



DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL
CENTRO CIBERNÉTICO POLICIAL



Capitán César Eduardo Galvis Pedroza
Jefe Centro Cibernético Policial



Dirección de Investigación
Criminal e INTERPOL de la
Policía Nacional - DIJIN



Misión

La Dirección de Investigación Criminal e INTERPOL de la Policía Nacional tiene como misión **contribuir a la seguridad y convivencia ciudadana**, mediante el desarrollo efectivo de la **investigación judicial, criminalística, criminológica y la administración de la información criminal**, así como la asistencia a la **organización internacional de Policía Criminal, autoridades nacionales e internacionales**, orientada a brindar apoyo oportuno a la **administración de justicia en la lucha contra la impunidad**.



CENTRO CIBERNÉTICO POLICIAL

Unidad especializada de la **Dirección de Investigación Criminal e INTERPOL**, encargada de enfrentar las conductas delictivas en materia de delitos informáticos, a partir de los enfoques preventivo, investigativo, análisis de evidencia digital y alianzas estratégicas.

CONCEPTUALIZACIÓN DEL CIBERDELITO

Cibercrimen

Actividades mediadas por computador que son ilegales o consideradas ilícitas por ciertas partes y que pueden ser conducidas por redes electrónicas globales

Thomas y Loader (2000)

Cualquier crimen que es facilitado o cometido usando un computador, red o dispositivo hardware.

Gordon y Ford (2006)

Comportamientos ilícitos que se dirigen a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación previa o posterior, y ejecución automática de datos o sistemas informáticos sin el consentimiento o con abuso del mismo.

La finalidad usual de estos comportamientos es lesionar o poner en peligro de manera ilícita la seguridad de las funciones informáticas, (confiabilidad/confidencialidad, integridad, la disponibilidad, el no repudio de los datos y los sistemas informáticos protegidos y la recuperación de información; sin perjuicio de que esto implique la lesión o la puesta en peligro de otros bienes jurídicos tutelados.

 *Ricardo Posada Maya*

Delitos Informáticos

Directamente lesionan o ponen en peligro bienes jurídicos como el patrimonio económico, la fe pública, la intimidad personal, la libertad y la formación sexual, el honor, los derechos morales y patrimoniales de autor.

La lesión o el peligro a la seguridad de la información es indirecto y solo tiene explicación a partir del uso del medio empleado; los datos y los sistemas informáticos.

 *Ricardo Posada Maya*

Categorización tipologías de los delitos

1 DICOTOMÍA

CIBERDEPENDIENTES O TIPO I

- Son de naturaleza más técnica agrupando aquellos delitos que atentan contra la persona o la propiedad.

CIBER HABILITADOS O TIPO II

- Son aquellos delitos tradicionales anteriores a la llegada de la tecnología y que ahora son llevados al ciberespacio. Ejemplo el acoso, tráfico de drogas, terrorismo. Implican más contacto humano.

2 TRICOTOMÍAS

CRÍMENES CONTRA LA MÁQUINA

- Son aquellos que atentan contra la integridad informática (ataques de DOS, DDOS, Craqueo, ransomware, borrado no autorizado de información, malware).

CRIMENES EN LA MÁQUINA

- Son aquellos crímenes que se cometen mediante el uso de contenidos multimedia (Pornografía infantil, acoso, distribución de contenidos de odio).

DELITOS CON LA MÁQUINA

- Delitos que para su comisión requieren ser asistidos por una computadora (Piratería, estafas, phishing, robo de identidad).

Gordon y Ford, Thomas y Loader

Tsakalidis, Vergidis y Madas

Paralelos investigativos



Cibernético.



Tradicional.

1

Identidad



Identidades virtuales (múltiples).
ID*



Deepfake/deepvoices (IA).



KYC.



Bots.



Identificación real

2

EMP, EF y ED



Transnacionalidad del internet



Información en el sector privado.



Descentralización (activos virtuales).



Infraestructuras BPH - BulletProof Hosting.



Volatilidad.



Disponibilidad (streaming).



Tiempos de almacenamiento



Lugar de los hechos
definido



Acceso a información de
manera local.



Infraestructuras
convencionales



Infraestructura criminal de
difícil acceso.



Evidencia traza.



Base de datos centralizada
en una empresa (servidor
controlado).

3

Entornos facilitadores



Relación costo-beneficio favorable.



Automatización de ataques.



Anonimato y enmascaramiento de
conexiones.



Falta de regulación (medidas
cautelares phishing – sim card, etc) .



Encriptación.



Darkweb



Crimen colaborativo.



Rápida propagación y escala global

CIBERATAQUES RELEVANTES

País: Estados Unidos

Actor del ataque: Dark Sade

Fecha del ataque: 10 de mayo de 2021

Descripción: consistió en un ciberataque a la **red de oleoducto Colonial Pipeline CO. de Estados Unidos**, en el cual **robaron casi 100 gigabytes de datos** amenazando con publicarlos en Internet si no se pagaba el rescate y se debieron modificar múltiples vuelos e incluso **suspensión temporal de aeropuertos por la escases de combustible**.

Fuente: <https://bit.ly/3lv89lp>



País: Estados Unidos

Actor del ataque: Cyber Av3ngers

Fecha del ataque: 29 de noviembre de 2023

Descripción: consistió en un ciberataque contra la Autoridad Municipal del Agua de Aliquippa en Pensilvania, **tomando el control de la estación de refuerzo que monitorea y regula la presión del fluido**, comprometiendo diversas etapas y procesos de tratamiento de aguas residuales, **evitando el acceso a agua limpia y potable**.

Fuente: <https://bit.ly/4a2Stfb>



País: Estados Unidos

Actor del ataque: Ransomware Sodinokibi

Fecha del ataque: 31 de diciembre de 2023

Descripción: consistió en un ciberataque a los sistemas de la empresa de intercambio de divisas Travelex mediante un malware que cifró toda la información, eliminó los archivos de backup y copió más de **5GB de información personal**, la compañía desconectó los sistemas para evitar la propagación del virus a través de la red y se vió obligada a **cerrar 1.500 de sus sucursales**.

Fuente: <http://bit.ly/48Tck7k>



País: Alemania

Actor del ataque: Anónimo.

Fecha del ataque: 18 de septiembre de 2020

Descripción: consistió en ataque informático que bloqueó los servidores del Hospital Universitario de Düsseldorf en Alemania, **provocando el fallecimiento de una mujer** que estaba siendo atendida en el lugar quien se encontraba en una situación crítica y debía ser operada de inmediato.

Fuente: <https://bit.ly/3wK1arv>



País: Ucrania

Actor del ataque: Hackers rusos

Fecha del ataque: 20 de abril de 2022

Descripción: consistió en un ataque que intentó destruir los ordenadores de una empresa de energía ucraniana, **el cual habría causado el mayor apagón inducido por un ciberataque de la historia**, agravando el conflicto generado entre Rusia y Ucrania.

Fuente: <https://bit.ly/3lu9jny>



País: Albania

Actor del ataque: Anónimo

Fecha del ataque: 15 de junio de 2022

Descripción: consistió en un ciberataque contra la infraestructura digital del Gobierno de Albania, que amenazó la ejecución de servicios públicos y las comunicaciones en los sistemas del Gobierno, **lo cual generó una alerta por un posible conflicto entre miembros de la OTAN contra el estado iraní**.

Fuente: <https://bit.ly/3wUHfae>



CONTEXTO DEL CIBERCRIMEN

El **phishing** se **sexuplicó** en América Latina con el reinicio de la actividad económica y el apoyo de la Inteligencia Artificial, en el que se ha identificado el incremento de ataques de malware en un **617%**.

(Kaspersky, 2023).

América Latina representa el **13%** de los ataques y es la quinta región del mundo con mayor afectación.

(Kaspersky, 2023).

América Latina registra **7,160 ataques diarios**, lo que supone un promedio de **cinco intentos** de infección por **minuto**.

(Kaspersky, 2023).

