

VERSION PRELIMINAR  
SUSCEPTIBLE DE CORRECCION  
UNA VEZ CONFRONTADO  
CON EL EXPEDIENTE ORIGINAL

DIRECCION GENERAL DE EMISIONES

DIRECCION GENERAL DE EMISIONES

(S-2285/2020)

## PROYECTO DE COMUNICACIÓN

El Senado de la Nación

En el marco de la emergencia generada por el virus COVID-19 y a consecuencia del establecimiento de la cuarentena obligatoria y de los requerimientos de distanciamiento social que ella implica, se trasladaron muchas de las prácticas laborales, sociales, comerciales y bancarias al mundo virtual, con un gran aumento de todas las operaciones online, produciéndose como consecuencia y de acuerdo a los indicadores de las estadísticas oficiales según datos de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) de la Procuración, un incremento del 50% de las causas por delitos cibernéticos durante el aislamiento obligatorio.

En atención a ello, solicita que el Poder Ejecutivo Nacional, a través del Banco Central de la República Argentina y demás organismos competentes, a la brevedad arbitre los mecanismos de seguridad avanzada y estrategias necesarias para garantizar la máxima seguridad en sus operaciones virtuales a todos los usuarios del sistema financiero regulados o no por el BCRA, Fintechs, prestadores de servicios, operadores de redes, tanto en el ámbito bancario como del comercio electrónico en general, entre otros, para lo cual es vital que el Estado disponga de una planificación que garantice seguridad ante todos los nuevos riesgos asociados a la actual expansión digital.

Víctor Zimmermann.- Pablo D. Blanco.- Alfredo L. De Angeli.- María B. Tapia.- Laura E. Rodríguez Machado.- Humberto L. A. Schiavoni.- Juan C. Marino.- Mario R. Fiad.- Claudio J. Poggi.- Silvia B. Elías de Pérez.- Stella M. Olalla.- Silvia del Rosario Giacoppo.- Néstor P. Brillard Pocard.- Oscar A. Castillo.-

## FUNDAMENTOS

Señora Presidente:

En este tiempo de pandemia, muchas modalidades sociales han cambiado, las reuniones sociales se hacen por videollamada, se generalizó la modalidad de trabajo home office, ante el cierre de los centros comerciales y shoppings el comercio de productos a través de Internet tuvo un crecimiento nunca antes visto

A pesar de la crisis, las ventas en línea en Argentina crecieron por encima de la inflación. De acuerdo al último reporte de la Cámara Argentina de Comercio Electrónico (CACE), en 2019 las compras

realizadas a través de la vía digital sumaron \$ 403.278 millones, un 76% más que 2018.

La facturación correspondió a la comercialización de 146 millones de productos, un 22% más que el año anterior. Asimismo, la CACE contabilizó 89 millones de compras, un 12% interanual.

La llegada de la tecnología cambió nuestras costumbres y en la actualidad no es necesario ir a la ventanilla del banco para realizar trámites. Hoy se ejecutan a través del homebanking, cajeros automáticos y líneas telefónicas. Además los bancos también realizan ofrecimientos de préstamos a través de llamados telefónicos, lo que dificulta el reconocimiento de la veracidad de la llamada.

La complejización de los métodos bancarios afecta principalmente a los adultos mayores, y también a ciudadanos de todas las edades, que muchas veces otorgan los números de sus tarjetas ante requerimientos que suponen de buena fe.

Esto también debe exigir al banco extremar las medidas de seguridad del sistema, evitando la vulnerabilidad del mismo, garantizando que quien lo opera es el titular de la cuenta bancaria a la que accede.

Los mismos criterios deberán ser aplicables a todo el sistema financiero regulado o no por el BCRA, Fintechs, prestadores de servicios, operadores de redes, tanto en el ámbito bancario como del comercio electrónico en general, entre otros.

