

Ciber Seguridad

2026

Presentada por:

Ing. Oscar Pérez



Sitio Web
www.norboy.coop



¿QUÉ RECORDAMOS DE 2025?

Phishing: Mensajes o correos falsos que buscan engañarnos.

Malware: Programas o archivos que pueden afectar nuestros equipos o información.

Suplantación: Alguien intenta hacerse pasar por una persona o entidad conocida.

Información sensible: Datos que requieren especial protección.

“La mayoría de los ataques necesitan que alguien haga algo: abrir, responder, descargar, entregar información o autorizar.”

DETÉNGASE → VERIFIQUE → ACTÚE



LAS AMENAZAS CAMBIARON

MENSAJE ANTIGUO

**"URGENTE!!
su cuenta esta bloqueada
haga CLICK aki"**

MENSAJE ACTUAL

"Buenos días, Margarita. Estamos actualizando los permisos de acceso al sistema. Para evitar inconvenientes durante la jornada, agradecemos confirmar su cuenta corporativa en el siguiente enlace."

"Un mensaje bien escrito también puede ser falso"

¿CUÁL PARECE MÁS PELIGROSO?

La apariencia profesional ya no es una señal suficiente para validar un mensaje.

INGENIERÍA SOCIAL: EL ATAQUE EMPIEZA POR LA PERSONA

Manipular a alguien para conseguir información o lograr que realice una acción.



Urgencia

"Necesito esto inmediatamente."



Miedo

"Su cuenta será bloqueada."



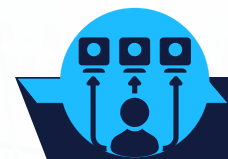
Oportunidad

"Ha recibido un beneficio."



Autoridad

"Lo solicita Gerencia."



Curiosidad

"Revise este documento."



Los atacantes buscan que reaccionemos antes de pensar.

DETÉNGASE → VERIFIQUE → ACTÚE

EL PHISHING YA NO LLEGA SOLAMENTE POR CORREO



✓ SMS → Smishing

✓ Correo

✓ Llamada → Vishing

✓ WhatsApp → Suplantación

✓ Código QR → QRishing



Su cuenta presenta un
movimiento pendiente.
Ingrese aquí para verificar.
<https://seguridad-norboy.co>

INTELIGENCIA ARTIFICIAL, VOCES FALSAS Y DEEPFAKES

CASO SIMULADO NORBOY

Recibe un audio que aparentemente corresponde a un directivo:

"Estoy en reunión. Necesito que me envíe inmediatamente el archivo de asociados. No puedo recibir llamadas."

REGLA: Si la solicitud es inusual o sensible, confirme por un segundo canal.

DETÉNGASE → VERIFIQUE → ACTÚE



Imágenes y documentos aparentes



Videos manipulados



Mensajes muy bien redactados



Imitaciones de voz



Perfiles y conversaciones falsas

SUPLANTACIÓN DE DIRECTIVOS Y PROVEEDORES



01

Urgencia

02

**Cambio de
procedimiento**

03

Solicitud Financiera

04

**Imposibilidad
de verificar**

05

**Posible
suplantación**

CONTRASEÑAS ROBADAS Y AUTENTICACIÓN EN DOS PASOS

AUTENTICACIÓN EN DOS PASOS (2FA)
Aunque alguien conozca mi contraseña,
necesita una segunda verificación para
ingresar.

NUNCA comparta códigos de verificación
recibidos por SMS, WhatsApp, correo o
aplicaciones de autenticación.



DETÉNGASE → VERIFIQUE → ACTÚE

RANSOMWARE CUANDO LA INFORMACIÓN QUEDA SECUESTRADA

1. 8 a.m.

Un funcionario abre un archivo aparentemente normal.

2. 8:15 a. m.

Los documentos comienzan a cambiar de nombre.

3. 8:30 a. m.

Varias carpetas dejan de abrir.

Un programa malicioso puede bloquear equipos o cifrar archivos.



LA INFORMACIÓN DE NORBOY Y LAS HERRAMIENTAS DE IA

PARECE INOFENSIVO:

“Voy a copiar este documento en una herramienta de IA para que me lo resuma.”

Datos de asociados

Información financiera

Decisiones internas

Contratos y documentos

Información crediticia



DETÉNGASE → VERIFIQUE → ACTÚE

CELULAR, WHATSAPP Y CÓDIGOS DE SEGURIDAD



**"Le llegó un código por SMS,
¿me lo puede enviar?"**

**Este es mi nuevo número,
agrégume."**

**Escanee este QR para
confirmar la cuenta."**

**Descargue esta aplicación
para continuar."**

¿QUÉ HAGO SI YA HICE CLIC?

Abrí un enlace sospechoso
Deténgase y reporte.

Ingresé mi contraseña
Reporte inmediatamente.

Abrí un archivo extraño
Deje de trabajar en el equipo y comuníquese con
Sistemas.

Compartí información
Indique exactamente qué información entregó.

Mi computador se comporta extraño
Reporte antes de intentar repararlo.



DETÉNGASE → VERIFIQUE → ACTÚE

CASOS REALES RECIENTES EN COLOMBIA

Bancolombia – falsos asesores de seguridad (2025)
Llamadas que simulaban alertas de movimientos y luego dirigían a enlaces falsos para obtener credenciales.

Banco Caja Social – vishing y cambiazo (2026)
Falsos asesores utilizaron llamadas, mensajeros y suplantación para obtener tarjetas o información financiera.

COLCERT – campañas de phishing (2025)
Se identificaron campañas con kits especializados para crear sitios falsos y capturar credenciales.

Sistema financiero colombiano – 2025
La Superintendencia Financiera reportó cerca de 27.000 millones de ataques cibernéticos en el primer semestre de 2025.

Los ataques actuales muchas veces buscan vulnerar a la persona que tiene acceso a la información o al sistema.





Gracias, por su atención

Soporte



Telefono
3134127040



Sitio Web
www.norboy.coop

DETÉNGASE → VERIFIQUE → ACTÚE



NORBOY

SOMOS SU FUTURO