Para el año **2025** el **mercado de la ciberseguridad** crecería más del **51%** en Latinoamérica con respecto a 2019, alcanzando los **26 billones de dólares**.

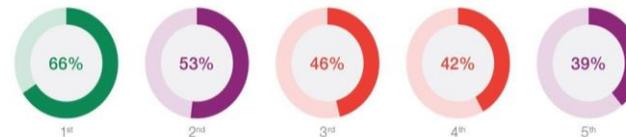
(Banco Internacional de Desarrollo (BID), 2022)

Global Risks Report 2024

Current risk landscape

WORLD
ECONOMIC
FORUM

"Please select up to five risks that you believe are most likely to present a material crisis on a global scale in 2024."



Extreme weather
AI-generated misinformation and disinformation
Societal and/or political polarization
Cost of living crisis
Cyberattacks

Risk categories | Economic | Environmental | Geopolitical | Societal | Technological

Source: World Economic Forum Global Risks Perception Survey 2023-2024.

El cibercrimen ocupa el **5to** puesto en el top de riesgos globales para el 2024.

(Foro Económico Mundial, 2024).

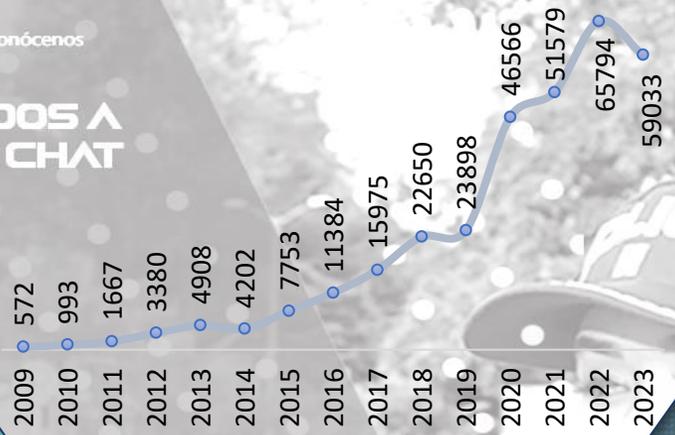
BIENVENIDOS A
NUESTRO CHAT

CONTEXTO NACIONAL

En el **2023**, se registraron **59.033** denuncias por delitos informáticos (*contemplados en la ley 1273 del 2009*), representando una reducción del **10%** con relación al año **2022** con **65.794** denuncias.

Para el año **2024**, se registra un incremento del delito con **17.721** denuncias representando el **1%** con relación con el mismo corte del año **2023** con **17.534** denuncias.

El hurto por medios informáticos, es el delito más frecuente en el país con **9.123** denuncias reportadas en lo transcurrido del **2024**, con una variación porcentual del **3%** frente al mismo periodo del **2023**.



Histórico denuncias por año (Ley 1273/2009)



INCIDENTES CAI VIRTUAL 3.568

- Phishing **562**
- Robo de cuentas de redes sociales **343**
- Estafa por compra y venta en internet **241**
- Falsedad en entornos digitales **226**
- Gota a gota virtual **218**

CONTEXTO NACIONAL

Denuncias 9 Delitos informáticos

	2023	2024	
Hurto por medios informáticos y semejantes	9.300	11.025	18%
Acceso abusivo a un sistema informático	3.673	3.849	5%
Violación de datos personales	3.634	2.877	-21%
Suplantación de sitios web	1.522	1.798	18%
Transferencia no consentida de activos	1.173	1.208	3%
Intercepción de datos informáticos	527	357	-32%
Daño informático	164	115	-30%
Obstaculización ilegítima de sistema informático o red de telecomunicación	132	83	-37%
Uso de software malicioso	126	74	-41%
TOTAL	20.251	21.386	Incremento 6%

Datos extraídos el día 03 de mayo 2024. Cifras sujetas a variación, en proceso de integración y consolidación con información de Fiscalía General de la Nación.

6 Ciudades de mayor afectación

	Denuncias	% Fenómeno
• Bogotá	7.003	33%
• Medellín	1.617	7.5%
• Cali	1.202	5.6%
• Barranquilla	738	3.4%
• Cartagena	463	2.1%
• Ibagué	388	1.81%

53%

FENÓMENO

Corte del 01 de enero al 03 de mayo 2023, vs 01 de enero al 03 de mayo 2024.

MARCO NORMATIVO Y EVOLUCIÓN

EVOLUCIÓN DEL CECIP

POLÍTICAS PÚBLICAS

NORMATIVIDAD NACIONAL

NORMATIVIDAD INTERNACIONAL



GRIDI
Grupo Investigativo Delitos Informáticos
Res no. 02762/2001

GITEC
Grupo Investigaciones Tecnológicas
Res No. 02057 2007
Creación CAI Virtual

CSIRT PONAL
Res No. 00319 2010

ARCIP
Área Centro Cibernético Policial.

CECIP
Centro Cibernético Policial
Res No. 05839 2015

Oficial Enlace en Ciberdelitos de **EUROPOL**

Resolución 0260 del 25 de enero
Por la cual se define la estructura orgánica interna de la DIJIN y el Centro Cibernético Policial.

CONPES 3701 del 14 de julio
Se establecen los Lineamientos de política para la Ciberseguridad y Ciberdefensa en Colombia.

CONPES 3854 del 11 de abril
Política Nacional de Seguridad Digital de Colombia"

CONPES 3995 del 01 de julio
Política Nacional de Confianza y Seguridad Digital.

PND 2022 – 2026 Colombia Potencia Mundial de la Vida

Estrategia Nacional Digital de Colombia 2023 - 2026

LEY 527 DE 1999
Uso de los mensajes de datos, del comercio electrónico y de las firmas digitales...

LEY 1273 del 05 de enero "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"

Decreto 1078 del 26 de mayo
Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

LEY 1928 del 24 de julio
Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

Resolución 500 del 08 de abril
Lineamientos y estándares para la estrategia de seguridad digital.

Decreto 338 del 08 de marzo
Establece lineamientos generales para la gobernanza digital (se incorpora en el marco jurídico a los PMU-Ciber).

Directiva Presidencial 02 del 24 de febrero
Política pública en materia de seguridad digital.

Convenio de Budapest
Primer tratado internacional que busca hacer frente a los delitos informáticos.

El 1 de marzo entró en vigor el Protocolo Adicional a la Convención sobre el delito cibernético.

Consejo de Europa invitó a nuestro país a formar parte del Convenio de Budapest.

El 12 de mayo Colombia suscribe el II Protocolo Add. al Convenio de Budapest sobre la ciberdelincuencia

