UNIVERSIDAD FASTA

FACULTAD DE CS. JURÍDICAS Y SOCIALES

LICENCIATURA EN SEGURIDAD CIUDADANA

TRABAJO FINAL

ESTAFAS INFORMÁTICAS EN LA CIUDAD DE CORONEL SUÁREZ EN EL AÑO 2022.

Autor: Osvaldo Ramiro Olmedo

Correo electrónico: ramiroolmedo47@gmail.com

Tutora: Mg. Paula Ariadna

AÑO 2023

Índice

Tema

Análisis de las Estafas Informáticas en Coronel Suárez durante el Año 2022: Un Estudio sobre la Seguridad Ciudadana.

Introducción

Contextualización

La seguridad ciudadana se ha visto crecientemente amenazada por el avance de las tecnologías de la información y comunicación (TIC), que si bien han aportado innumerables beneficios, también han facilitado la aparición de nuevas formas de criminalidad, como las estafas informáticas. Estas se definen como cualquier fraude cometido a través de medios digitales con el objetivo de obtener un beneficio económico, ya sea mediante engaños, phishing, malware o cualquier otra técnica (Córdoba, 2020).

En Argentina, el auge de las estafas informáticas se ha convertido en un fenómeno preocupante. De acuerdo con datos del Ministerio de Seguridad de la Nación, en los últimos años se ha registrado un aumento significativo en la cantidad de denuncias por delitos informáticos, reflejando un crecimiento paralelo al de la adopción de nuevas tecnologías por parte de la población (Ministerio de Seguridad de la Nación, 2022).

La ciudad de Coronel Suárez, situada en la provincia de Buenos Aires, no ha sido ajena a esta problemática. A pesar de ser una localidad de menor escala en comparación con grandes centros urbanos, los habitantes de Coronel Suárez han experimentado un incremento en la frecuencia y sofisticación de las estafas informáticas, lo que ha generado una preocupación creciente entre sus ciudadanos (García, 2022).

El análisis de las estafas informáticas en Coronel Suárez durante el año 2022 resulta fundamental para comprender el impacto de estos delitos en la seguridad ciudadana local. Este trabajo se centrará en identificar los métodos más comunes de estafa, los perfiles de las víctimas y delincuentes, y las respuestas de las autoridades y la comunidad frente a esta amenaza.

La relevancia de este estudio radica en su capacidad para ofrecer una visión detallada y específica de la problemática en una ciudad pequeña, contribuyendo así a la generación de conocimientos que puedan ser aplicados tanto en Coronel Suárez como en otras localidades con características similares. Para ello, se adoptará un enfoque metodológico riguroso basado en la obra de Hernández Sampieri, que guiará la recolección y análisis de datos de manera sistemática y fundamentada (Hernández Sampieri et al., 2014).

Marco Teórico

El marco teórico de esta investigación se centrará en tres áreas principales: la criminología aplicada a los delitos informáticos, la seguridad informática y la sociología del delito. Este enfoque interdisciplinario permitirá un análisis exhaustivo y contextualizado de las estafas informáticas en Coronel Suárez durante el año 2022.

Criminología y Delitos Informáticos

La criminología estudia las causas, efectos y formas de prevención del crimen. En el contexto de los delitos informáticos, esta disciplina proporciona herramientas para comprender los motivos detrás de las estafas y los perfiles de los delincuentes. Según De Maio (2019), las estafas informáticas se caracterizan por la manipulación de la información digital para obtener beneficios ilícitos, y suelen involucrar un alto grado de planificación y sofisticación técnica.

Garrido (2021) argumenta que los ciberdelincuentes aprovechan las vulnerabilidades tecnológicas y el desconocimiento de los usuarios para perpetrar sus fraudes. Además, destaca que estos delitos a menudo son transnacionales, complicando la persecución legal y la cooperación entre jurisdicciones. En el caso de Coronel Suárez, es importante analizar cómo estas dinámicas globales se manifiestan a nivel local.

Seguridad Informática

La seguridad informática es fundamental para prevenir y mitigar las estafas informáticas. Este campo abarca la protección de los sistemas de información y los datos contra accesos no autorizados, daños o interferencias. Según López y Martínez (2020), las medidas de seguridad informática incluyen la implementación de firewalls, antivirus, y prácticas seguras de manejo de contraseñas y datos sensibles.

En Argentina, la legislación ha avanzado para adaptarse a las nuevas formas de delito. La Ley de Delitos Informáticos (Ley 26.388) establece sanciones específicas para los delitos cometidos a través de medios digitales. Sin embargo, como señala Sánchez (2020), la efectividad de estas medidas depende en gran medida de la educación y concienciación de la población sobre los riesgos y prácticas seguras en internet.

Sociología del Delito

La sociología del delito ofrece una perspectiva sobre cómo los factores sociales y económicos influyen en la aparición y desarrollo de las estafas informáticas. Teorías como la "Teoría de la Oportunidad" sugieren que el crimen ocurre cuando un delincuente percibe una oportunidad con bajo riesgo de aprehensión (Clarke, 2016).

En el contexto de Coronel Suárez, es relevante examinar cómo las condiciones socioeconómicas locales pueden influir en la vulnerabilidad de sus habitantes a las estafas informáticas. García (2022) menciona que la falta de acceso a educación tecnológica y la limitada infraestructura de seguridad informática en pequeñas ciudades pueden aumentar la susceptibilidad de los residentes a estos delitos.

Integración Teórica

La integración de estos tres enfoques permitirá un análisis comprensivo de las estafas informáticas en Coronel Suárez. La criminología proporcionará una base para entender las motivaciones y métodos de los delincuentes, la seguridad informática ofrecerá estrategias para la prevención y respuesta, y la sociología del delito contextualizará el fenómeno dentro de las dinámicas sociales y económicas locales.

Esta combinación teórica no solo facilitará la comprensión del problema, sino que también servirá como base para desarrollar recomendaciones prácticas y efectivas para mejorar la seguridad ciudadana en Coronel Suárez.

Estado de la Cuestión

El estado de la cuestión es una revisión exhaustiva de la literatura existente sobre el tema de las estafas informáticas, con un enfoque particular en el contexto argentino y, más específicamente, en Coronel Suárez. Esta sección se centrará en analizar los estudios previos, identificar las lagunas en el conocimiento y destacar la importancia de la presente investigación.

Estudios Previos sobre Estafas Informáticas en Argentina

En Argentina, las estafas informáticas han sido objeto de creciente atención académica y legislativa en los últimos años. Los estudios indican que el aumento de la conectividad y el uso de dispositivos electrónicos han llevado a un incremento en la incidencia de delitos informáticos (Ministerio de Seguridad de la Nación, 2022).

Un informe del Centro de Estudios en Tecnología y Sociedad (CETyS) de la Universidad de San Andrés revela que las estafas informáticas representan uno de los delitos cibernéticos más reportados en el país, con un crecimiento del 35% entre 2020 y 2022 (CETyS, 2022). Este informe subraya la necesidad de mejorar las capacidades de respuesta y prevención tanto a nivel individual como institucional.

Según una investigación realizada por Pérez y Alonso (2021), los métodos más comunes de estafas informáticas en Argentina incluyen el phishing, el fraude de comercio electrónico y el robo de identidad. Estos métodos explotan las vulnerabilidades de los usuarios, quienes a menudo no están suficientemente informados sobre las medidas de seguridad necesarias para protegerse.

Impacto en Pequeñas Comunidades

En contraste con las grandes ciudades, las pequeñas comunidades como Coronel Suárez enfrentan desafíos únicos en la lucha contra las estafas informáticas. García (2022) destaca que la falta de infraestructura tecnológica avanzada y recursos limitados para la capacitación en seguridad digital aumentan la vulnerabilidad de los residentes de estas localidades. Además, la percepción de menor riesgo en ciudades pequeñas puede llevar a una menor vigilancia y preparación.

Un estudio de la Universidad Nacional del Sur analiza el impacto de los delitos informáticos en pequeñas ciudades de la provincia de Buenos Aires y concluye que la respuesta de las autoridades locales suele ser reactiva más que preventiva, debido a la falta de recursos y capacitación específica (Universidad Nacional del Sur, 2021).

Gaps en la Literatura

A pesar del creciente número de estudios sobre estafas informáticas en Argentina, existen importantes lagunas en la literatura que justifican la realización de esta investigación. Primero, la mayoría de los estudios se concentran en grandes

urbes como Buenos Aires y Córdoba, dejando una brecha en el conocimiento sobre la incidencia y características de estos delitos en comunidades más pequeñas.

Además, los estudios existentes tienden a enfocarse en aspectos técnicos de la seguridad informática, sin integrar adecuadamente las perspectivas criminológicas y sociológicas que son cruciales para una comprensión completa del fenómeno (Córdoba, 2020). Esta investigación busca abordar estas lagunas proporcionando un análisis interdisciplinario y detallado de las estafas informáticas en Coronel Suárez durante 2022.

