ISACA Costa Rica Chapter

ISACA COMMUNITY DAY
PEOPLE | SERVICE | PURPOSE
3 de Octubre

# ¡Alerta!
# ¿Cómo prevenir los fraudes digitales?


**Lic. Freddy Roca Abarca**

Seguridad de la Información, Banco Popular y de Desarrollo Comunal

Licenciado en Informatica con efasis en Gerencia Informática

CISA, CISM, CDPSE, ISO 27005-LI, ISO 27001-LI, COBIT-F e ITIL-F

# Fraude Digital /Delito Informático

El **“fraude digital”** o **“ciberfraude”,** se refiere al fraude realizado a través del uso de la informática o del Internet.

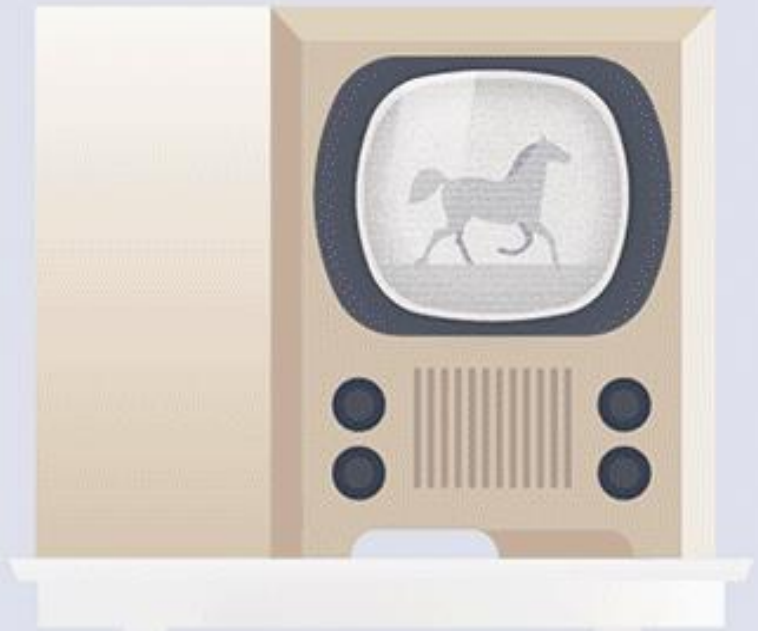
Un **"delito informático"** o "**ciberdelito**" es toda acción **antijurídica** y culpable a través de vías informáticas **(instrumento)** o que tiene como **objetivo** destruir, alterar y/o dañar sistemas de información.

## Leyes, convenios y estrategias:

- ✓ (07/12) Ley 9048 de **Delitos Informáticos**.
- ✓ (05/17) Convenio internacional **Budapest**.
- ✓ (10/17) **Estrategia Nacional** de Ciberseguridad.