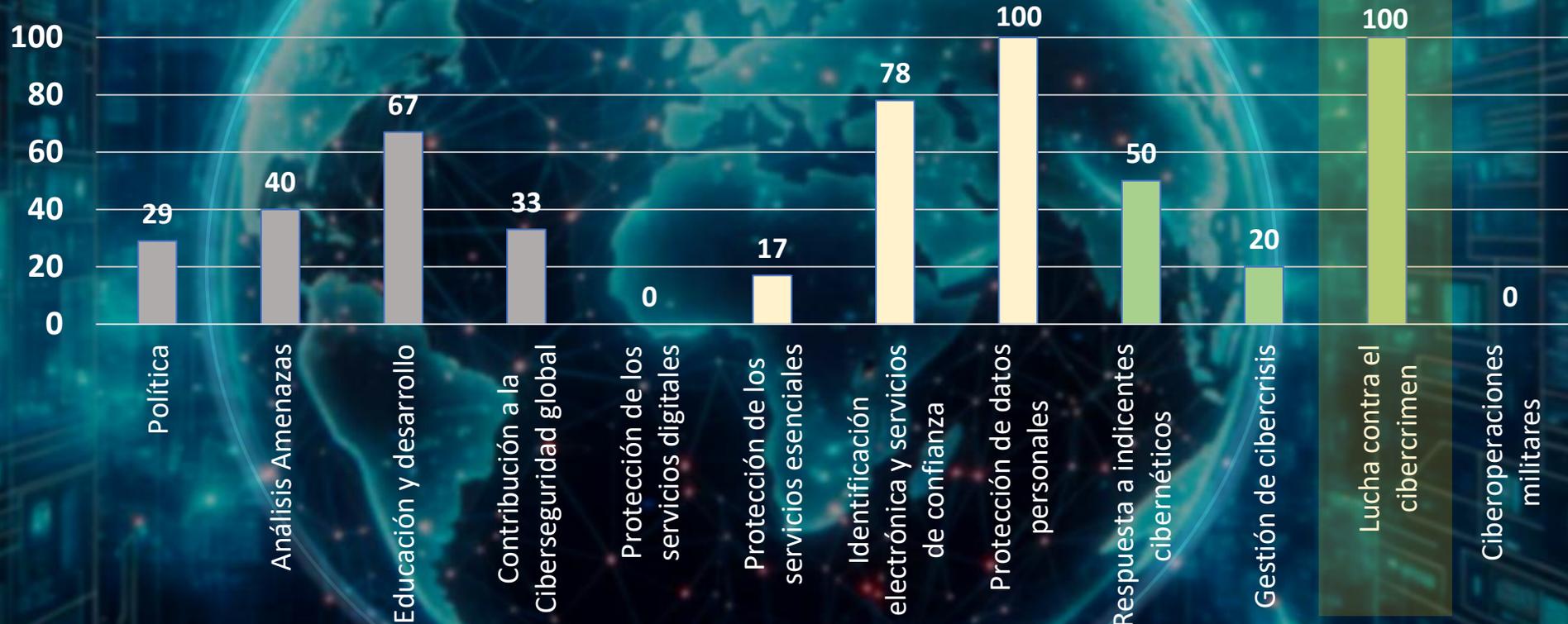


Promedio

Puesto 69

176
países
evaluados

Ítems evaluados



Indicadores generales de ciberseguridad (Estratégicos)

Indicadores básicos de ciberseguridad (Preventivos)

Indicadores de gestión de incidentes y crisis (Operacionales)



CAPACIDADES CENTRO CIBERNÉTICO POLICIAL

GESTIÓN COMUNITARIA

Participación cívica

(información, sensibilización e intervención)

- Balance de Cibercriminalidad
- Boletines y videos informativos
- Campañas de prevención
- Gestión de bloqueo de páginas*
- OSINT
- Análisis de Criptoactivos
- Análisis de Vulnerabilidades



70k

Chainalysis
VERACODE

CAI VIRTUAL 24/7

Servicio pionero en Iberoamérica en la atención de incidentes cibernéticos

Servicio 24/7
Atención al ciudadano



Canales de atención



C4



COOPERACIÓN INTERNACIONAL

Comunicación 24/7



INTERPOL



AMERIPOL



G7



EUROPOL



CONSEIL DE L'EUROPE

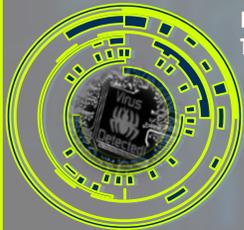
Convenio de BUDAPEST

Organizaciones, organismos y mecanismos internacionales

PERSECUSIÓN PENAL

Dirección Nacional Especializada contra los Delitos Informáticos.

Delitos de Alta Tecnología
Ley 1273/09



Fraudes Informáticos
Ley 1273/09



Afectación a Niños, Niñas y Adolescentes en entornos digitales

Art. 218 y 219° CP

ANÁLISIS DE EVIDENCIA DIGITAL

09 LABORATORIOS INFORMÁTICA FORENSE



CSIRT-POWAL



ESCIB

RELACIONAMIENTO

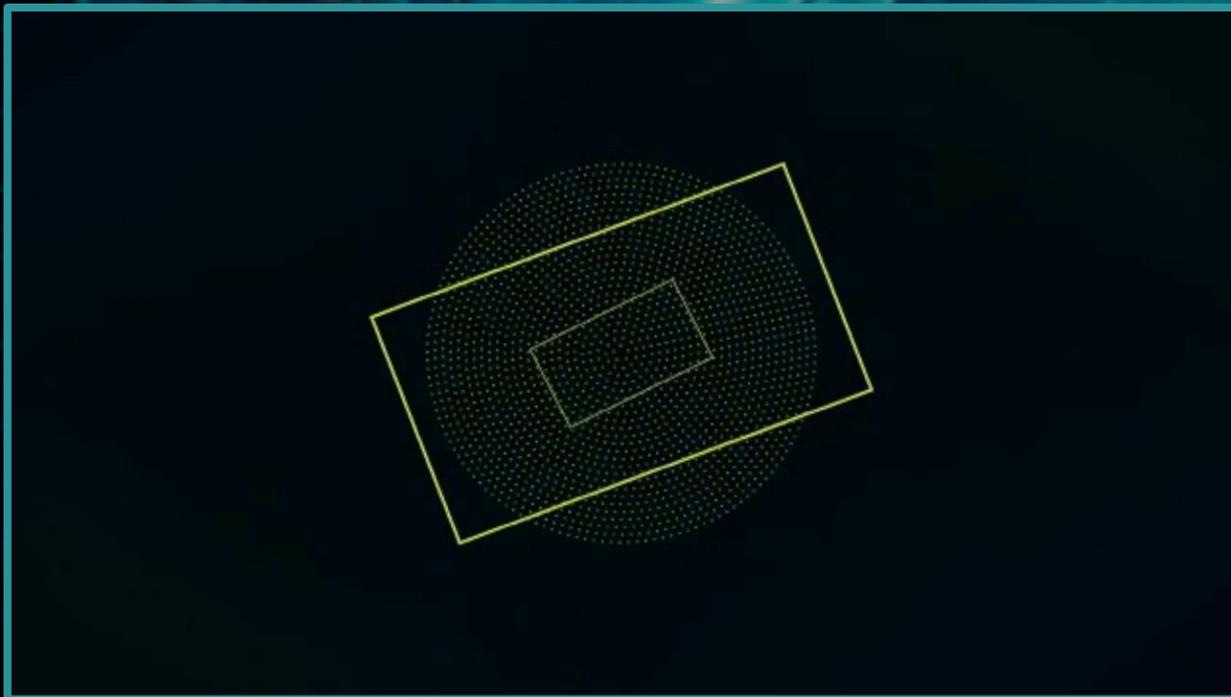
Coordinación nacional



PMU ELECTORAL

SERVICIO CAI VIRTUAL 24/7

Plataforma dispuesta por la Policía Nacional para la prevención, orientación y atención de incidentes informáticos de la ley 1273 del 2009



Afectación por modalidad



Durante el año 2024 se han atendido **140 incidentes informáticos** relacionados a los sectores **E-Commerce** e **industrial**, por estas modalidades

SECTOR

HIDROCARBUROS

FINANCIERO

ASEGURADOR

AERONÁUTICA

AUTOMOTRIZ

PHISHING

Modalidad utilizada por ciberdelincuentes para captar de manera irregular datos personales como credenciales de inicio de sesión, números de tarjetas de crédito a través de ingeniería social, esta modalidad es generada por correos electrónicos, mensajes de texto, sitios web falsos o llamadas fraudulentas.

¡ASPECTOS PARA IDENTIFICAR POSIBLES SITIOS FALSOS!