Importancia de la Investigación Actual

La presente investigación es significativa porque ofrece una perspectiva única y necesaria sobre las estafas informáticas en una pequeña comunidad argentina. Al centrarse en Coronel Suárez, este estudio no solo enriquecerá la literatura existente, sino que también proporcionará datos empíricos que pueden informar políticas y estrategias de prevención tanto a nivel local como nacional.

Asimismo, al combinar enfoques de criminología, seguridad informática y sociología del delito, esta investigación contribuirá a una comprensión más holística del problema, facilitando el desarrollo de soluciones integrales y efectivas para mejorar la seguridad ciudadana en Coronel Suárez.

Justificación

La justificación de esta investigación se sustenta en la necesidad de abordar un problema creciente que afecta directamente la seguridad ciudadana en Coronel Suárez: las estafas informáticas. Este estudio no solo es relevante por su contribución al conocimiento académico, sino también por sus implicaciones prácticas y su potencial impacto en la formulación de políticas públicas.

Relevancia Social

Las estafas informáticas representan una amenaza significativa para la seguridad y el bienestar de los ciudadanos. Estos delitos no solo generan pérdidas económicas, sino que también pueden provocar angustia psicológica y deteriorar la confianza en los sistemas digitales. En Coronel Suárez, donde la comunidad es relativamente pequeña y la interacción social es intensa, el impacto de estos delitos

puede ser aún más profundo, afectando la cohesión social y la percepción de seguridad (García, 2022).

La comprensión detallada de cómo operan las estafas informáticas en Coronel Suárez permitirá desarrollar estrategias más efectivas para prevenir y mitigar estos delitos. Además, este estudio ofrecerá datos específicos que pueden ser utilizados por las autoridades locales y las organizaciones comunitarias para diseñar campañas de concienciación y programas de educación en seguridad informática.

Contribución Académica

Desde una perspectiva académica, esta investigación llenará un vacío significativo en la literatura sobre delitos informáticos en pequeñas comunidades. La mayoría de los estudios existentes se enfocan en grandes ciudades, lo que deja un conocimiento limitado sobre la dinámica de estos delitos en contextos rurales o semiurbanos (De Maio, 2019; Pérez y Alonso, 2021).

Al adoptar un enfoque interdisciplinario que combina criminología, seguridad informática y sociología del delito, este estudio ofrecerá una perspectiva más completa y matizada del problema. Esta integración teórica no solo enriquecerá el campo de estudio de los delitos informáticos, sino que también proporcionará una base sólida para futuras investigaciones en contextos similares.

Implicaciones para Políticas Públicas

Los resultados de esta investigación tendrán importantes implicaciones para la formulación de políticas públicas. Los datos empíricos recolectados podrán informar la creación de leyes y regulaciones más efectivas, así como la implementación de programas de prevención del delito. Además, al identificar las estrategias que han resultado más efectivas en la prevención y respuesta a las estafas informáticas, este estudio puede guiar la asignación de recursos y la capacitación de las fuerzas de seguridad locales (Sánchez, 2020).

En particular, la investigación podría influir en la implementación de políticas educativas que mejoren la alfabetización digital de la población, reduciendo así la vulnerabilidad a las estafas informáticas. También podría destacar la necesidad de una mayor cooperación entre las autoridades locales, provinciales y nacionales para

combatir estos delitos de manera más coordinada y eficiente (Ministerio de Seguridad de la Nación, 2022).

Justificación Personal

A nivel personal, esta investigación representa una oportunidad para contribuir de manera significativa al bienestar de la comunidad de Coronel Suárez. La autora, originaria de esta localidad, tiene un interés particular en mejorar la seguridad y la calidad de vida de sus conciudadanos. Este estudio no solo es una contribución académica, sino también un esfuerzo por retribuir a la comunidad a través de la generación de conocimientos que puedan ser aplicados en la práctica para hacer de Coronel Suárez un lugar más seguro.

Problema

¿Cuáles fueron las características de las estafas informáticas en la ciudad de Coronel Suárez en el año 2022?

Objetivos

Objetivo general

Analizar las características de las estafas informáticas ocurridas en la ciudad de Coronel Suárez en todo el año 2022.

Objetivos específicos

- Identificar los bancos que utilizan los delincuentes para las transferencias electrónicas
- Identificar los tipos más comunes de estafas informáticas
- Determinar la franja etaria de las víctimas de estafa informática
- Determinar los modus operandi de las estafas informáticas

Método

En esta investigación del tipo básico, no experimental como diseño, transversal descriptivo retrospectivo, se medirán las variables luego del que el hecho se halla consumado, no se manipularan las variables independientes, sino que trabajamos sobre lo que generó las variables dependientes, el análisis es de carácter cuantitativo, ósea cantidad de estafas de índole informáticas. Al ser de carácter transversal

tomamos un año especifico donde se sucedieron tales acontecimientos, en este caso todo el año 2022.

Población

Dicha población utilizada para la investigación se basa en las denuncias radicadas por los ciudadanos que fueron damnificados por las estafas informáticas en el distrito de Coronel Suárez en sus distintos modos de actuar, abarcando las localidades de Huanguelen, Santa María, San José, Santa Trinidad, Pasman y Curumalan respectivamente. Cabe señalar que Coronel Suárez es un distrito perteneciente a la provincia a de Buenos Aires, con escasa estadística de hechos delictivos en general.

Marco de muestreo

En este caso analizamos las denuncias realizadas por ciudadanos damnificados de estafas informáticas en el distrito de Coronel Suárez y las dependencias pertenecientes a la misma como Huanguelen, Santa María, San José, Santa Trinidad, Curumalan y Pasman por lo cual no será necesario una muestra, ya que se analizará desde la estadística suministrada por la Jefatura Comunal de Coronel Suárez en todo el transcurso del año 2022.

Operacionalización de las variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIÓN	INDICADORES	INSTRUMENTO
Estafa informática	"Conductas delictivas que derivan de metodologías vinculadas a modificar, manipular, ocultar o alterar datos, sistemas y programas informáticos"	Toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet, combinado con lo telefónico ya sea llamadas, correos WhatsApp.	Perjuicio económico – violación de identidad – detrimento psíquico	Damnificados
Rango etario	Determinado grupo de personas dentro de un rango de edades expuestos o vulnerables a tal situación	Franja de edades	Entre 18 y 30 años, de 30 a 50 años y mayores de 50 años	Damnificados
Tipo de entidad o corporación utilizada para el delito	Conexión entre la entidad financiera o la entidad sin fines de lucro y el delito acaecido	Entidades financieras – Entidades sin fines de lucro	Hospital Español Bahía Blanca – Entidad bancaria - Entidad benéfica	Damnificados
Medios utilizados para concretar el delito	Tipos de ardid o técnica utilizadas por los victimarios para concretar las estafas informáticas	Correos electrónicos falsos – links fraudulentos – WhatsApp – Perfiles de redes sociales falsos	Manipulación social y psicológica	Damnificados

Instrumento de recolección de datos

N° de IPP denuncia	Medios usados para concretar estafa	Tipo de estafa informática	Cuenta bancaria, Alias, CBU perpetrador	Fecha y hora en que se cometió la estafa	Edad del damnificado	Ciudad de residencia del damnificado	Cuenta bancaria Alias, CBU del damnificado

Tipos de estafas informáticas.

- Phishing
- Vishing – Smishing
- Fraude en compraventa en línea
- Paginas falsas o falsos alquileres
- Estafas en redes sociales
- Robo de datos de tarjetas
- Otros fraudes

Datos que aportan los damnificados.

- Fecha, hora y lugar
- Teléfono de contacto
- Datos filiatorios
- Medio por el cual fue contactado
- Motivo del llamado o contacto
- Dinero transferido
- Plataforma o medio empleado ya sea celular, computadora, cajero.
- Cuentas bancarias de destino, CBU, alias.
- Evidencia tales como capturas de pantalla, tiques cajero, comprobantes posnet.

Rango etario de los damnificados.

- De 18 a 30 años
- De 31 a 40 años
- De 41 a 50 años
- De 51 a 60 años
- Mayores de 61 años

Datos obtenidos desde las oficinas de la Jefatura Departamental Coronel Suárez en lo que respecta a las estafas informáticas acaecidas y denunciadas en el transcurso del año 2022:

- Cantidad estafas informáticas analizadas: 63
- Inicio de la muestra: 01 de enero de 2022
- Fin de la muestra: 30 de diciembre de 2022
- Días analizados: 364
- Distrito geográfico: Coronel Suárez, provincia de Buenos Aires.

Entidades financieras involucradas en las distintas estafas informáticas:

- Banco Provincia de Buenos Aires.
- Banco Nación.
- Banco Galicia.
- Banco Patagonia.
- Banco Pampa.
- Banco Santander.
- Banco Macro.
- Ualá.
- Mercado Pago.
- Naranja X.
- Banco HSBC
- Wilobank S.A.