Algunas organizaciones delictivas están utilizando la pandemia de Covid-19 para cometer delitos. Con distintos engaños, buscan obtener números de cuentas y contraseñas como también manipular a sus eventuales víctimas para que realicen pagos y transferencias por supuestos beneficios, premios o donaciones.

Las estafas las realizan a través de diversos canales de comunicación: correos electrónicos, llamadas telefónicas, mensajes de WhatsApp y de texto o a través de redes sociales como Facebook o Instagram.

Las víctimas en su mayoría suelen ser jubilados, pensionados, personas con problemas económicos o sin acceso al crédito bancario.

Los tipos de fraude informático más utilizados son los siguientes:

**10**  
**Métodos más comunes de Fraude Informático**

- 1 PHARMING**  
Redirecciona al usuario a una URL fraudulenta, robando contraseñas e información personal importante.
- 2 SPYWARE**  
Es un programa espía que de manera silenciosa se instala en el ordenador y roba información personal del usuario.
- 3 TROYANO**  
Instrucciones ocultas en un programa "confiable" que causa efectos nocivos.
- 4 VISHING**  
Hace relación a un fraude telefónico. El usuario proporciona información personal o confidencial a través de una llamada.
- 5 MASCARADA**  
Consiste en enviar muchos correos a un router, impidiendo el acceso al servicio y saturándolo, con el objetivo de intervenir la página mientras está fuera de servicio.
- 6 PHISHING**  
Consiste en enviar correos electrónicos falsos, robando contraseñas, datos bancarios e información confidencial.
- 7 SPOOFING**  
Esta modalidad se enfoca en suplantar la identidad de otra persona y/o empresa para sustraer información.
- 8 CABALLO DE TROYA**  
Es un programa que posibilita a otra el acceso a un PC, permitiendo ver, copiar y borrar archivos.
- 9 WORM**  
Programa que se replica instalando copias de sí mismo en el equipo a través de una red.
- 10 EAVESDROPPING**  
Modalidad que obtiene información confidencial sin que el usuario se percate, mediante un monitoreo de radiaciones electromagnéticas.

AUDITOOL

Las estadísticas oficiales ya lo reflejan. Según datos de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) de la Procuración, que conduce el fiscal Horacio Azzolín, las causas por delitos cibernéticos aumentaron un 50% durante el aislamiento obligatorio.

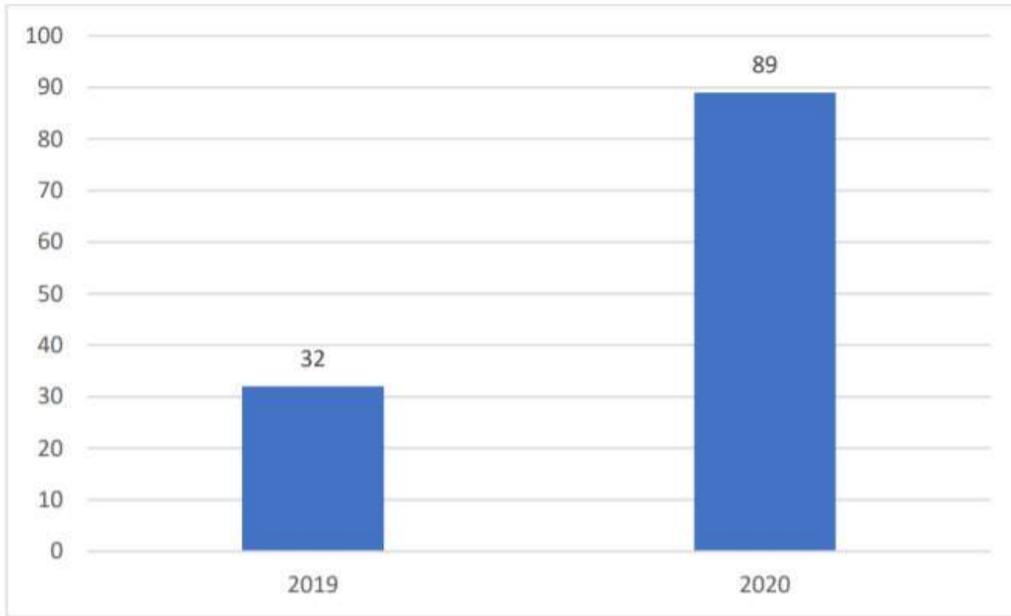
De acuerdo a información estadística de la AALCC (Asociación Argentina de Lucha contra el Cibercrimen), podemos ver en el siguiente gráfico el crecimiento comparativo del cibercrimen 2016-2020 para el mismo período desde marzo a julio:



Dice AALCC respecto del Fraude: se observa un considerable incremento de esta modalidad delictiva a partir del segundo semestre de 2019 incrementándose con la cuarentena iniciada en marzo de 2020. En comparativa primer semestre de 2019 y primer semestre de 2020 se observa un incremento de casi un 72%. Representa el 16,56% de las consultas recibidas durante la cuarentena pudiendo incrementarse un 12,45% en los casos de phishing utilizado para extraer datos y luego cometer fraude.



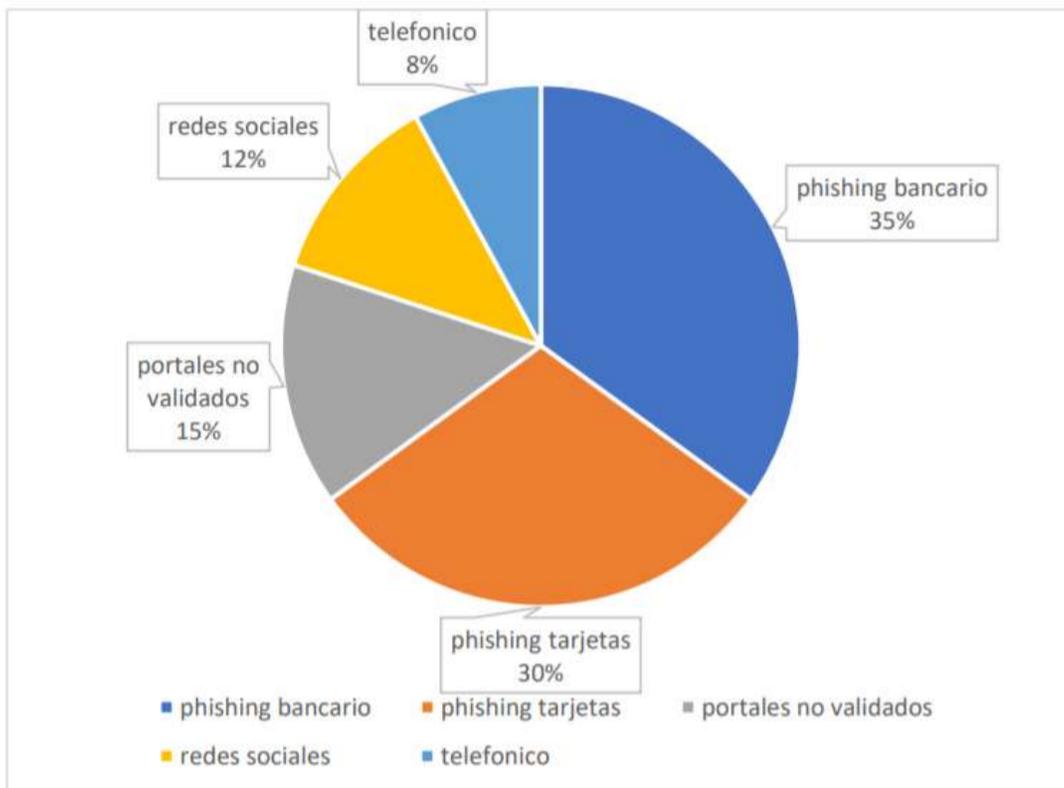
Comparativa entre los periodos 1/3 – 1/7/2019 y 1/3 al 1/7/2020