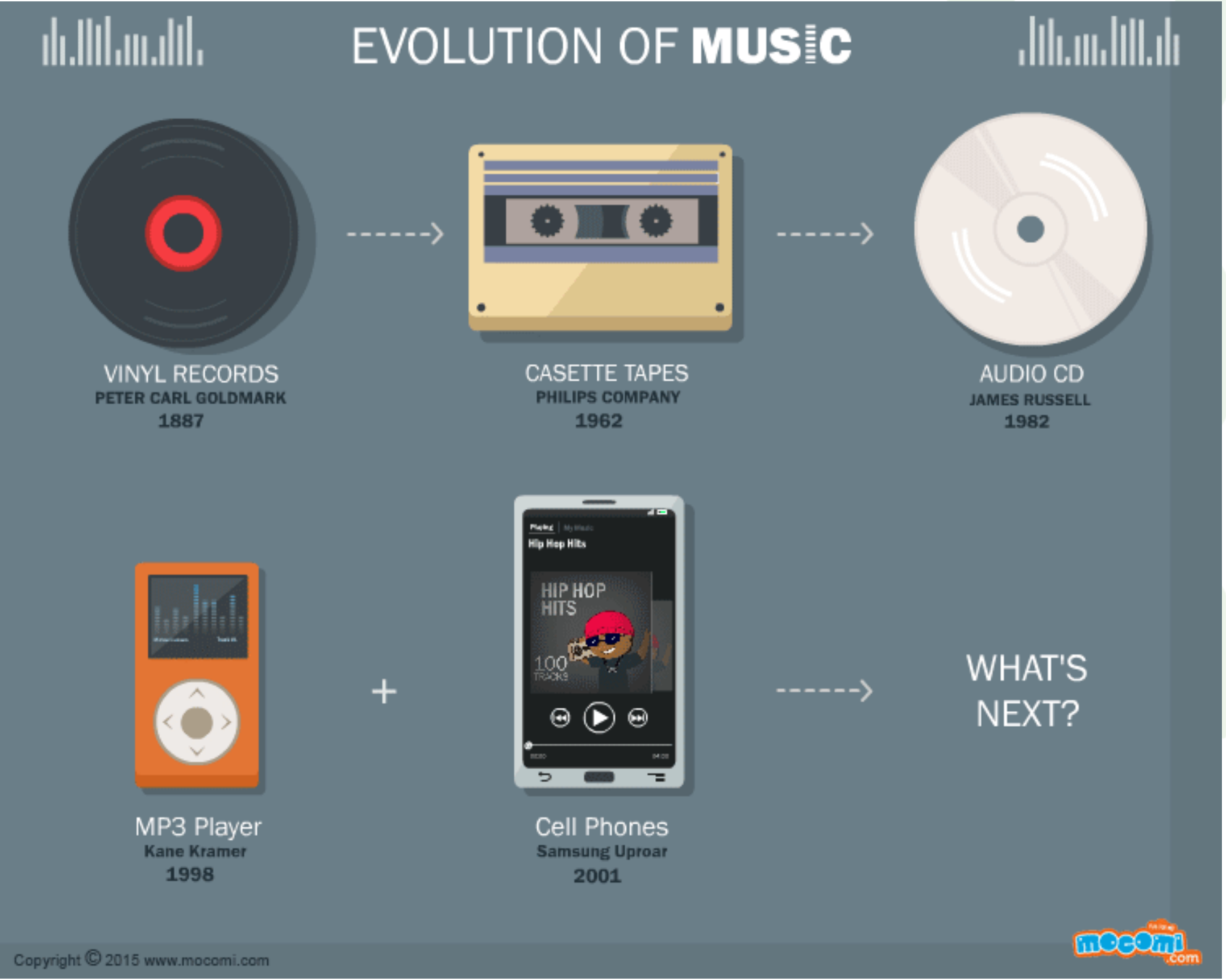
ISACA Costa Rica Chapter

# Evolución de la tecnología



ISACA
Costa Rica Chapter

# Evolución de la tecnología




ISACA Costa Rica Chapter

# Evolución de la tecnología


Motorola MicoTac from 1991

ISACA
Costa Rica Chapter

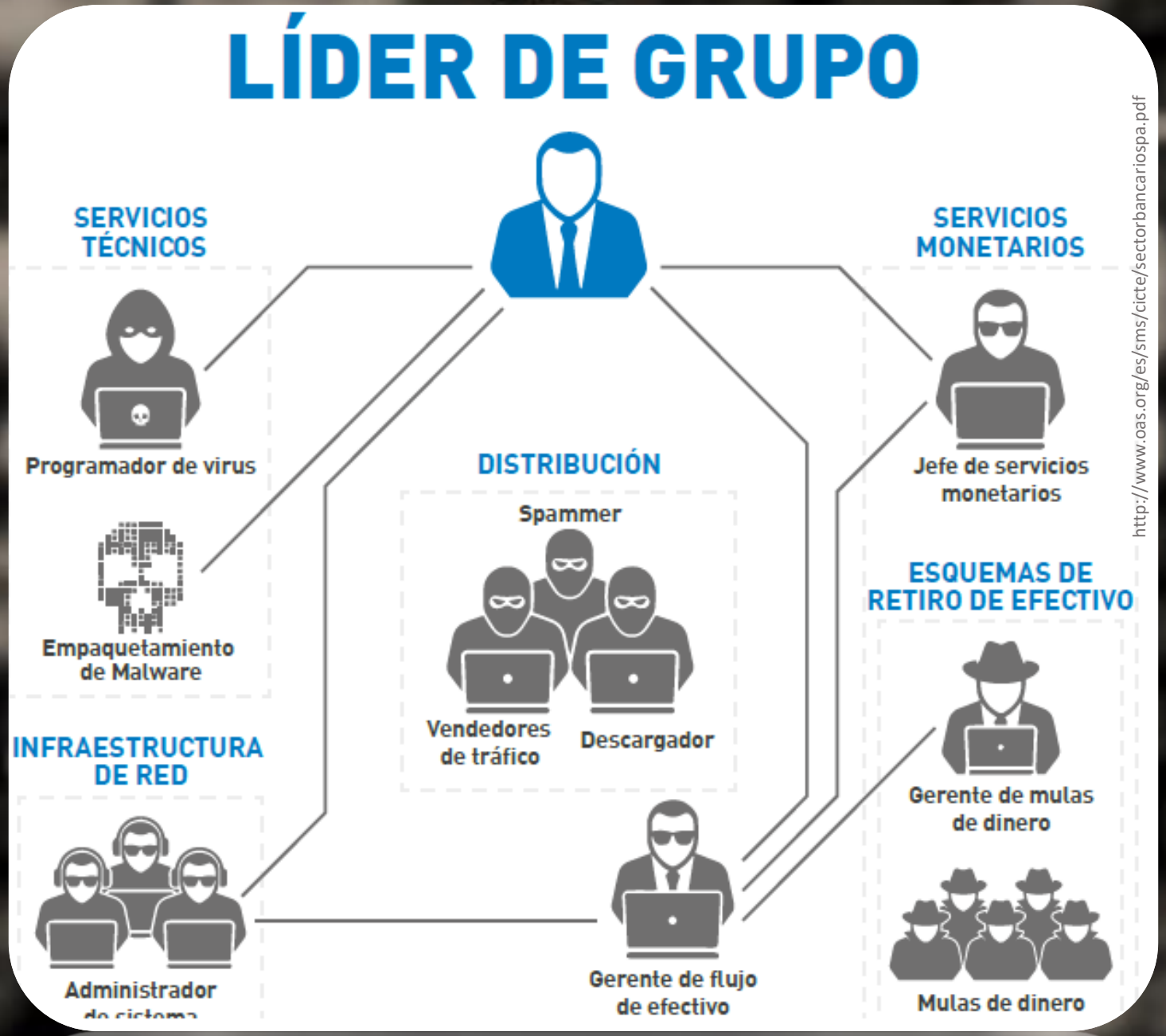
# Evolución de la tecnología


1980

ISACA
Costa Rica Chapter

# Evolución del Cibercrimen

# LÍDER DE GRUPO




http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

# Modo de Operación

## Identificación:

Los cibercriminales **identifican un objetivo y tratan de detectar** cualquier oportunidad para realizar un **fraude digital**.

## Ataque:


Buscan obtener información sensible (**usuarios, claves, códigos, información de tarjetas y datos personales**), para ello aprovechan diversas técnicas de Ingeniería Social, Suplantación (Phishing), Correos Falsos, Llamadas Telefónicas, Intercepción de Datos (Man in the Middle), Software Malicioso, entre otros.

## Monetización:

Pueden obtener beneficios **vendiendo la información** obtenida, y también por la **apropiación de credenciales y códigos de acceso para generar fraude digital**.

ISACA
Costa Rica Chapter


# ¿Cuáles son y cómo prevenir los fraudes digitales?

## 4 +Comunes

# Aumentan casos de intentos de estafas bancarias

Desde agosto se ha presentado un incremento en las denuncias por llamadas telefónicas y correos electrónicos en los que personas inescrupulosas solicitan datos en nombre del Banco Central de Costa Rica.

El Banco Central de Costa Rica (BCCR) alerta al público en general sobre el aumento de intentos de estafa, tanto por la vía telefónica como por correo electrónico, en los cuales personas inescrupulosas se hacen pasar por supuestos funcionarios de la Institución, con el fin de obtener datos como números de cuentas bancarias y claves de acceso.

https://www.bccr.fi.cr/seccion-comunicados-de-prensa/ComunicadosPrensa/Aumentan%20casos%20de%20intentos%20de%20estafas%20bancarias.aspx