Resultados

Analizada toda la información recabada en la Jefatura Departamental Coronel Suárez en el transcurso del año 2022, arroja como modalidad predominante ante una estafa informática, la de phishing, en todas sus variantes.

Esta técnica que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta consiste en apropiarse de la identidad de las personas enviando mails falsos como anzuelo para pescar contraseñas y datos personales de gran valor que ha sido usado de manera reiterativa en los casos analizados.

Estos correos electrónicos o mails tienen contenido falso y enlaces que redirigen las respuestas hacia páginas de web falsas con formularios y preguntas para obtener datos personales o privados.

Estos correos electrónicos pueden aparecer como mensajes de bancos, servicios de pago, mercados de compra en línea o proveedores de algún servicio público.

En general estos correos o mails solicitan:

- completar formularios o hacer clic en un link para obtener alguna información o archivo clave;
- hacer clic en un link que redirige a una página fraudulenta;
- descargar un archivo adjunto importante.

Los ciberdelincuentes desean obtener:

- datos de contraseñas privadas
- números y claves de tarjetas de crédito
- DNI
- CUIT o CUIL
- Nombres o claves de usuario
- códigos PIN

Cuando adquieren estos datos pueden realizar compras, reservas o extracciones de dinero a nombre del damnificado.

Las distintas estafas informáticas discriminadas por modalidad desde el mes de enero a diciembre del año 2022 en el distrito de Coronel Suárez llegando a la suma de 63 y son:

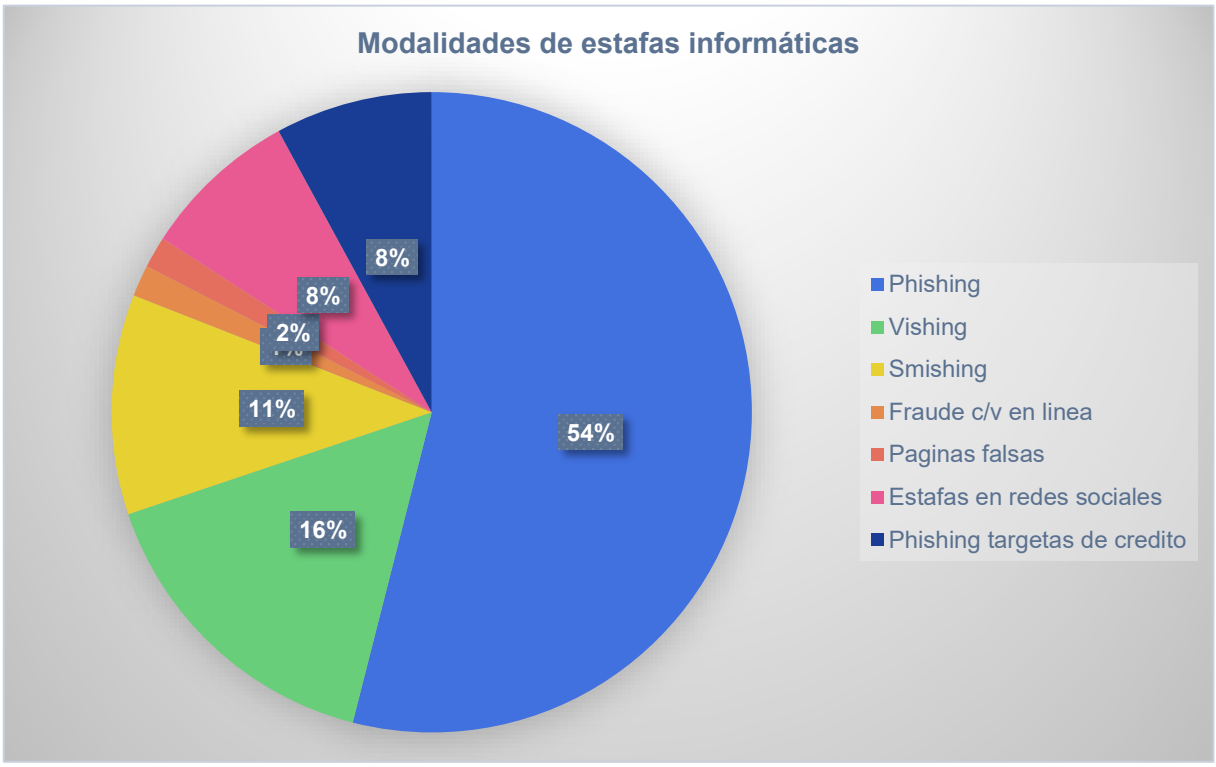
- Phishing: 34
- Vishing: 10
- Smishing: 7
- Fraude por compra y venta en línea: 1
- Paginas falsas: 1
- Estafas en redes sociales: 5
- Phisihing en tarjetas credito: 5

Gráfico N°1

Modalidades de estafas informáticas

El auge de la tecnología y la creciente digitalización de las transacciones financieras han traído consigo nuevos desafíos en materia de seguridad ciudadana. En este contexto, las estafas informáticas se han convertido en una preocupación significativa para las comunidades, incluida la ciudad de Coronel Suárez. El Gráfico 1 presenta una visión panorámica de las diferentes modalidades de estafas informáticas registradas en esta localidad durante el año 2022, ofreciendo una perspectiva cuantitativa de los métodos empleados por los delincuentes cibernéticos.

Este análisis resulta crucial para comprender la naturaleza y la prevalencia de las amenazas digitales que enfrentan los ciudadanos de Coronel Suárez. La información proporcionada no solo ilustra la diversidad de tácticas utilizadas por los estafadores, sino que también pone de manifiesto la necesidad de implementar estrategias de prevención y educación adaptadas a las modalidades más frecuentes. Además, estos datos pueden servir como base para que las autoridades locales y las instituciones financieras desarrollen medidas de seguridad más efectivas y dirijan sus esfuerzos hacia la protección contra los tipos de estafas más comunes en la región.



Fuente: Jefatura de policía comunal Coronel Suárez.

El Gráfico 1 revela una distribución desigual entre las diferentes modalidades de estafas informáticas en Coronel Suárez durante el año 2022. El phishing se destaca como la técnica predominante, con 34 casos reportados, lo que representa aproximadamente el 54% del total de incidentes. Esta prevalencia sugiere que los estafadores están aprovechando la falta de conocimiento o precaución de los usuarios al interactuar con comunicaciones electrónicas aparentemente legítimas.

El vishing y el smishing ocupan el segundo y tercer lugar, con 10 y 7 casos respectivamente. Estas modalidades, que implican el uso de llamadas telefónicas (vishing) y mensajes de texto (smishing) para engañar a las víctimas, indican una diversificación en las tácticas de los delincuentes, adaptándose a diferentes canales de comunicación.

Las estafas en redes sociales y el phishing de tarjetas de crédito comparten el cuarto lugar, con 5 casos cada uno. Esto refleja la explotación de plataformas populares y la persistencia de métodos tradicionales de fraude financiero en el entorno digital.

Es notable que las modalidades de fraude en compra-venta en línea y el uso de páginas falsas sean las menos frecuentes, con solo un caso reportado cada una. Esto podría indicar una mayor conciencia entre los usuarios sobre los riesgos

asociados con estas formas de estafa o una preferencia de los delincuentes por métodos más directos de engaño.

La diversidad de modalidades observadas subraya la importancia de una educación integral en seguridad digital para los ciudadanos de Coronel Suárez. Asimismo, estos datos pueden orientar a las autoridades locales y entidades financieras en la implementación de medidas preventivas específicas, centrándose especialmente en combatir el phishing, que representa más de la mitad de los casos reportados.