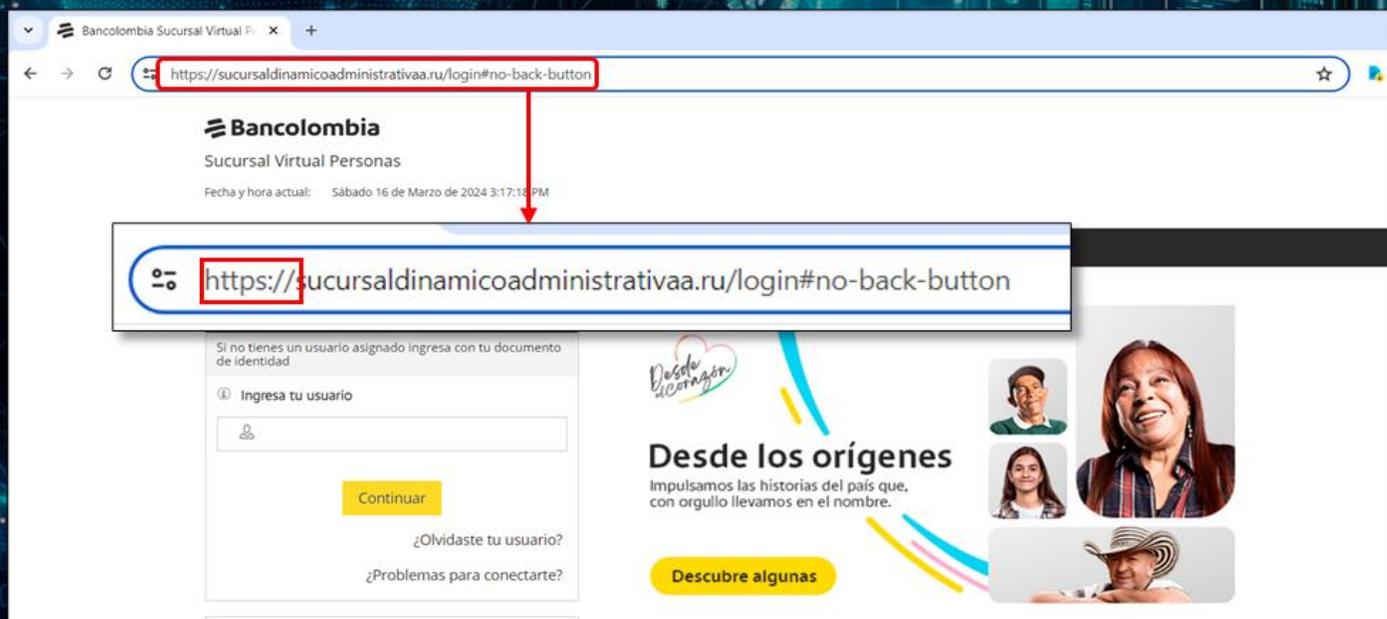
Los correos electrónicos hacen una oferta que parece demasiado buena para ser verdad. Podría decir que ha ganado la lotería, un premio caro o alguna otra cosa de alto valor.

Tenga cuidado si el correo electrónico tiene un lenguaje alarmista para crear un sentido de urgencia, instándole a que haga clic y “actúe ahora” antes de se elimine su cuenta. Recuerde, las organizaciones responsables no solicitan detalles personales a través de Internet.

El mensaje contiene archivos adjuntos inesperados o extraños. Estos adjuntos pueden contener malware, ransomware o alguna otra amenaza online.

Las páginas web hacia donde lo dirigen para que ingrese sus datos personales, no coinciden con la página autentica de la entidad.

MODALIDADES MÁS REPORTADAS



EMAIL SPOOFING

Usted tiene un proceso pendiente y no se le permitira la salida del pais .

MC

Migración Colombia

notijudicial@migracioncolombia.gov.co

viernes, 21 de octubre 19:10

Prioridad alta

Dominio suplantado de entidad del estado, Fraudulento que roba información.

PROCESOID2036521045875.pdf
PDF - 72 KB

.pdf Malicioso que al abrirlo contiene un scrip que desencadena líneas de código que terminara infectando el equipo.

MIGRACIÓN
MINISTERIO DE RELACIONES EXTERIORES

acion Colombia <notificaciones@migracioncolombia.gov.co>
: jueves, 26 de abril de 2018 3:17:36 p.m.
(Documento corregido) Usted tiene un Proceso pendiente y no se le permitira la salida del pais

MIGRACIÓN
MINISTERIO DE RELACIONES EXTERIORES

Saludo cordial

ficamos hoy 26 de abril que Usted tiene un proceso pendiente y hasta no recibir notificacion de la caducidad de este proceso no se le permi
pais como lo estipula el artículo 12 de la ley migratoria

Para mayor informacion hemos adjuntado dicho proceso

Este documento adjunto contiene una clave es : proceso

¿CÓMO IDENTIFICAR UN CORREO SPOOFING?

- Verificar la autenticidad de la dirección de correo remitente (para este caso, la dirección oficial de Migración Colombia corresponde a noti.judiciales@migracioncolombia.gov.co).
- Como se trata de email spoofing, revise en detalles del mensaje el **RECEIVED SPF**, debiendo visualizarse como "Pass".
- Suelen ser mensajes cuyo contenido busca generar **urgencia**, para obligar al destinatario a instalar software en su dispositivo.
- Por lo general, anexan archivos con contraseña, los cuales suelen ser **.pdf** o **.exe** (ejecutables).
- Generalmente omiten relacionar datos del destinatario del mensaje, al tratarse de correos masivos.
- En algunos casos, los delincuentes "reciclan" las campañas (utilizadas en el año **2018** y nuevamente en **2022**).
- Contienen faltas ortográficas en la redacción de los mensajes.
- Uso de logos o emblemas desactualizados.
- Advierten sanciones en caso de no seguir las instrucciones generadas (multas, embargos, restricciones, entre otros).

ANÁLISIS DEL PHISHING

SITIO WEB REAL

Enlace compartido por el sitio oficial de Nequi.

<https://transacciones.nequi.com/bdigital/login.jsp>

TIPO DE LETRA

Letra utilizada en sus plataformas, con la misma intensidad de color.

CAPTCHA

Información compartida por el CAPTCHA completa, sin faltar datos.

PORTAL WEB FALSO

Identifique que el enlace si corresponda al de la entidad.

FALLAS DE EDICIÓN

Identifique que el enlace si corresponda al de la entidad.

CAMBIO DE PALABRAS

Identifique que el enlace si corresponda al de la entidad.

transacciones.nequi.com

Nequi

Entra a tu Nequi

Podrás bloquear tu Nequi, consultar tus datos.

+57 Número de celular

Contraseña

No soy un robot

Este sitio supera la cuota de reCAPTCHA.

reCAPTCHA Privacidad - Términos

Entra

nequi.pro

Nequi

Entra a tu Nequi

Podrás bloquear tu nequi, consultar tus datos

+57 Número de celular

Contraseña

No soy un robot

reCAPTCHA Privacidad - Términos

Enviar

Nequi

Grupo Bancolombia

ANÁLISIS DEL PHISHING

Screenshot of a phishing website. The browser address bar shows the URL: `servicioseguroenlineabb.com/Ecuad3/Colpatriaa/`. The page features the Scotiabank and COLPATRIA logos, a red alarm bell icon, and the heading "Ingresa a tu Banca Virtual". The login form includes fields for "Nombre de usuario" and "Contraseña", a "¿Necesitas ayuda para ingresar?" link, a "Recordar mi nombre de usuario" checkbox, and a red "Ingresar" button. A "¿No te has registrado?" link is followed by a "Regístrate aquí" button. A blue "REGRESAR" button is in the bottom left corner.

PORTAL WEB FALSO

- Enlace difundido a través de correo electrónico.
- Se evidencia repetición de caracteres dentro del enlace.

© 2024 Todos los Derechos Reservados Scotiabank Colpatría.

Screenshot of the real Scotiabank website. The browser address bar shows the URL: `banco.scotiabankcolpatria.com/banca-virtual/login/`. The page features the Scotiabank and COLPATRIA logos and the heading "Ingresa a tu Banca Virtual". The login form includes fields for "Nombre de usuario" and "Contraseña", a "¿Necesitas ayuda para ingresar?" link, a "Recordar mi nombre de usuario" checkbox, and a red "Ingresar" button. A "¿No te has registrado?" link is followed by a "Regístrate aquí" button.

