.

## Smishing (Phishing por SMS)

- No confíes en mensajes que intenten obtener información personal.
- Ten cuidado con tácticas similares en plataformas como WhatsApp, Facebook Messenger, Instagram y otras aplicaciones de mensajería.
- Trata estos mensajes igual que tratarías un correo electrónico sospechoso: piensa antes de hacer clic.

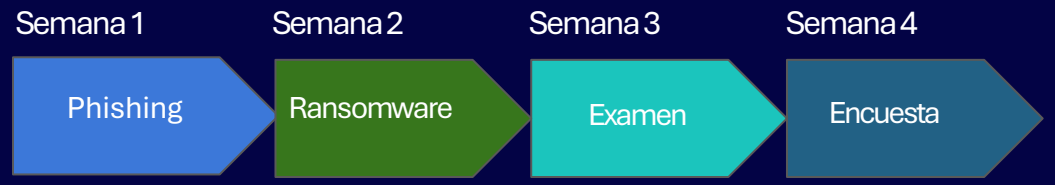
## Vishing (Phishing por Voz)

- No respondas solicitudes telefónicas o por correo electrónico que pidan información financiera o personal.
- Si tienes dudas, contacta directamente a la institución financiera utilizando el número oficial que aparece en tu tarjeta o estado de cuenta.
- Nunca hagas clic en enlaces incluidos en correos comerciales no solicitados.
- Proporciona información de cuentas únicamente a personas reales y solo cuando tú hayas iniciado la llamada.
- Instala herramientas que te ayuden a identificar si un sitio web es legítimo o fraudulento.

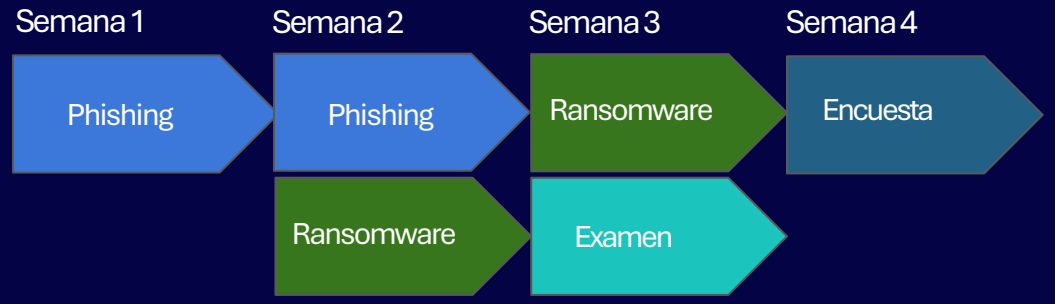
**La seguridad móvil depende tanto de la tecnología como de los hábitos de los usuarios.**
**Mantener buenas prácticas puede prevenir la mayoría de los ataques dirigidos a dispositivos móviles.**

# Línea Base/Diagnóstico

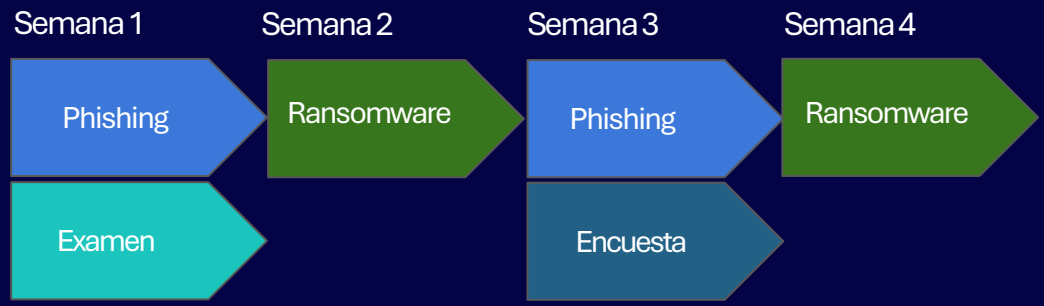
## Opción 1



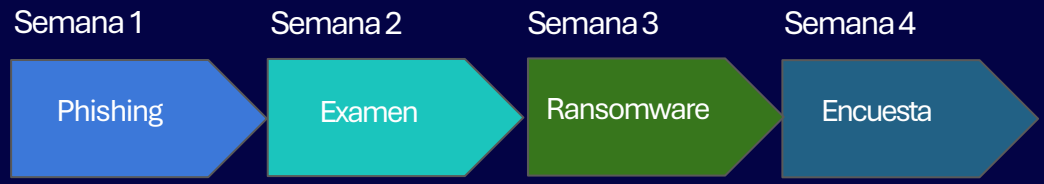

## Opción 2




## Opción 3




## Opción 4



SEGURIDAD AMÉRICA.COM

# FIN

# Ingeniería Social