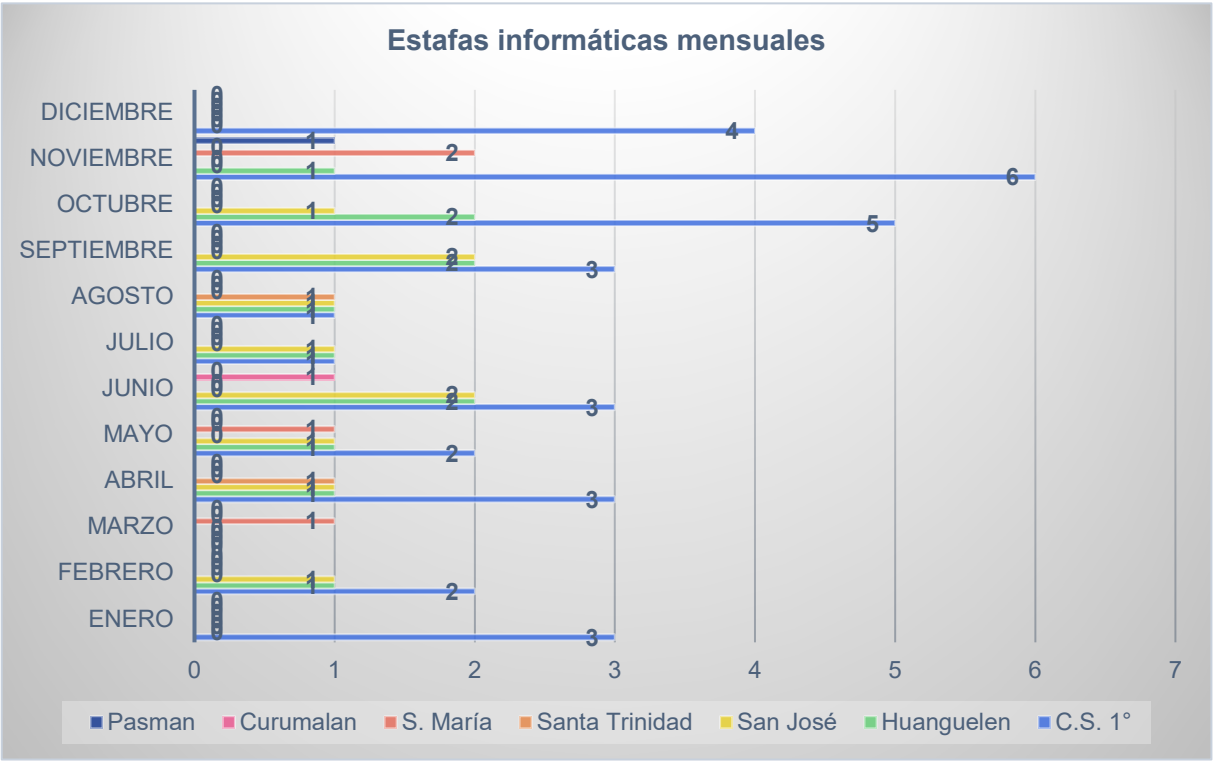
Gráfico N°2

Estadística mensual en el distrito de Coronel Suárez en el transcurso del año 2022.

El Gráfico 2 presenta una visión detallada de la distribución mensual de estafas informáticas en el distrito de Coronel Suárez durante el año 2022, desglosando los incidentes por localidades específicas. Este análisis temporal y geográfico es fundamental para comprender las tendencias y patrones de la ciberdelincuencia en la región, proporcionando información valiosa para las autoridades locales y los responsables de la seguridad ciudadana.

La representación gráfica abarca siete localidades del distrito: Coronel Suárez 1°, Huanguelén, San José, Santa Trinidad, Santa María, Curumalan y Pasman. Esta desagregación permite una evaluación más precisa de la distribución espacial de las estafas informáticas, revelando potenciales focos de actividad delictiva y áreas que podrían requerir una atención especial en términos de prevención y educación en seguridad digital.

El análisis mensual, por su parte, ofrece la oportunidad de identificar posibles estacionalidades o períodos de mayor vulnerabilidad a lo largo del año. Esta información es crucial para la planificación de estrategias de seguridad y campañas de concientización, permitiendo una asignación más eficiente de recursos y esfuerzos en la lucha contra el cibercrimen en el distrito de Coronel Suárez.



Fuente: Jefatura de policía comunal Coronel Suárez.

El análisis del Gráfico 2 revela patrones interesantes en la incidencia de estafas informáticas en el distrito de Coronel Suárez durante 2022. En primer lugar, se observa que Coronel Suárez 1° es consistentemente la localidad más afectada, registrando casos en todos los meses excepto marzo. Esto sugiere que, como centro urbano principal del distrito, podría ser un objetivo preferente para los ciberdelincuentes.

Se percibe un aumento notable en la frecuencia de estafas hacia el final del año, con picos en octubre (9 casos en total) y noviembre (10 casos). Este incremento podría estar relacionado con un aumento en las transacciones en línea durante la temporada de compras previa a las fiestas de fin de año, lo que subraya la necesidad de reforzar las medidas de seguridad y las campañas de concientización durante estos períodos.

Huanguelén y San José muestran patrones similares, con incidentes repartidos a lo largo del año, pero con una frecuencia menor que Coronel Suárez 1°. Estas localidades podrían beneficiarse de programas de educación en ciberseguridad adaptados a sus características específicas.

Las localidades de Santa Trinidad, Santa María, Curumalan y Pasman presentan casos esporádicos, lo que podría indicar una menor exposición a riesgos

cibernéticos o una subnotificación de incidentes. Sin embargo, la presencia de casos aislados en estas áreas menos pobladas subraya la necesidad de una estrategia de seguridad digital que abarque todo el distrito.

Es notable la ausencia de un patrón estacional claro, con fluctuaciones mes a mes en la mayoría de las localidades. Esto sugiere que las estafas informáticas son un problema persistente durante todo el año, requiriendo una vigilancia constante y esfuerzos continuos de prevención.

Gráfico N°3

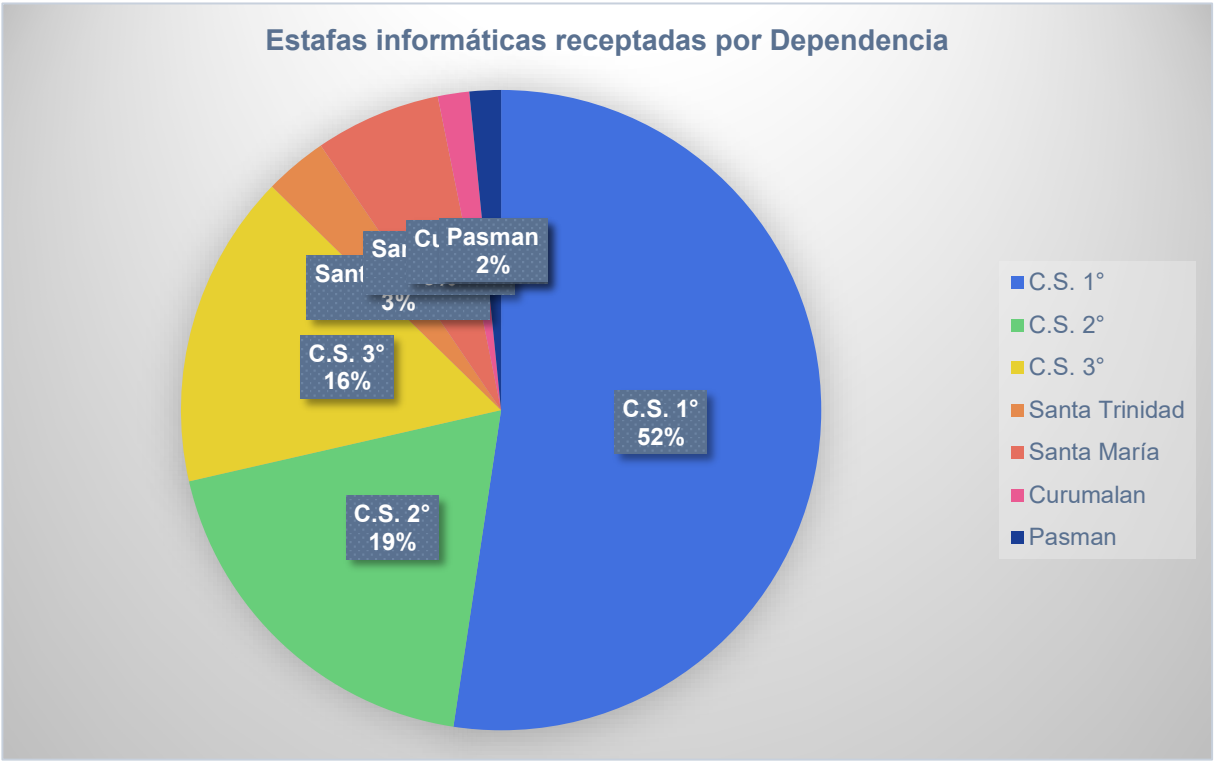
Estafas informáticas receptadas por Dependencia

El Gráfico 3 presenta una visión detallada de la distribución de estafas informáticas receptadas por las diferentes dependencias policiales en el distrito de Coronel Suárez durante el año 2022. Este análisis es fundamental para comprender la carga de trabajo relacionada con ciberdelitos que enfrenta cada dependencia y para identificar las áreas geográficas más afectadas por este tipo de delincuencia.

La información proporcionada por este gráfico es crucial para la planificación estratégica de recursos y personal en las distintas dependencias policiales del distrito. Además, ofrece una perspectiva valiosa sobre la posible concentración de actividades delictivas en ciertas zonas, lo que puede ayudar a las autoridades a desarrollar estrategias de prevención más efectivas y focalizadas.

Este tipo de datos no solo es relevante para las fuerzas de seguridad, sino también para los responsables de políticas públicas y para la comunidad en general. Comprender la distribución geográfica de las estafas informáticas puede contribuir a una mayor concienciación ciudadana y a la implementación de programas de

educación en seguridad digital adaptados a las necesidades específicas de cada área del distrito de Coronel Suárez.