SITIO WEB REAL

Enlace compartido por el sitio oficial de Scotiabankcolpatría, en su sección: **Ingresar > Banca Virtual Personas**

ANÁLISIS DEL PHISHING

SITIO WEB FALSO

Enlace difundido a través de SMS, donde se informa de un crediagil de libre inversión preaprobado.

Bancolombia
Sucursal Virtual Personas
Fecha y hora actual: Sábado 16 de Marzo de 2024 3:17:18 PM

<https://sucursaldinamicoadministrativaa.ru/login#no-back-button>

Si no tienes un usuario asignado ingresa con tu documento de identidad

Ingresa tu usuario

Continuar

¿Olvidaste tu usuario?
¿Problemas para conectarte?

Desde los orígenes
Impulsamos las historias del país que, con orgullo llevamos en el nombre.

Descubre algunas

¿No conoces la Sucursal Virtual Personas de Bancolombia? Conoce más aquí

- Conoce sobre Sucursal Virtual Personas
- Aprende sobre Seguridad
- Reglamento Sucursal Virtual
- Política de Privacidad

SITIO WEB FALSO

Enlace difundido a través de SMS, donde se informa la activación de un seguro mensual.

Bancolombia
Sucursal Virtual Personas
Fecha y hora actual: Sábado 16 de Marzo de 2024 3:50:34 PM

<http://transaccionalsucvirtual.ru/login#no-back-button>

Si no tienes un usuario asignado ingresa con tu documento de identidad

Ingresa tu usuario

Continuar

¿Olvidaste tu usuario?
¿Problemas para conectarte?

Desde los orígenes
Impulsamos las historias del país que, con orgullo llevamos en el nombre.

Descubre algunas

¿No conoces la Sucursal Virtual Personas de Bancolombia? Conoce más aquí

- Conoce sobre Sucursal Virtual Personas
- Aprende sobre Seguridad
- Reglamento Sucursal Virtual
- Política de Privacidad

← REGRESAR

BUSINESS EMAIL COMPROMISE BEC



● Crea dominios de correos electrónicos, para suplantar entidades públicas y privadas.

● Remite pliegos de contratación, cuentas de cobro, solicitud de transferencias a empresas proveedores de tecnología.

● Genera procesos falsos de contratación con el fin de concretar el envío de elementos tecnológicos o pagos de recursos.

● Intenta robar dinero o datos confidenciales de una empresa.

● **Incorporar sistemas de detección de intrusos (IDS), para identificar y señalar correos electrónicos con extensiones muy similares a la del correo oficial de la compañía, indicando, de esa manera, posibles intentos de acceso.**

Empleado entregó 26 millones de dólares a ladrones que imitaron a su jefe con IA



La doctora Carol Brown y su hermano Kenneth Preston, fueron asesinados mientras Brown se encontraba en una video llamada por Zoom con un colega del trabajo. FOTO: Stock

Empleados de la compañía recibieron un mensaje por medio del 'phishing' y fueron estafados.

Dentro de esta modalidad, suplantan a gerentes y/o proveedores, mediante correos electrónicos, y mensajería instantánea, con el fin de provocar transacciones o desviar entregas de productos.

DISTRIBUCIÓN DE SOFTWARE MALICIOSO

MODALIDADES MÁS REPORTADAS



Operación
CASA
BLANCA.

Fase II
2024

02 capturas, 374 equipos víctimas identificados, 01 allanamiento y 1.499 muestras de malware tipo RAT identificadas.

1

Identificación de una base de datos con 420.135 correos electrónicos de los cuales 2.717 son gubernamentales.

2

Análisis de más de 1 millón de capturas de pantallas de víctimas.

3

Mantenga sus sistemas, software y aplicaciones actualizadas.

Evite abrir archivos adjuntos o dar clic sobre links en correos de procedencia desconocida.

Realice copias de seguridad (Backup) de su información de manera periódica.

Verifique directamente en las páginas oficiales cualquier supuesto reporte.

Copie el link y verifique que no este oculto (ofuscado).

Evite dar clic en correos que generen zozobra como **fotomultas, reporte datacrédito o citación judicial**; repórtelos a nuestro @caivirtual para determinar su veracidad.

ATAQUES NACIONALES



“El 06 de febrero de 2022, el INVIMA fue objeto de un **ransomware** que impactó la **disponibilidad** de la información en al menos un **80%** de los datos que reposa en sus servidores.”

- variable **BLACKBITE**.
- Afectación a **40 servidores físicos y 200 virtuales**.



“El 28 de noviembre de 2022, recibe un ataque de **ransomware** a su infraestructura tecnológica, se evidenció la afectación de **30 máquinas virtuales** que incluían aproximadamente **500 servidores**.”

- Impactó los servicios de facturación, sistemas de gestión automatizada (**chatbot**), portales **Web** y de servicio al cliente
- Se identificaron canales de **Telegram** que comparten sitios de **Dark Web**, con **13 archivos correspondientes de tipo (.xlsx, docs, csv)**.



“El 12 de septiembre de 2023, **IFX Networks**, un proveedor de servicios en la nube, sufrió un ataque tipo **Ransomware** que afectó al menos a **50 entidades estatales** colombianas, incluyendo al **Ministerio de Salud y Protección Social** y al **Consejo Superior de la Judicatura**.”

- Afectación de **762 compañías en Latinoamérica**.
- Los responsables de este ciberataque serían el colectivo **Ransomhouse**.



“El 13 de diciembre de 2022 voceros de **EPM**, informan a la opinión pública que están siendo víctimas de un ataque de ransomware de la variante **BlackCat**, el cual comprometió la **disponibilidad de sus servicios**.”

- Tuvo una afectación del **Data Center** alterno y generó una **afectación del 25%** de la **infraestructura**.
- **Pérdida de información de aproximadamente 3,7 terabytes**.



RANSOMWARE

Declaración conjunta de la Iniciativa Internacional Contra el Ransomware 2023

Los ataques de Ransomware aumentaron en un 122% en comparación a 2021 y las denuncias crecieron 26%.
(Cámara Colombiana de Informática y Telecomunicaciones)

42 mil millones USD

Colombia y Brasil

Países de Latam que aparecen en el listado de los 10 países del mundo con más ataques de ransomware en el 2022.
(Prensarioiila.com)

85%

De las empresas colombianas con trabajo remoto son vulnerables a ataques de ransomware. (Infobae.com)

De las PYMES, no pueden sostener sus negocios más de 6 meses, luego de sufrir un ciberataque importante.
(Cámara Colombiana de Informática y Telecomunicaciones)

60%

80.000 exploits

Detectados en Colombia, que se utilizan para ingresar a los sistemas de información y materializar amenazas como el ransomware. (FortiGuard)

Intentos de ataques de ransomware en Colombia.
(Kaspersky)

80.000 intentos de ataques



Miembros de la CRI, en su tercera reunión, refuerzan compromisos contra el ransomware. Se centran en el desarrollo de capacidades, intercambio de información y medidas políticas para desalentar pagos. La International Counter Ransomware Task Force - ICRTF se expande para colaborar con la industria y abordar las amenazas de ransomware a nivel internacional.

- Se realiza reunión de la Iniciativa Internacional Contra el Ransomware (CRI) con 50 países miembros, inclusive Colombia.
- Identificación del error humano como causa principal en violaciones recientes de datos en la nube según IBM.
- Compromisos renovados en la tercera convocatoria del CRI para fortalecer la resiliencia ante el ransomware.
- Desarrollo de capacidades para interrumpir ataques y mejorar la ciberseguridad.
- Enfoque en compartir información a través de nuevas plataformas y tecnologías.
- Compromisos políticos para desalentar el pago de rescates y crear una lista negra compartida de billeteras ilícitas.
- Continua expansión de la ICRTF para colaborar con la industria y abordar las amenazas de ransomware.