En la coparativa se observa un incremento de este tipo de delitos superio al 110%

Metodologías :

- Phishing bancario
- Phishing con tarjeta de crédito
- Compras en portales no validados
- Compras a través redes sociales
- Compras / validaciones de datos telefónicas



Debemos tener claro que el fraude no solo se produce por impericia del usuario, sino también por las vulnerabilidades de seguridad que poseen las bases de datos de las entidades bancarias o empresas, falencias tanto en el software como en el hardware, ya que además de los métodos de fraude por engaño del usuario también es habitual el hackeo de servidores, con el consecuente robo de números de cuentas y de tarjetas de crédito con sus claves.

A este respecto, la información disponible en los medios periodísticos indica que en 2016 el promedio mundial era de 54 cajeros automáticos cada 100.000 habitantes, un 44% de la población global cuenta con tarjeta de débito, según estadísticas del Banco Mundial. Esta proliferación de equipos disponibles de acceso público atrae a las organizaciones delictivas que se dedican a los fraudes bancarios.

Además, casi todos los cajeros automáticos son PC que usan versiones muy antiguas de sistemas operativos, algunas, incluso, Windows XP. Según especialistas de Kaspersky Lab una de las más conocidas empresas globales de seguridad informática, esto los hace vulnerables a todo tipo de ataques.

"La gran mayoría del hardware de los cajeros automáticos son viejos y no soportarían la instalación de un sistema operativo nuevo y más seguro", explicó a LA NACIÓN Fabio Assolini, analista de seguridad senior de Kaspersky Lab. Los bancos aún usan sistemas operativos que ya no cuentan con el soporte técnico de su fabricante, Microsoft.

"Estos sistemas discontinuados son utilizados de manera masiva y están llenos de vulnerabilidades, lo que facilita el trabajo de los criminales", continuó Assolini. Otro problema que detalla es el fácil acceso que tienen los cibercriminales a los puertos USB, cables y otras entradas de las máquinas detrás de los cajeros para llevar a cabo un ataque.

Los casos más habituales son aquellos en los que el reclamo del usuario proviene de algún tipo de fraude de terceros en el que se han empleado virus, troyanos o técnicas de phishing o ingeniería social, para tomar el control de los equipos y los terminales del usuario y hacer uso de sus instrumentos de pago para realizar transferencias, solicitudes de créditos o compras.

Ante esta realidad surge la necesidad de implementar medidas de seguridad avanzada, establecer una obligación para las entidades de hacer más en este ámbito, en la medida en que disponen de mayor capacidad para implementar mejores medios de seguridad y control. Entre estas acciones adicionales, las entidades pueden y deberían mejorar todas sus estrategias y acciones tendientes a disponer de mecanismos de seguridad avanzada para eliminar los riesgos y

garantizar la máxima seguridad en sus operaciones virtuales a todos los usuarios del sistema.

Es por ello que creo muy importante adoptar medidas como las que estoy proponiendo ut supra a los efectos de sostener y acompañar de la mejor manera a nuestra población en los nuevos desafíos de vida que nos ha planteado esta nueva forma de desarrollar nuestras actividades por imperio de la pandemia, que aceleró cambios que ya venía transitando la sociedad pero en forma más lenta de la que las circunstancias del COVID-19 lo exigieron.

Por los fundamentos expuestos, solicito a mis pares en este H. Senado de la Nación, acompañen con su voto la aprobación del presente Proyecto de Comunicación.

Víctor Zimmermann.- Pablo D. Blanco.- Alfredo L. De Angeli.- María B. Tapia.- Laura E. Rodríguez Machado.- Humberto L. A. Schiavoni.- Juan C. Marino.- Mario R. Fiad.- Claudio J. Poggi.- Silvia B. Elías de Pérez.- Stella M. Olalla.- Silvia del Rosario Giacoppo.- Néstor P. Brillard Pocard.- Oscar A. Castillo.-

DIRECCION GENERAL DE PUBLICACIONES