Fuente: Jefatura de policía comunal Coronel Suárez.

El análisis del Gráfico 3 revela una distribución desigual de las estafas informáticas entre las diferentes dependencias policiales del distrito de Coronel Suárez. La dependencia Coronel Suárez 1° se destaca significativamente, habiendo receptado 33 casos, lo que representa aproximadamente el 52% del total de estafas informáticas reportadas en el distrito durante 2022. Este dato sugiere que el área cubierta por esta dependencia podría ser un punto focal para las actividades de ciberdelincuencia, posiblemente debido a una mayor densidad poblacional o a una mayor actividad económica y digital en la zona.

Las dependencias Coronel Suárez 2° y 3° siguen en orden de importancia, con 12 y 10 casos respectivamente. Juntas, estas tres dependencias principales de Coronel Suárez acumulan el 87% de todos los casos reportados, lo que indica una concentración significativa de la actividad delictiva informática en el núcleo urbano principal del distrito.

En contraste, las dependencias de las localidades más pequeñas como Santa María (4 casos), Santa Trinidad (2 casos), Curumalan (1 caso) y Pasman (1 caso) muestran una incidencia notablemente menor de estafas informáticas. Esta disparidad

podría reflejar diferencias en el acceso y uso de tecnologías digitales entre las áreas urbanas y rurales del distrito, o posiblemente una menor tasa de reporte en las localidades más pequeñas.

Estos resultados sugieren la necesidad de un enfoque diferenciado en la prevención y combate de las estafas informáticas en el distrito. Mientras que las dependencias de Coronel Suárez podrían requerir recursos adicionales y programas de prevención más intensivos, las localidades más pequeñas podrían beneficiarse de campañas de concientización específicas y mejoras en los canales de reporte de incidentes.

Además, esta distribución podría indicar la necesidad de una mayor cooperación entre las dependencias, especialmente en términos de compartir información y recursos para abordar este problema de manera más efectiva en todo el distrito.

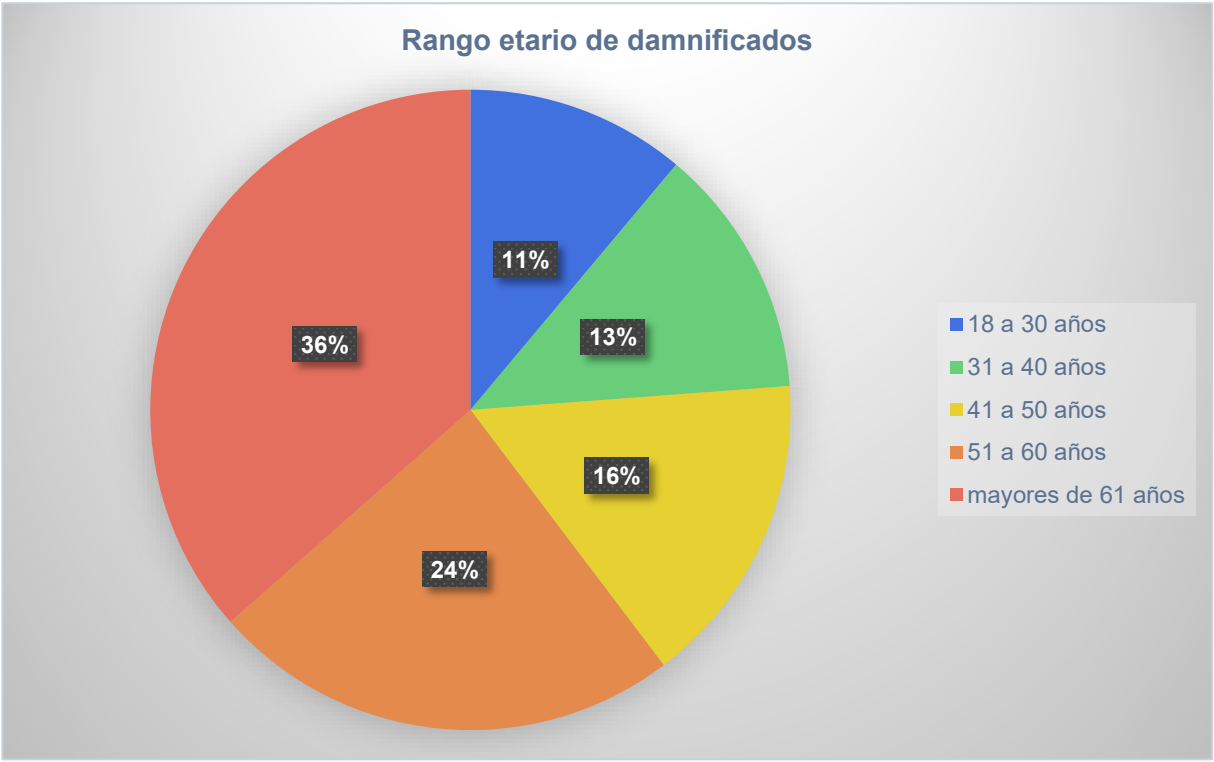
Gráfico N°4

Rango etario de damnificados

El Gráfico 4 presenta una distribución detallada del rango etario de las víctimas de estafas informáticas en el distrito de Coronel Suárez durante el año 2022. Este análisis demográfico es crucial para comprender qué grupos de edad son más vulnerables a los ciberdelitos en la región, proporcionando información valiosa para el diseño de estrategias de prevención y educación en seguridad digital.

La segmentación por edades permite identificar patrones de vulnerabilidad que pueden estar relacionados con factores como la familiaridad con la tecnología, los hábitos de uso de internet, o incluso las circunstancias socioeconómicas de diferentes grupos etarios. Esta información es fundamental no solo para las autoridades encargadas de la seguridad ciudadana, sino también para instituciones educativas, entidades financieras y organizaciones comunitarias que buscan proteger a la población de las amenazas cibernéticas.

Además, el análisis de estos datos puede revelar brechas en la educación digital y la concienciación sobre seguridad en línea entre diferentes generaciones. Esto, a su vez, puede guiar el desarrollo de programas de alfabetización digital y campañas de prevención específicamente dirigidas a los grupos de edad más afectados, mejorando así la resiliencia de la comunidad frente a las estafas informáticas.



Fuente: Jefatura de policía comunal Coronel Suárez.

El análisis del Gráfico 4 revela una tendencia clara en la distribución etaria de las víctimas de estafas informáticas en Coronel Suárez durante 2022. Se observa un aumento progresivo en el número de víctimas a medida que aumenta la edad, con el grupo de mayores de 61 años siendo el más afectado.

El grupo de 18 a 30 años registra el menor número de víctimas (7 casos), seguido de cerca por el grupo de 31 a 40 años (8 casos). Esta menor incidencia en los grupos más jóvenes podría atribuirse a una mayor familiaridad con la tecnología y una mejor comprensión de los riesgos asociados con las actividades en línea.

Se observa un incremento en los casos para el grupo de 41 a 50 años (10 casos), que se acentúa significativamente en el rango de 51 a 60 años (15 casos). Este aumento podría indicar una brecha generacional en términos de alfabetización digital y conciencia sobre seguridad en línea.

El dato más alarmante es el correspondiente al grupo de mayores de 61 años, con 23 casos, representando aproximadamente el 36% del total de víctimas. Esta sobrerrepresentación sugiere una vulnerabilidad particular en este grupo etario, posiblemente debido a una menor familiaridad con las nuevas tecnologías, una mayor confianza en las comunicaciones recibidas, o quizás por ser percibidos como objetivos más lucrativos por los estafadores.

Estos hallazgos subrayan la necesidad urgente de implementar programas de educación en seguridad digital específicamente dirigidos a adultos mayores. Asimismo, sugieren la importancia de fortalecer las redes de apoyo comunitario y familiar para proteger a los grupos más vulnerables.

Para los grupos de edad más jóvenes, aunque menos afectados, sigue siendo crucial mantener y actualizar los programas de concientización sobre seguridad en línea, adaptándolos a las nuevas tendencias y tecnologías emergentes.