El Observador

VISIÓN PAÍS TODO POLÍTICA RETINA ECONÓMICA LENTE MUNDIAL DEPORTES AVENIDA O DESDE LA COLUMNA BUENAS NOTICIAS BBC

DESTACADO VISIÓN PAÍS

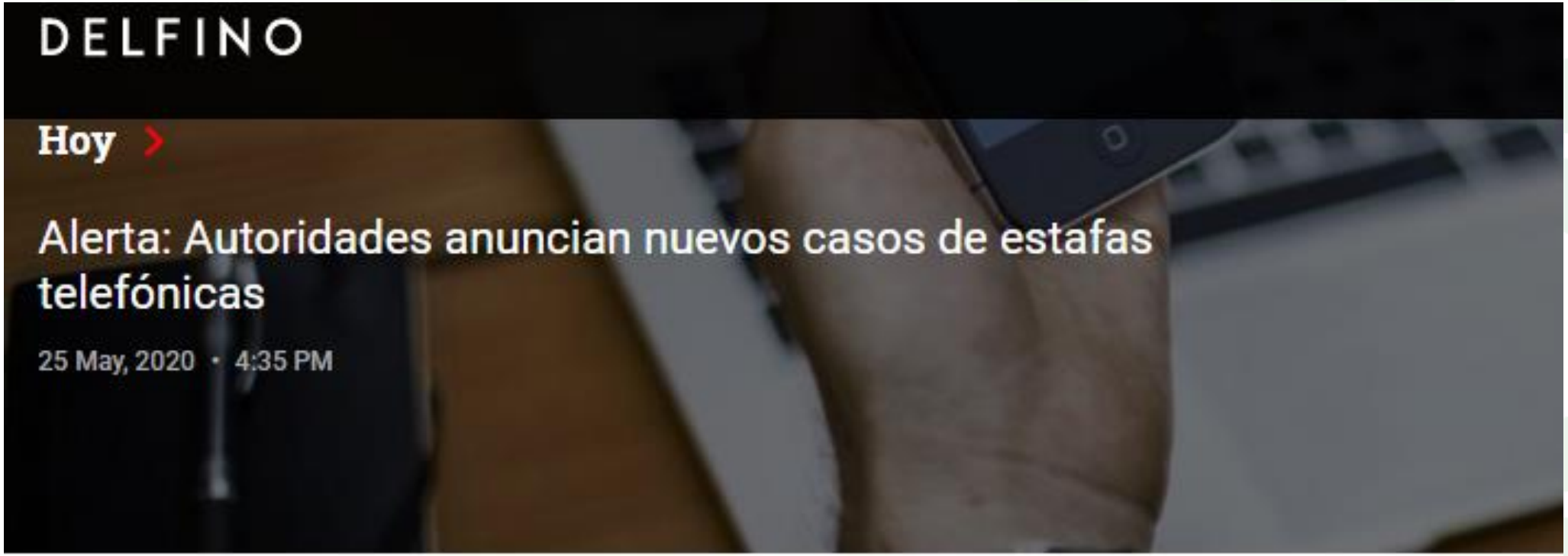
# Fraude telefónico de “falso funcionario público” provocó pérdidas de ¢500 millones solo en San José

Estafadores se identifican como funcionarios de Hacienda y dicen que detectaron rebajas en salarios o que serán exonerados de impuestos

Por PAULA UMAÑA - 10:50 AM 13 MAYO, 2020

https://observador.cr/noticia/fraude-telefonico-de-falso-funcionario-publico-provoco-perdidas-de-%C2%A2500-millones-solo-en-san-jose/

ISACA Costa Rica Chapter




El **Ministerio de Economía, Industria y Comercio** (MEIC) informó el día de hoy que personas inescrupulosas han estado realizando **estadas telefónicas**, haciéndose pasar por funcionarios de la institución y hacen que el usuario se conecte en diversas páginas y le piden a las personas que introduzcan información confidencial de sus cuentas bancarias.

https://delfino.cr/2020/05/alerta-autoridades-anuncian-nuevos-casos-de-estafas-telefonicas

ISACA
Costa Rica Chapter

# 1 Fraude mediante Llamada del Falso Funcionario

## Método:

Mediante llamadas telefónicas los atacantes **suplantan funcionarios(as) y números de teléfonos** de instituciones financieras y gubernamentales, utilizando **engaños** relacionados con FCL, ROP, Seguros, Firma Digital, Sorteos, Transacciones Bloqueadas, Supuestos Intentos de Fraude, Impuestos, Bono Proteger, **etc, etc, y etc**.

Solicitan información de **usuarios, contraseñas, códigos de seguridad, información de tarjetas e ingresar en enlaces de mensajes, correos o sitios falsos** para suministrar la información.