ROBO DE CUENTAS DE WHATSAPP



MODALIDADES MÁS REPORTADAS

CUENTA OFICIAL

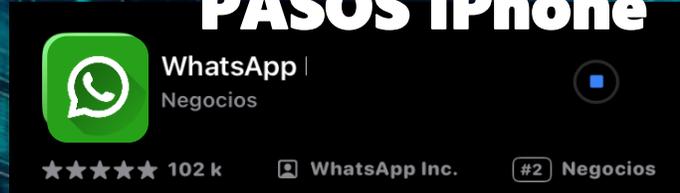
Esta cuenta es oficial y cuenta con la verificación **verde**, que certifica que es un espacio de comunicación directa desde **Meta**.

CHAT OFICIAL

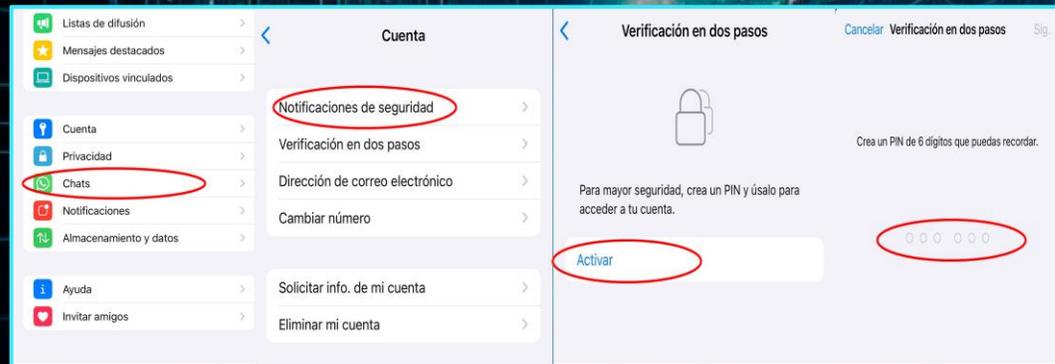
Brinda recomendaciones y nuevas novedades de la aplicación. Nunca solicita **códigos de verificación**.

La única forma de interacción es leyendo el contenido publicado, viendo las imágenes o videos e ingresando a los links compartidos, ya que **no es posible responder**, comentar, reaccionar o reenviar esa información.

CÓMO REALIZAR LA AUTENTICACIÓN EN DOS PASOS iPhone



En ajustes, ingrese a cuenta, verificación en dos pasos, presione activar e ingrese un PIN de seis dígitos.



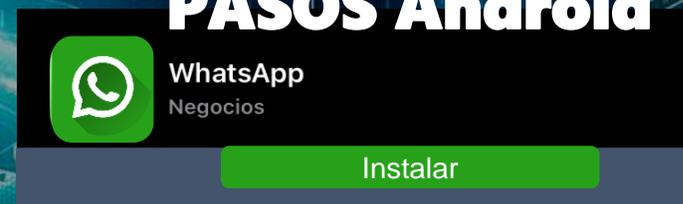
Después de esto, si desea, proporcione una dirección de correo electrónico o elija omitir.



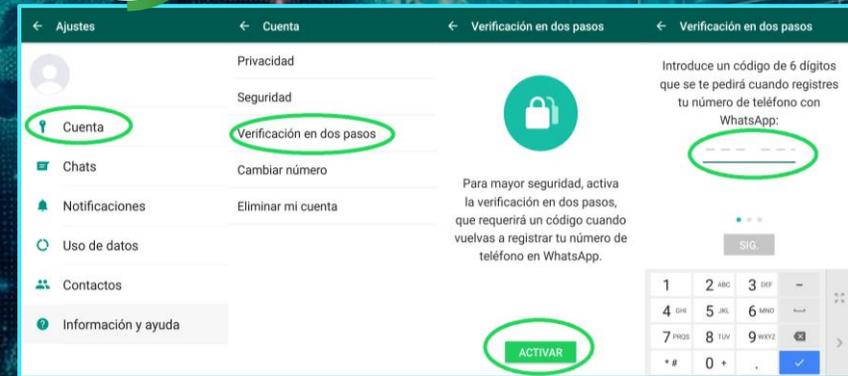
Confirme la dirección de correo electrónico (si la registró), posteriormente, guardar los cambios.

“Si no añade una dirección de correo electrónico y olvida su PIN, deberá esperar 7 días para restablecerlo”.

CÓMO REALIZAR LA AUTENTICACIÓN EN DOS PASOS Android



En ajustes, ingrese a cuenta, verificación en dos pasos, presione activar e ingrese un PIN de seis dígitos.



Después de esto, si desea, proporcione una dirección de correo electrónico o elija omitir.



Confirme la dirección de correo electrónico (si la registró), posteriormente, guardar los cambios.

“Si no añade una dirección de correo electrónico y olvida su PIN, deberá esperar 7 días para restablecerlo”.



GOTA A GOTA VIRTUAL

Modalidad utilizada por ciberdelincuentes, para ofrecer créditos de fácil acceso mediante la descarga de aplicaciones móviles, los cuales solicitan permisos de acceso a diferentes funciones del dispositivo móvil con el fin de capturar información personal.

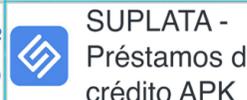
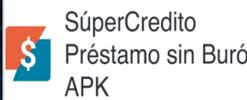
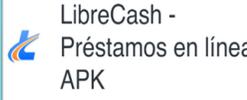
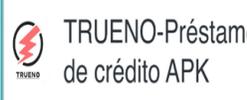
FACTORES DE ENGAÑO

- Se promociona el servicio por motores de búsqueda y redes sociales reconocidas.
- Se accede al servicio por aplicación.
- Eslogan: "préstamos rápidos" o "créditos fáciles prestan dinero rápido, sin requisitos, sin codeudores, sin revisar la puntuación en Data Crédito.
- Estudio del caso dura pocos minutos.
- Prometen bajas tasas de interés.

Los victimarios crean contenidos gráficos falsos, con la intención de chantajear e intimidar a las víctimas para que estas accedan con el pago.

MODALIDADES MÁS REPORTADAS

APLICACIONES IDENTIFICADAS

 Solventa	 Wadana.	 MONET CRÉDITO PARA TODOS
 credy	 Fast Rupee लोन?	 SUPLATA - Préstamos de crédito APK
 CREDIFIJO	 CrediBus Préstamos de crédito APK	 PezCrédito: Préstamos de dinero APK
 SúperCredito Préstamo sin Buró APK	 PopCash - préstamos en línea "Aplicación Gratis"	 PROFIN- Préstamos de Crédito APK
 RápiPréstamo- Préstamos crédito APK	 LibreCash - Préstamos en línea APK	 CopMás- Préstamo de crédito APK
 RapiCredit CRÉDITO CUANDO LO NECESITAS	 Loco Cash- Préstamos de Crédito APK	 RicoPréstamo- Préstamos crédito APK
 Descargar Vida Luja - Crédito Préstamos APK	 TRUENO-Préstamo de crédito APK	 Parcecash
 PlataHoy- Préstamos de crédito APK	 Perfecto Crédito - Préstamos APK	 Dezzum - Banca móvil personal