Gráfico N°5

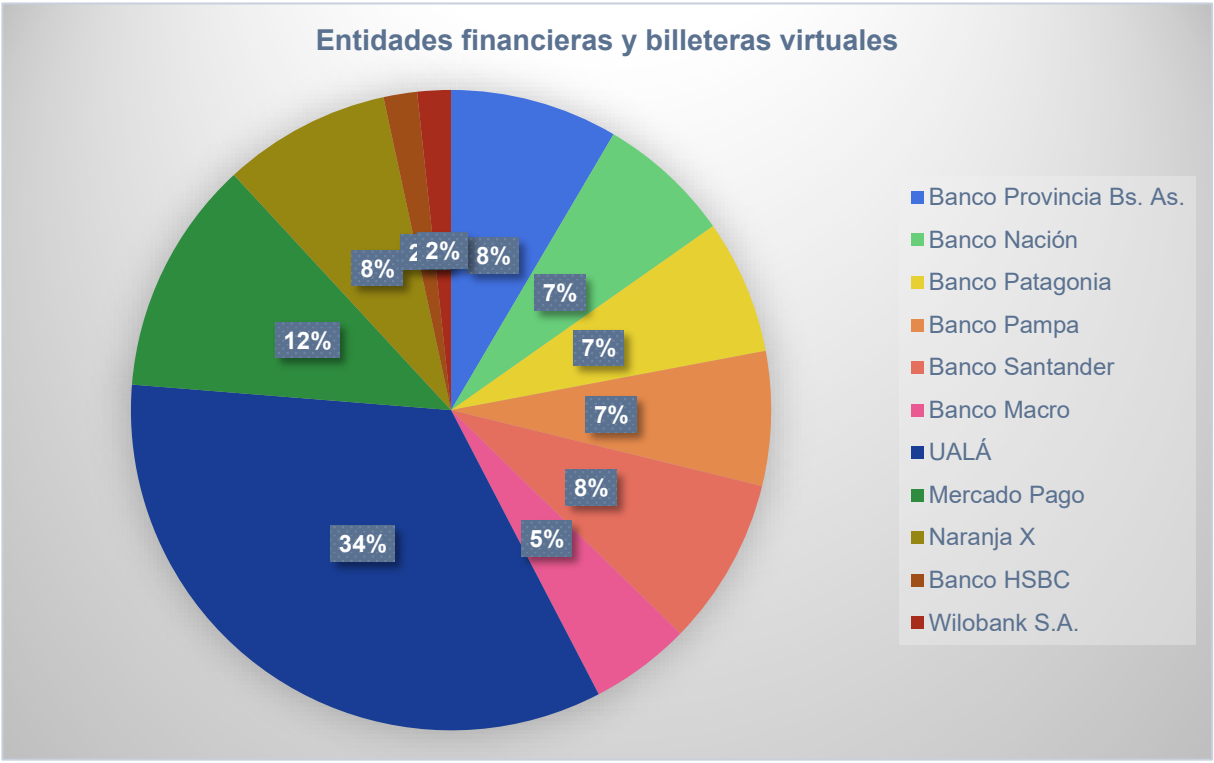
Entidades financieras y billeteras virtuales

El Gráfico 5 presenta una visión detallada de las entidades financieras y billeteras virtuales involucradas en los casos de estafas informáticas en Coronel Suárez durante el año 2022. Este análisis es fundamental para comprender el panorama de la ciberdelincuencia financiera en la región, revelando las preferencias de los estafadores y las posibles vulnerabilidades en diferentes plataformas financieras.

La información proporcionada abarca una amplia gama de instituciones, desde bancos tradicionales hasta nuevas fintech, ofreciendo una perspectiva integral del ecosistema financiero digital y su susceptibilidad a actividades fraudulentas. Este tipo de datos es crucial no solo para las entidades financieras en su lucha contra el fraude, sino también para los reguladores y las fuerzas de seguridad en el desarrollo de estrategias de prevención más efectivas.

Además, este gráfico proporciona información valiosa para los ciudadanos de Coronel Suárez, ayudándoles a comprender los riesgos asociados con diferentes plataformas financieras. Esta concienciación es esencial para promover prácticas más

seguras en las transacciones digitales y para fomentar una cultura de vigilancia entre los usuarios de servicios financieros en línea.



Fuente: Jefatura de policía comunal Coronel Suarez.

El análisis del Gráfico 5 revela patrones significativos en la distribución de estafas informáticas entre diferentes entidades financieras y billeteras virtuales en Coronel Suárez durante 2022. Lo más destacable es la predominancia de UALÁ, una billetera virtual, con 20 casos reportados, lo que representa aproximadamente el 33.9% del total. Este dato sugiere una clara preferencia de los estafadores por las plataformas fintech, posiblemente debido a su facilidad de uso, rápidas transacciones y, quizás, medidas de seguridad menos robustas en comparación con los bancos tradicionales.

Entre las entidades bancarias tradicionales, el Banco Provincia de Buenos Aires y el Banco Santander lideran con 5 casos cada uno, seguidos de cerca por el Banco Nación, Patagonia y Pampa, cada uno con 4 casos. Esta distribución relativamente uniforme entre los bancos principales sugiere que los estafadores no se centran en una institución específica, sino que explotan oportunidades en múltiples entidades.

Mercado Pago, otra plataforma de pagos digitales popular, aparece con 7 casos, reforzando la tendencia hacia el uso de servicios financieros digitales en las

estafas. Naranja X, con 5 casos, también contribuye a esta tendencia de preferencia por las billeteras virtuales.

Es notable la baja incidencia en entidades como HSBC y Wilobank S.A., con solo un caso cada uno. Esto podría indicar una menor penetración de estos bancos en la región o posiblemente la implementación de medidas de seguridad más efectivas.

La prevalencia de plataformas fintech como UALÁ y Mercado Pago en estos incidentes subraya la necesidad urgente de fortalecer la seguridad en estas plataformas emergentes. Para los bancos tradicionales, aunque la incidencia es menor, la distribución de casos entre varias entidades indica la importancia de mantener y mejorar constantemente sus medidas de seguridad.

Estos hallazgos sugieren la necesidad de un enfoque integral en la prevención de estafas que incluya tanto a las instituciones financieras tradicionales como a las emergentes plataformas fintech, así como una mayor educación financiera digital para los usuarios de Coronel Suárez.

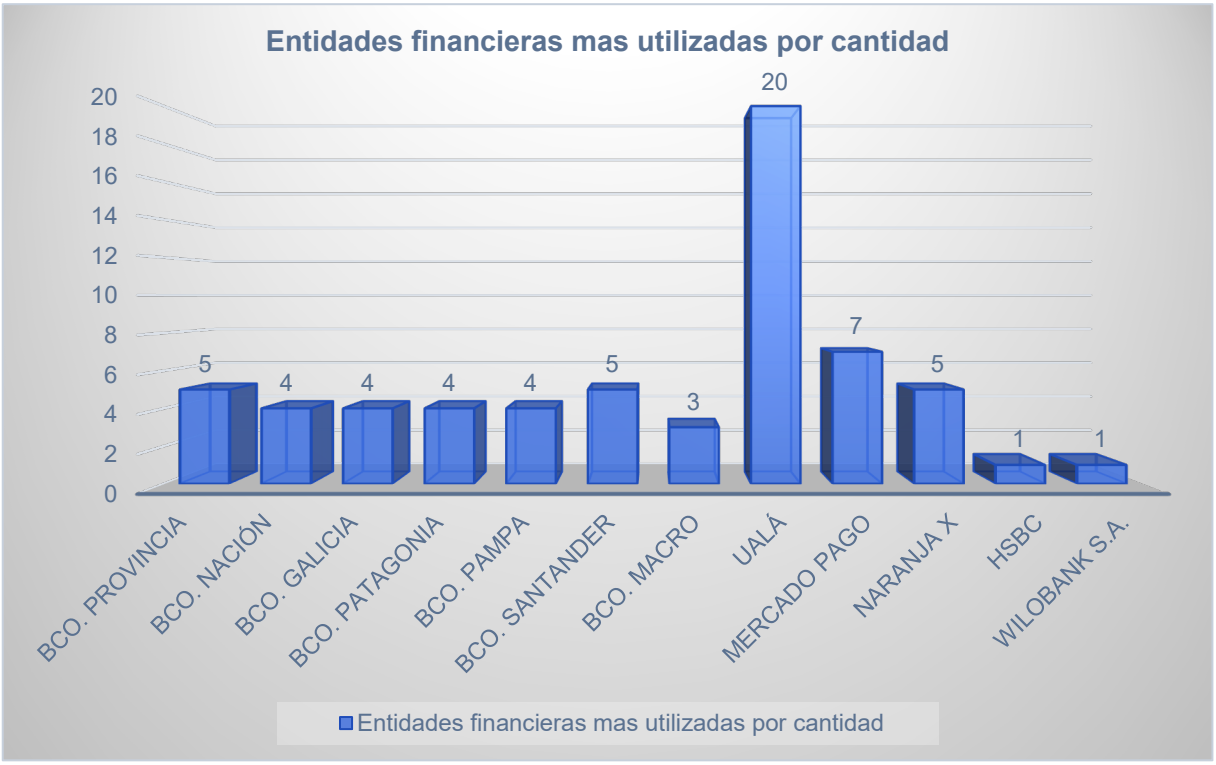
Gráfico N°6

Entidades financieras más utilizadas por cantidad

El Gráfico 6 presenta una visión detallada de las entidades financieras más utilizadas en los casos de estafas informáticas en Coronel Suárez durante el año 2022. Este análisis es crucial para comprender las preferencias de los ciberdelincuentes y las vulnerabilidades potenciales en los sistemas financieros locales. La información proporcionada no solo revela cuáles son las instituciones más frecuentemente implicadas en estos incidentes, sino que también ofrece una perspectiva sobre la evolución del panorama financiero digital en la región.