## Consejos:

1. **Desconfié** de toda llamada, correo o mensaje de texto que no espera.
2. No acceda ante la **presión** de una llamada telefónica.
3. Nunca **ingrese sus credenciales de acceso o códigos de seguridad** en sitios web que le indiquen.
4. **No instale** ningún software o aplicación que le indiquen en su PC o Celular.
5. No intente **evidenciar** que es un posible fraude o **increpar** al delincuente.
6. Ante la mínima duda **cuelgue inmediatamente y contacte directamente a la entidad.**

ISACA Costa Rica Chapter

SOLUCIONES PARA PROFESIONALES
LA REPUBLICA .net

ÚLTIMA HORA

# Casi un 50% de los ataques de phishing ocurren a smartphones

Johnny Castro johnnycastro.asesor@larepublica.net | Martes 04 agosto, 2020 10:34 am


ISACA
Costa Rica Chapter

# 2 Fraude mediante *"Phishing"* (Páginas de internet que suplantan sitios oficiales)


## Método:

A través de redes sociales, anuncios en buscadores de internet, correos electrónicos, mensajes texto, WhatsApp, entre otros.

Envían o anuncian enlaces para ingresar en sitios falsos donde roban información de **usuarios, contraseñas, códigos de seguridad o información de tarjetas**.

## Consejos:

1. Nunca ingrese mediante **enlaces, buscadores o anuncios a sitios web transaccionales** financieros.
2. **Desconfié de mensajes** con información de supuestos premios o contenido intimidante (plazos cortos, bloqueos, sanciones, etc), además, si presentan **faltas de ortografía.**
3. **Digite siempre la dirección** del sitio web oficial de su Institución financiera en el navegador de internet.
4. Nunca abra los **archivos adjuntos** de correos o mensajes que usted no espera.
5. Verifique siempre el saldo previo y posterior a sus transacciones para detectar **movimientos sospechosos.**
6. Ante la mínima duda **contacte directamente a su entidad** financiera.