PERMISOS SOLICITADOS

<p>• Número de teléfono</p> <p>También obtendremos su número de teléfono para ayudar a identificar su identidad para garantizar la seguridad de la cuenta y los fondos. Una vez que se encuentra una excepción, congelaremos su cuenta a tiempo y le enviaremos una notificación a tiempo. La información del número de teléfono móvil será cifrada y cargada en nuestro servidor, la dirección del servidor es https://dez.dezzumtr.com/ que solo se utiliza para servicios antifraude y evaluación crediticia. No venderemos, intercambiamos ni alquilaremos la información de su número de teléfono móvil a ningún tercero.</p>	<p>• Álbum</p> <p>Esto se usa para acceder a su Álbum y cargar documentos KYC o imágenes necesarias en el proceso de préstamo.</p>
<p>• Cámara</p> <p>Necesitamos permiso para acceder a su cámara para que pueda escanear o tomar fotografías fácilmente de los documentos requeridos para la solicitud del préstamo. Estos documentos ayudan a probar su identidad real, que es uno de los pasos importantes de KYC.</p>	<p>• Almacenaje</p> <p>Necesitamos permiso para Almacenaje para poder guardar su información en su celular.</p>
<p>• SMS financieros</p> <p>Recopilamos, almacenamos y monitoreamos todos sus mensajes SMS, lo que también incluye sus datos históricos de SMS. Los datos recopilados se utilizan para identificar transacciones relacionadas con bancos, nombres de contrapartes, descripciones de transacciones y montos de transacciones utilizados para evaluar el riesgo crediticio; también verifique si tiene mal crédito o situaciones de morosidad para evitar fraudes. Estos datos se utilizan para proporcionar los mejores préstamos y mantenga el proceso de préstamo conveniente y sin problemas. Además, utilizaremos la API de seguridad para enviar esta información de manera intermitente a nuestro servidor (incluida la primera autorización, ingrese a la página de inicio, ingrese a la recopilación de información de la página, los datos se enviarán inmediatamente a nuestro servidor, dirección del servidor: https://dez.dezzumtr.com/). No la compartimos con otros terceros. También puede deshabilitar este acceso, pero si lo hace, no podrá usar la aplicación.</p>	<p>• Lista de contactos</p> <p>Recopilaremos, almacenaremos y monitorearemos la información de sus contactos, incluido el nombre, número de teléfono, tipo de cuenta, contactos, marcadores y modificaremos los datos opcionales, estos datos estarán en su autorización, por primera vez contacto para cargar, ingrese a la página de inicio, a través de la API de seguridad, la información del libro de direcciones se enviará de manera intermitente a nuestro servidor (la dirección del servidor es https://dez.dezzumtr.com/). La información de la libreta de direcciones se recopila para usarla para enriquecer su situación financiera, comprender mejor su reputación y ayudarnos a detectar solicitudes de préstamos fraudulentos y reducir el riesgo crediticio. Y nuestra aplicación necesita este permiso para brindar una mejor experiencia de usuario para ciertas funciones en la aplicación (como cargas de contactos).</p>
<p>• Información de dispositivo</p> <p>Necesitamos información específica sobre su dispositivo, incluido el modelo de hardware, versión del sistema, RAM, almacenamiento, identificadores únicos de dispositivo (como IMEI, número de serie, SSNID), información de SIM, incluido el operador de red, estado de roaming, código MNC y MCC, información WiFi incluyendo la dirección MAC. Esta información nos ayudará a identificar el dispositivo y garantizar que ningún dispositivo no autorizado actúe en su nombre y evitar fraudes.</p>	<p>• Apps Instaladas</p> <p>Necesitamos recopilar información de Apps instaladas en su celular, incluido el nombre de la App, el nombre del paquete de la App, fecha de instalación, versión, fecha de actualización, etc. Esta información será una parte integral de su evaluación crediticia y nos ayudará a valorar su solvencia.</p>
<p>• Información personal</p> <p>Necesitamos recopilar sus datos e información personal. Estos datos incluyen, nombre, género, fecha de nacimiento, edad, dirección, correo electrónico, Cédula de Ciudadanía, información laboral, entre otra, información básica necesaria para solicitar el Préstamo, y necesaria también para el proceso KYC.</p>	<p>• Recopilación de información de ubicación</p> <p>Recopilamos y rastreamos información sobre la ubicación de su equipo para garantizar que su solicitud de préstamo esté disponible, reducir los riesgos asociados con su solicitud de préstamo y proporcionar ofertas de préstamo personalizadas presprobadas. También nos ayuda a verificar direcciones, tomar mejores decisiones de riesgo crediticio y completar el proceso de conocimiento de su cliente (KYC).</p>

FISCALÍA

RECOMPENSA

MARIA CAMILA MORALES PINEDA

a quien o quienes proporcionen información veraz y útil, que coadyuve eficaz, eficiente, efectiva y oportunamente para la localización, detención o aprehensión de

ESTAFA A FINANCIERAS

TU DENUNCIA ES CONFIDENCIAL

AYÚDENOS A IDENTIFICARLOS

SE BUSCA INVESTIGADA POR FRAUDE Y EVASIÓN DE PAGO EN MORA INFORME A LAS AUTORIDADES SOBRE SU PRESENCIA YA QUE ES UN DELINCUENTE EN PROCESO DE INVESTIGACIÓN POR ROBO VIRTUAL

LINEA DIRECTA- 3209994892

ABSOLUTA RESERVA

SU DISPOSITIVO HASTA QUE EL PAGO SE VEA REFLEJADO

SI NO RECIBO RESPUESTA POSITIVA ME VEO EN LA OBLIGACIÓN DE SEGUIR EL CONDUCTO REGULAR Y LLAMAR A SUS CONTACTOS A QUE ME DEN RESPUESTA POR USTED Y EL DINERO YA QUE AL ACEPTAR TÉRMINOS Y CONDICIONES NOS DIÓ ACCESO A SU LIBRETA DE CONTACTOS. EN CINCO MINUTOS PROCEDEREMOS A BLOQUEAR SU DISPOSITIVO HASTA QUE EL PAGO SE VEA REFLEJADO

SI NO RECIBO RESPUESTA POSITIVA ME VEO EN LA OBLIGACIÓN DE SEGUIR EL CONDUCTO REGULAR Y LLAMAR A SUS CONTACTOS A QUE

ESTAFAS POR COMPRA Y VENTA DE PRODUCTOS Y SERVICIOS POR INTERNET

Corresponde a la publicación de una serie de servicios atractivos hacia un consumidor puntual a muy bajo costo, solicitan pagos por adelantado, una vez se realiza la consignación, las cuentas son cerradas o bloqueadas generando así la estafa (las cuentas en redes sociales utilizadas para estas actividades usualmente son falsas).

MODALIDADES MÁS REPORTADAS

MÉTODOS MÁS UTILIZADOS

- **VENDEROR HURTADO:** El delincuente contrata un producto o servicio contra entrega, una vez llega al sitio acordado es ultimado con armas de fuego hurtándoles sus productos.
- **COMPRADOR ESTAFADO:** el ciberdelincuente crea un sitio Web o una cuenta en redes sociales, un ciudadano lo contacta para adquirir el producto, una vez se realiza el envío del dinero, nunca recibe el artículo.
 - El ciudadano compra un producto y realiza el pago, cuando lo recibe, se percató que no fue lo que pidió o es simplemente una caja vacía.
- **VENDEDOR ESTAFADO:** determinado usuario publica un producto en una cuenta de compra-venta de artículos en redes sociales o sitio web, el ciberdelincuente lo contacta y adquiere el producto, pero nunca recibe el dinero acordado o desaparece.

Hola Buenas Noches,
Mi nuevo numero por favor guardarlo gracias.

12:28 AM

Hola 10:16 AM ✓

¿Y eso qué pasó con el otro ?
10:16 AM ✓

Lo 10:17 AM

Ah bueno, ya voy a guardar este entonces
10:19 AM ✓

Si y borra los otros 10:19 AM

También estoy haciendo negocios vendiendo dólares y euros si necesitas en efectivo y cuentas bancarias bank of América wellfargo
10:21 AM

Ah si y eso ? 10:23 AM ✓

Por que el periodismo está un poco pésimo
10:24 AM

Es verdad 10:24 AM ✓

Gracias por comunicarte con



Mi nombre es soy tu asesora personalizada.

Para poder verificar en sistema el valor de tu póliza SOAT, me indicas la placa de tu vehículo o motocicleta.

5:29 p. m.

Seller Center ENVÍO GRATIS

HOY SOLO 150.000 COP

1 like
¡Descubre un mundo interminable de juegos con PlayStation 5... more
View 1 comment
See translation

DIFICULTADES DE LA INTELIGENCIA ARTIFICIAL (IA)

DESAFIOS DE LA IA EN COLOMBIA

Identificación de nuevas amenazas, considerando que los ataques informáticos cada día son más sofisticados. Se requiere evolucionar en el ámbito tecnológico y disponer de herramientas que permitan la identificación, prevención e investigación.