Este gráfico es particularmente relevante para las instituciones financieras, las autoridades reguladoras y los cuerpos de seguridad, ya que proporciona datos concretos sobre los canales más explotados por los estafadores. Además, esta información puede ser invaluable para el desarrollo de estrategias de prevención más efectivas y para la implementación de medidas de seguridad reforzadas en las entidades más afectadas.

La diversidad de instituciones representadas en el gráfico, que incluye tanto bancos tradicionales como nuevas plataformas de fintech, refleja la complejidad del ecosistema financiero actual y los desafíos que presenta para la seguridad de los usuarios en Coronel Suárez.



Fuente: Jefatura de policía comunal Coronel Suárez.

El análisis del Gráfico 6 revela patrones significativos en cuanto a las entidades financieras utilizadas en los casos de estafas informáticas en Coronel Suárez durante 2022. Lo más destacable es el predominio de UALÁ, una billetera virtual, con 20 casos reportados, lo que representa aproximadamente el 31.7% del total. Este dato sugiere una preferencia marcada de los estafadores por las plataformas fintech, posiblemente debido a la facilidad de uso y la rápida transferencia de fondos que ofrecen.

Entre las entidades bancarias tradicionales, el Banco Provincia y el Banco Santander lideran con 5 casos cada uno, seguidos de cerca por el Banco Nación, Galicia, Patagonia y Pampa, cada uno con 4 casos. Esta distribución relativamente uniforme entre los bancos principales sugiere que los estafadores no se centran en una institución bancaria específica, sino que explotan oportunidades en múltiples entidades.

Mercado Pago, otra plataforma de pagos digitales, aparece con 7 casos, reforzando la tendencia hacia el uso de servicios financieros digitales en las estafas. Naranja X, con 5 casos, también contribuye a esta tendencia.

Es notable la presencia de entidades con menor incidencia, como HSBC y Wilobank S.A., con solo un caso cada uno. Esto podría indicar una menor penetración de estos bancos en la región o posiblemente mejores medidas de seguridad implementadas.

La prevalencia de plataformas fintech como UALÁ y Mercado Pago en estos incidentes sugiere la necesidad de una mayor regulación y supervisión de estos servicios, así como la implementación de medidas de seguridad más robustas. Para los bancos tradicionales, aunque la incidencia es menor, la distribución de casos entre varias entidades indica la necesidad de una colaboración interinstitucional para combatir estas estafas.

Estos hallazgos subrayan la importancia de educar a los usuarios sobre los riesgos asociados con las nuevas tecnologías financieras, sin descuidar la seguridad en las operaciones bancarias tradicionales. Además, sugieren la necesidad de un enfoque integral en la prevención de estafas que incluya tanto a las instituciones financieras tradicionales como a las emergentes plataformas fintech.

Discusión y conclusiones

Discusión sobre el logro de los objetivos:

El presente estudio sobre las estafas informáticas en Coronel Suárez durante el año 2022 se propuso analizar las características de estos delitos cibernéticos, estableciendo objetivos específicos que han sido abordados a través de los datos presentados en los seis gráficos analizados.

En cuanto al objetivo general de analizar las características de las estafas informáticas ocurridas en la ciudad de Coronel Suárez en todo el año 2022, se puede afirmar que se ha logrado satisfactoriamente. Los gráficos proporcionados ofrecen una visión completa de diversos aspectos de estas estafas, desde las modalidades empleadas hasta la distribución temporal y geográfica de los incidentes.

Respecto a los objetivos específicos, el estudio ha cumplido en gran medida con las metas propuestas:

1. Identificar los bancos que utilizan los delincuentes para las transferencias electrónicas: El Gráfico 5 y el Gráfico 6 proporcionan información detallada sobre las entidades financieras y billeteras virtuales involucradas en las estafas. Se observa una clara identificación de las instituciones más utilizadas, destacando la prevalencia de plataformas fintech como UALÁ y Mercado Pago, así como la participación de bancos tradicionales como el Banco Provincia y el Banco Santander.

2. Identificar los tipos más comunes de estafas informáticas: El Gráfico 1 cumple directamente con este objetivo, mostrando las diferentes modalidades de estafas y su frecuencia. El phishing se destaca como el método más común, seguido por el vishing y el smishing.

3. Determinar la franja etaria de las víctimas de estafa informática: El Gráfico 4 aborda específicamente este objetivo, proporcionando una clara distribución de las víctimas por grupos de edad. Se observa una tendencia creciente de vulnerabilidad con la edad, siendo los mayores de 61 años el grupo más afectado.

4. Determinar los modus operandi de las estafas informáticas: Aunque no se proporciona un gráfico específico sobre los métodos detallados, el Gráfico 1

ofrece información valiosa sobre las modalidades utilizadas, que se puede considerar como una aproximación a los modus operandi de los estafadores.

Se puede afirmar que los objetivos del trabajo se han alcanzado en gran medida. La investigación ha proporcionado una visión comprensiva de las características de las estafas informáticas en Coronel Suárez, cumpliendo con el objetivo general. Los objetivos específicos se han abordado de manera satisfactoria, aunque el último, relacionado con los modus operandi, podría beneficiarse de información más detallada sobre las tácticas específicas empleadas por los estafadores. No obstante, la información proporcionada ofrece una base sólida para comprender la naturaleza y el alcance de las estafas informáticas en la región durante el período estudiado.

Entendido. A continuación, desarrollaré una discusión sobre las limitaciones del trabajo, con una extensión mínima de 250 palabras.

Limitaciones del trabajo:

A pesar de los valiosos insights proporcionados por este estudio sobre las estafas informáticas en Coronel Suárez durante el año 2022, es importante reconocer y discutir las limitaciones inherentes a la investigación. Estas limitaciones no solo contextualizan los hallazgos, sino que también ofrecen oportunidades para futuras investigaciones en el campo.

1. Alcance geográfico limitado: El estudio se centra exclusivamente en Coronel Suárez y sus alrededores. Aunque esto proporciona una visión detallada de la situación local, limita la capacidad de generalizar los resultados a otras regiones o contextos urbanos más amplios. Las dinámicas de las estafas informáticas pueden variar significativamente entre diferentes áreas geográficas, lo que sugiere la necesidad de estudios comparativos más amplios.
2. Período de tiempo acotado: La investigación se limita al año 2022, lo que ofrece una instantánea valiosa pero no permite observar tendencias a largo plazo o cambios en los patrones de estafas informáticas a lo largo del tiempo. Esto puede ocultar variaciones cíclicas o evolutivas en las tácticas de los ciberdelincuentes.

3. Subregistro potencial: Los datos analizados se basan en casos reportados a las autoridades locales. Existe la posibilidad de un subregistro significativo, ya que muchas víctimas de estafas informáticas pueden optar por no denunciar los incidentes por vergüenza, desconocimiento o falta de confianza en el sistema. Esto podría llevar a una subestimación de la magnitud real del problema.

4. Falta de detalles sobre los modus operandi: Aunque el estudio identifica las modalidades generales de estafas, carece de información detallada sobre las tácticas específicas empleadas por los estafadores. Esta limitación dificulta la comprensión profunda de cómo se ejecutan estas estafas y, por ende, cómo prevenirlas más efectivamente.

5. Ausencia de datos sobre el impacto económico: El estudio no proporciona información sobre las pérdidas financieras asociadas con estas estafas, lo que limita la comprensión del impacto económico real en la comunidad de Coronel Suárez.

6. Limitaciones en la categorización de las estafas: La clasificación de las estafas en categorías generales como phishing, vishing, etc., puede simplificar excesivamente la naturaleza compleja y en constante evolución de los ciberdelitos, perdiendo potencialmente matices importantes en las tácticas utilizadas.

7. Falta de información sobre la eficacia de las medidas preventivas: El estudio no aborda la efectividad de las estrategias de prevención o educación existentes en la comunidad, lo que limita la capacidad de proponer mejoras basadas en evidencia.

8. Ausencia de perspectiva de los perpetradores: La investigación se centra en las víctimas y los métodos utilizados, pero carece de información sobre los perpetradores, sus motivaciones y su organización, lo que podría ser crucial para desarrollar estrategias de prevención más efectivas.

Estas limitaciones, aunque significativas, no disminuyen el valor de los hallazgos del estudio. Más bien, proporcionan un contexto importante para interpretar los resultados y ofrecen direcciones claras para futuras investigaciones en el campo de la ciberseguridad y la prevención de estafas informáticas en contextos locales.