ISACA Costa Rica Chapter

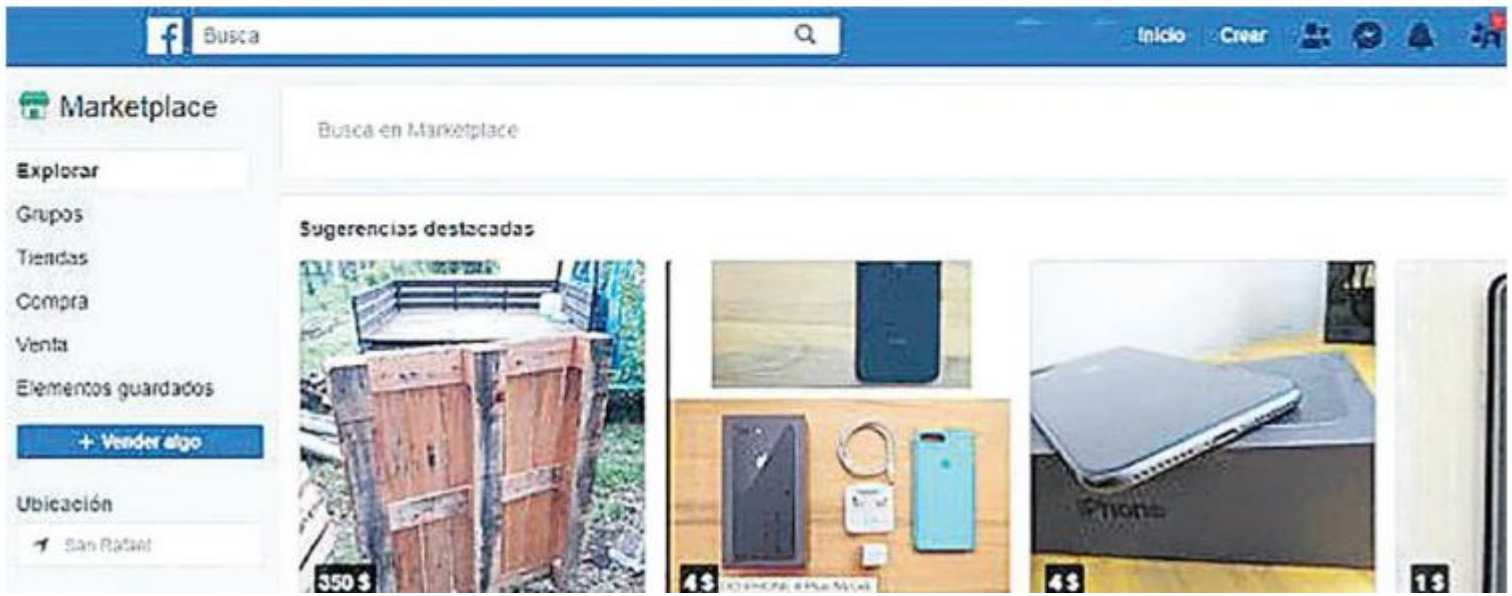
POPULAR

POLICIALES. 12 de septiembre de 2020

# Crecieron 350% las estafas de compras en internet

- Por Nicolás Fasolino

COMPARTIR: Guardar




https://www.diariopopular.com.ar/policiales/crecieron-350-las-estafas-compras-internet-n502143

ISACA Costa Rica Chapter

# 3 Fraude en Compras por Internet

## Método:

Utilizan sitios falsos de compras, venta de productos ficticios, comprobantes alterados de depósitos, promociones y publicidad de anuncios en redes sociales.

Mediante sitios falsos roban **información de tarjetas de crédito o débitos, falsifican comprobantes de depósitos, solicitan depósitos de garantía o pagos adelantados.**

## Consejos:

1. Digite **siempre la dirección del sitio** web oficial de compras en el navegador de internet.
2. Realice compras en sitios de **confianza y reconocidos**.
3. Nunca ingrese mediante **enlaces o buscadores de internet** a sitios web de compras.
4. **Desconfié** de promociones, ventas, premios y sorteos **irresistibles o de último minuto**.
5. Utilice **tarjetas virtuales** para realizar compras por internet.
6. Contrate **seguros** antifraude a sus tarjetas crédito y débito.
7. Valide y active **notificaciones** de compras de sus tarjetas.
8. Si es vendedor verifique los **depósitos y transacciones** antes de entregar su producto.
9. Ante sospechas en la compra o venta **valide la empresa y reputación del vendedor**.

ISACA Costa Rica Chapter

Empresa de seguridad informática Fortinet presentó su informe trimestral de incidencias

# Costa Rica registró casi 32 millones de intentos de ciberataques en primeros tres meses

Estafas mediante medios electrónicos superan los ¢500 millones durante estos meses, estima el OIJ

Johnny Castro johnnycastro.asesor@larepublica.net | Viernes 15 mayo, 2020

https://www.larepublica.net/noticia/costa-rica-registro-casi-32-millones-de-intentos-de-ciberataques-en-primeros-tres-meses

# 4 Fraude con Software Malicioso


## Método:

Utilizan **aplicaciones, virus o software malicioso** para intentar comprometer su computadora o dispositivo móvil.

Mediante programas maliciosos buscan **tomar control remoto y acceso a su información sensible de credenciales de acceso, información de tarjetas y hasta incluso secuestrar su información** (ransomware) para intentar realizar fraude digital.

## Consejos:

1. **Instale** las aplicaciones financieras siempre de las **tiendas oficiales** (Play Store, App Store o AppGallery).
2. **Mantenga** su computadora y dispositivo móvil con las **actualizaciones** más recientes.
3. Utilice una solución **antivirus** en su PC y dispositivo móvil, además manténgala **actualizada**.
4. Realice **respaldos** periódicos de su información y **valide** que funcionan.
5. No realice transacciones financieras en **redes públicas**.
6. Ante la sospecha de compromiso de su dispositivo **reinstálelo**.

ISACA Costa Rica Chapter

# Para Finalizar…

ISACA
Costa Rica Chapter

# (VIDEO)

https://youtu.be/NHlTtqmjy5k




Video Propiedad de ALFA Seguridad Información https://youtu.be/NHlTtqmjy5k

ISACA COMMUNITY DAY
PEOPLE | SERVICE | PURPOSE

3 de Octubre

# ¡MUCHAS GRACIAS!


LIC. FREDDY ROCA ABARCA

FREDDY.ROCA@HOTMAIL.COM

+506 8580-0032

FREDDY-M-ROCA-ABARCA


ISACA Costa Rica Chapter