Falta de talento humano idóneo para la investigación de conductas generadas con IA.

Ausencia de regulación normativa que permita la formulación de directrices que permitan el uso y desarrollo responsable de la IA en Colombia.

Facilidad en la distribución de aplicaciones y plataformas para la creación de contenido con IA.

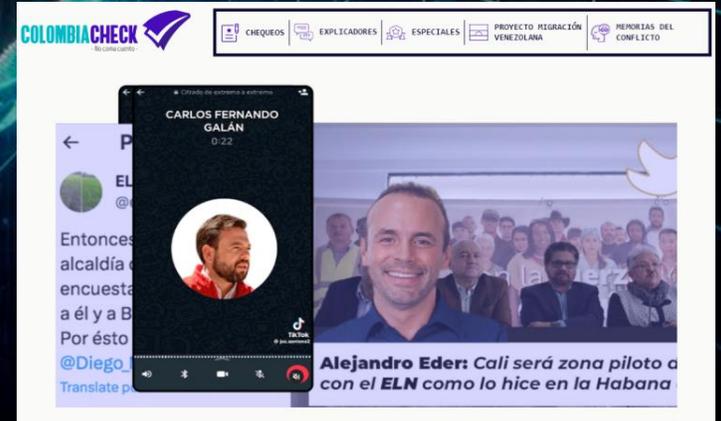
UTILIZACIÓN DE DEEPFAKE Y DEEPTVOICE

Caso ocurrido con el futbolista Luis Díaz y otras figuras públicas, donde se crean videos promocionando emprendimientos fraudulentos, para captar dinero.



LUIS DÍAZ ANUNCIA EL LANZAMIENTO DE UN NUEVO PROYECTO PARA EL PUEBLO DE COLOMBIA

Suplantación de la autoridad electoral y actores de la política nacional en las pasadas elecciones regionales con la finalidad de generar incertidumbre y desconfianza entre la ciudadanía.



DEEPPFAKE

Archivos de video, imagen o voz manipulados mediante softwares de inteligencia artificial, generados para inducir al error a las personas.



DESAFIOS CON LA INTELIGENCIA ARTIFICIAL (IA)

CASOS REGISTRADOS EN COLOMBIA

Caso ocurrido con el futbolista Luis Díaz, donde se creó un video para promocionar un supuesto emprendimiento fraudulento, en un intento por captar dinero.



LUIS DÍAZ ANUNCIA EL LANZAMIENTO DE UN NUEVO PROYECTO PARA EL PUEBLO DE COLOMBIA



TikTok @jojobiden46

DEEVOICE

Permite **clonar la voz de una persona** a partir de muestras de audio, para **suplantar la identidad de personas**, lo que ha llevado a casos de fraudes y estafas.



DESAFIOS CON LA INTELIGENCIA ARTIFICIAL (IA)

CASOS REGISTRADOS EN COLOMBIA

Caso ocurrido con la creación de audios con las voces de los entonces candidatos en las elecciones regionales GALAN, EDER y DILIAN, lo anterior con el fin de difundir mensajes falsos.

COLOMBIA CHECK

CHEQUES EXPLICADORES ESPECIALES PROYECTO HIGRACIÓN VENEZOLANA MEMORIAS DEL CONFLICTO

Alejandro Eder: Cali será zona piloto de diálogos con el ELN como lo hice en la Habana con las FARC.

Cifrado de extremo a extremo

CARLOS FERNANDO GALÁN

0:14

TikTok @jaz.santana2

Audio player controls: speaker, mute, video, volume, and call end button.

ELN

Alejandro Eder: Cali será zona piloto de diálogos con el ELN como lo hice en la Habana con las FARC.

ASPECTOS IMPORTANTES EN LA CIBERSEGURIDAD



PERSONAS

Necesario comprender y cumplir los principios básicos de seguridad de datos, como elegir contraseñas seguras, ser cautelosos con los archivos adjuntos en los correos electrónicos y realizar copias de seguridad de datos.

TECNOLOGÍA

Esencial para brindar las herramientas de seguridad informática a las organizaciones y a los individuos, que permitan protegerse de los ciberataques, enfocado en tres aspectos: dispositivos **Endpoints**, las redes y la nube.

PROCESOS

Las organizaciones requieren una estructura para contrarrestar de los ciberataques tentativos y sospechosos, orientada a identificar riesgos, proteger sistemas, responder a amenazas y recuperarse de ataques exitosos.

16 Operaciones

06 Nivel Central

10 Nivel Desconcentrado

Operaciones Destacadas

ANONYMOUS FASE I - II



Primera captura con fines de extradición

Ataques a más de 500 sitios web (hospitales, colegios e infraestructuras digitales gubernamentales de varios países de América Latina, Europa y Asia.

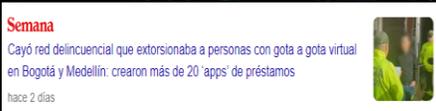
SIN FRONTERAS

FENIX



Desarticulación de una estructura dedicada a la comisión de delitos informáticos, bajo la modalidad ilegal de préstamos digitales gota a gota, afectando cerca de 1.365 personas.

OPERACIÓN "GOTA A GOTA VIRTUAL"



GESTIÓN SEGURIDAD DIGITAL 2024

- 128 Capturas
- 113 Delitos informáticos
- 15 Explotación sexual infantil en internet
- 14.915 Páginas bloqueadas
- 14.104 Material de abuso sexual infantil
- 811 Juegos ilegales de azar
- 3.568 Incidentes atendidos CAI Virtual
- 240 Alertas de ciberseguridad
- 78 Actividades de relacionamiento estratégico
- 27 Charlas ciberseguridad
- 2.387 Personas sensibilizadas
- 70.856 Seguidores redes sociales

NECESIDADES NORMATIVAS

1

Actualización de la Ley 1273 de 2009.

2

Medidas cautelares para números telefónicos vinculados en fraudes.

3

Creación de figura de solicitudes de conservación de datos con fines judiciales.

4

Regulación de cuentas de ahorro de trámite simplificado (CATS).

5

Legislación respecto a criptomonedas (**02** proyectos de ley archivados 139/2021 y 267/2022).

6

Suspensión de dominios relacionados con Phishing / fraudes y estafas.

7

Regulación técnica especial de investigación de agente encubierto para el desarrollo **Operaciones encubiertas en medios de comunicación virtual.**

8

Ley ratificatoria del convenio de Budapest.

9

Legislación que tenga como objeto prevenir, tipificar y sancionar el grooming.

Proyectos de ley para regulación de Inteligencia Artificial

Proyecto de ley 059 del 01/08/2023

Uso e implementación de Inteligencia Artificial.

Estado: pendiente rendir ponencia para segundo debate en Senado.

1

Proyecto de ley 091 del 09/08/2023

Uso de manera responsable y seguro para sus usuarios.

Estado: pendiente discutir ponencia para primer debate en Senado.

2

Proyecto de ley 130 del 06/09/2023

Protección de los derechos de los trabajadores y la correcta utilización de inteligencia artificial.

Estado: pendiente discutir ponencia para primer debate en Senado.

3

Proyectos de ley contra fraude / suplantación

Proyecto de ley 176 del 04/10/2023.

Registro e identificación de usuarios finales de tarjetas SIM y E-SIM.

Estado: pendiente rendir ponencia para primer debate en Senado.

1

Proyecto 303/23 senado 190/22 cámara

Medidas proteger a las personas del por suplantación de identidad ante centrales de riesgo.

Estado: se encuentra en revisión ante la Corte Constitucional.

2

CANALES DE ATENCIÓN



[Https://caivirtual.policia.gov.co](https://caivirtual.policia.gov.co)



@caivirtual



@caivirtual



GRACIAS



Capitán César Eduardo Galvis Pedroza
Jefe Centro Cibernético Policial