Futuras Investigaciones

El presente estudio sobre las estafas informáticas en Coronel Suárez durante el año 2022 ha proporcionado valiosos insights sobre la naturaleza y distribución de estos delitos cibernéticos en la región sin embargo también ha revelado áreas que requieren una exploración más profunda y detallada para comprender completamente el fenómeno y desarrollar estrategias de prevención más efectivas

Una dirección crucial para futuras investigaciones sería la ampliación del alcance geográfico del estudio para incluir otras ciudades y regiones lo que permitiría realizar análisis comparativos y identificar patrones más amplios en la incidencia y características de las estafas informáticas esto podría revelar si las tendencias observadas en Coronel Suárez son específicas de la localidad o parte de un fenómeno más amplio a nivel regional o nacional

Otra área importante para futuras investigaciones es la realización de estudios longitudinales que abarquen varios años esto permitiría identificar tendencias a largo plazo evolución de las tácticas de los estafadores y la efectividad de las medidas preventivas implementadas a lo largo del tiempo tal enfoque longitudinal podría proporcionar insights valiosos sobre cómo las estafas informáticas se adaptan a las cambiantes tecnologías y medidas de seguridad

Se recomienda también llevar a cabo investigaciones cualitativas que incluyan entrevistas detalladas con víctimas de estafas informáticas para comprender mejor los factores psicológicos y situacionales que contribuyen a la vulnerabilidad ante estos delitos este tipo de estudio podría arrojar luz sobre las experiencias personales de las víctimas sus procesos de toma de decisiones y las secuelas emocionales y financieras de las estafas lo que a su vez podría informar el desarrollo de programas de prevención y apoyo más efectivos

Futuras investigaciones deberían abordar también el aspecto económico de las estafas informáticas cuantificando las pérdidas financieras asociadas con estos delitos en la región esto proporcionaría una comprensión más clara del impacto económico real de las estafas en la comunidad y podría justificar mayores inversiones en medidas de prevención y educación

Un área de investigación particularmente importante sería el estudio de la efectividad de diferentes estrategias de prevención y educación en ciberseguridad

esto podría incluir la evaluación de programas de concientización campañas educativas y medidas de seguridad implementadas por instituciones financieras y autoridades locales tal investigación podría proporcionar evidencia empírica sobre qué enfoques son más efectivos para reducir la incidencia de estafas informáticas

Además, se sugiere realizar investigaciones sobre el perfil y las motivaciones de los perpetradores de estafas informáticas aunque desafiante desde el punto de vista metodológico este tipo de estudio podría proporcionar insights valiosos sobre cómo operan los estafadores sus redes y sus procesos de selección de objetivos esta información sería crucial para desarrollar estrategias de prevención más efectivas y mejorar las técnicas de investigación y enjuiciamiento

Otra área prometedora para futuras investigaciones es el estudio de la intersección entre las estafas informáticas y otras formas de delincuencia cibernética como el robo de identidad o el lavado de dinero esto podría revelar conexiones más amplias y complejas en el ecosistema del cibercrimen y proporcionar una comprensión más holística de los desafíos de seguridad que enfrenta la comunidad

Finalmente se recomienda explorar el papel de las nuevas tecnologías tanto en la perpetración como en la prevención de estafas informáticas esto podría incluir el estudio del uso de inteligencia artificial y aprendizaje automático en la detección temprana de actividades fraudulentas así como la investigación sobre cómo los estafadores podrían explotar estas mismas tecnologías para desarrollar tácticas más sofisticadas

Entendido. Desarrollaré las propuestas como futuro Licenciado en Seguridad Ciudadana con una extensión mínima de 250 palabras.

Propuestas como futuro Licenciado en Seguridad Ciudadana:

Como futuro Licenciado en Seguridad Ciudadana, y basándome en los resultados de este estudio sobre estafas informáticas en Coronel Suárez, propongo las siguientes medidas para mejorar la seguridad cibernética y reducir la incidencia de estos delitos en la comunidad:

1. Programa de Educación Digital Intergeneracional: Implementar un programa educativo que involucre a todas las generaciones, con especial énfasis en los adultos mayores, quienes se han mostrado más vulnerables a las estafas. Este

programa incluiría talleres prácticos sobre seguridad en línea, reconocimiento de estafas y uso seguro de plataformas financieras digitales. Se fomentaría la participación de jóvenes como mentores digitales para los adultos mayores, creando así un vínculo intergeneracional y aprovechando las habilidades tecnológicas de las generaciones más jóvenes.

2. Colaboración Público-Privada para la Seguridad Digital: Establecer una alianza estratégica entre el gobierno local, las instituciones financieras y las empresas de tecnología para desarrollar un enfoque integral de seguridad cibernética. Esta colaboración podría incluir la creación de un centro de respuesta rápida a incidentes cibernéticos, donde los ciudadanos puedan reportar y recibir asistencia inmediata en caso de sospecha de estafa.

3. Campaña de Concientización "Coronel Suárez Seguro en Línea": Lanzar una campaña de comunicación masiva utilizando medios locales, redes sociales y espacios públicos para educar a la población sobre los riesgos de las estafas informáticas. Esta campaña incluiría información actualizada sobre las tácticas más recientes utilizadas por los estafadores y consejos prácticos para la prevención.

4. Implementación de un Sistema de Alerta Temprana: Desarrollar un sistema de alerta que notifique a los ciudadanos sobre nuevas modalidades de estafas detectadas en la región. Este sistema podría utilizar mensajes de texto, aplicaciones móviles y anuncios en medios locales para mantener a la comunidad informada y alerta.

5. Programa de Certificación en Seguridad Digital para Comercios: Crear un programa de certificación para negocios locales que demuestren buenas prácticas en seguridad cibernética. Esto no solo mejoraría la seguridad general, sino que también fomentaría la confianza de los consumidores en las transacciones digitales locales.

6. Unidad Especializada en Ciberdelitos: Proponer la creación de una unidad policial especializada en ciberdelitos a nivel local, con personal capacitado en investigación digital y forense. Esta unidad trabajaría en estrecha colaboración con las autoridades nacionales y proporcionaría una respuesta más efectiva y rápida a los incidentes de estafas informáticas.

7. Línea de Ayuda y Asesoramiento 24/7: Establecer una línea telefónica y un chat en línea disponibles las 24 horas para brindar asesoramiento inmediato a los ciudadanos que sospechen ser víctimas de estafas o que necesiten verificar la legitimidad de una transacción o comunicación.

8. Programa de Rehabilitación Financiera para Víctimas: Desarrollar un programa de apoyo para las víctimas de estafas informáticas que incluya asesoramiento legal, apoyo psicológico y asistencia en la recuperación financiera. Este programa podría trabajar en conjunto con instituciones financieras locales para explorar opciones de compensación o planes de pago flexibles para las víctimas.

9. Foro Anual de Seguridad Cibernética: Organizar un evento anual que reúna a expertos en seguridad, representantes de instituciones financieras, autoridades locales y ciudadanos para discutir las últimas tendencias en ciberdelincuencia y compartir mejores prácticas en seguridad digital.

10. Integración de la Seguridad Digital en el Currículo Escolar: Trabajar con las instituciones educativas locales para incorporar módulos de seguridad cibernética en el currículo escolar desde la primaria hasta la secundaria, asegurando que las generaciones más jóvenes estén bien equipadas para navegar de manera segura en el mundo digital.

Bibliografía

CETyS, Universidad de San Andrés. (2022). Informe sobre Ciberdelitos en Argentina. Buenos Aires: CETyS.

Clarke, R. V. (2016). Situational Crime Prevention: Theory and Practice. New York: Harrow and Heston.

Córdoba, J. (2020). Delitos Informáticos en Argentina: Tipologías y Estrategias de Prevención. Editorial Universidad Nacional de Córdoba.

De Maio, S. (2019). Criminología y Delitos Informáticos: Un Enfoque Integrador. Buenos Aires: Editorial Del Sur.

García, M. (2022). Impacto de las Estafas Informáticas en Pequeñas Comunidades: El Caso de Coronel Suárez. Revista de Seguridad Ciudadana, 18(2), 45-62.

Garrido, V. (2021). Ciberdelincuencia: Estrategias y Prevención. Editorial Jurídica Argentina.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. P. (2014). Metodología de la Investigación (6ª ed.). McGraw-Hill.

López, J., & Martínez, R. (2020). Seguridad Informática: Teoría y Práctica. Buenos Aires: Ediciones Técnicas.

Ministerio de Seguridad de la Nación. (2022). Informe Anual sobre Delitos Informáticos en Argentina. Buenos Aires: Ministerio de Seguridad.

Pérez, L., & Alonso, R. (2021). Estafas Informáticas: Métodos y Prevención. Revista Argentina de Criminología, 19(1), 67-89.

Sánchez, M. (2020). Legislación y Delitos Informáticos en Argentina. Revista de Derecho Informático, 25(3), 120-138.

Universidad Nacional del Sur. (2021). Delitos Informáticos en Pequeñas Ciudades: Un Estudio de Caso. Bahía Blanca: Universidad Nacional del Sur.