República Argentina - Poder Ejecutivo Nacional

Informe

Número: IF-2026-09674756-APN-DCYAC#MSG

CIUDAD DE BUENOS AIRES
Martes 27 de Enero de 2026

Referencia: ANEXO - PLAN FEDERAL DE LUCHA CONTRA EL FRAUDE CIBERASISTIDO (2026 - 2027)

PLAN FEDERAL DE LUCHA CONTRA EL FRAUDE CIBERASISTIDO (2026 - 2027)

Introducción

La era digital en la que nos encontramos inmersos y el avenimiento de una sociedad cada vez más informatizada transformó la manera en que nos comunicamos, realizamos transacciones y accedemos a diferentes bienes y servicios. Sin embargo, este avance también dio lugar a nuevas formas de fraude en las que los ciberdelincuentes utilizan herramientas digitales y técnicas de ingeniería social para engañar a individuos, empresas e instituciones. Los fraudes ciberasistidos crecieron de manera exponencial en los últimos años aprovechando la masificación del acceso a Internet, el uso de redes sociales, la digitalización del comercio y la proliferación de dispositivos conectados.

Las modalidades de fraude ciberasistido son diversas y en constante evolución. Desde el *phishing* y las estafas bancarias hasta los fraudes con criptomonedas y la suplantación de identidad, los delincuentes emplean sofisticadas estrategias para manipular a sus víctimas y obtener información sensible o beneficios económicos. La globalización del ciberdelito y la dificultad para rastrear a los responsables plantean un desafío significativo para la prevención y persecución de este tipo de organizaciones criminales.

En este contexto, el **Plan Federal de Lucha contra el Fraude Ciberasistido** surge como una respuesta integral para fortalecer la capacidad del Estado contra este fenómeno. Esta iniciativa tiene como objetivo mejorar la prevención, detección y mitigación de estos delitos mediante una estrategia holística que integre la cooperación interinstitucional, el desarrollo de normativas actualizadas, el uso de tecnologías avanzadas y, principalmente, la concientización de la ciudadanía.

La prevención es un pilar fundamental en la estrategia de seguridad digital. Por ello, este plan contempla campañas de educación para reducir la vulnerabilidad de la población, así como el fortalecimiento de los canales de denuncia y asistencia a las víctimas. Además, fomenta la colaboración entre el sector público, el sector

financiero, el sector académico y las empresas tecnológicas con el fin de establecer mecanismos efectivos para la identificación temprana de amenazas y la respuesta rápida ante incidentes.

En un mundo cada vez más interconectado, la lucha contra los fraudes ciberasistidos debe ser una prioridad que permita garantizar un entorno digital seguro, confiable y resiliente que no solo proteja los derechos de los ciudadanos, sino que también contribuya a la estabilidad económica y la confianza en el ecosistema digital.

El éxito en la lucha contra el fraude ciberasistido depende de la colaboración y el compromiso de múltiples partes interesadas, entre ellas el sector público y privado, el sector académico, la sociedad civil y los usuarios individuales. Sólo a través de un esfuerzo coordinado y sostenido se podrá mitigar el impacto de estos delitos y construir un ciberespacio más seguro para todos.

Estado de situación

En la actualidad, el Ministerio de Seguridad Nacional por intermedio de la Dirección de Ciberdelito y Asuntos Cibernéticos diseña y lleva adelante la coordinación del esfuerzo nacional de policía en materia de lucha contra el ciberdelito y las amenazas cibernéticas a través del diseño y elaboración de las políticas y programas de fortalecimiento, de las fuerzas policiales y de seguridad federales para la investigación y el abordaje de la ciberdelincuencia en el territorio nacional tramitando las diferentes denuncias recepcionadas y asistencia a las víctimas.

En tal sentido, es necesario redoblar los esfuerzos de prevención, detección y respuesta ante el fraude ciberasistido, actividad criminal que se posicionó como una de las principales amenazas en el ciberespacio, situación que requiere un abordaje integral y prioritario mediante el diseño e implementación de un plan estratégico de lucha contra este fenómeno criminal.

Objetivos

Dada la ingente necesidad de llevar a cabo diferentes acciones altamente especializadas en materia de lucha contra la ciberdelincuencia, resulta oportuno contar con un **Plan Federal de Lucha contra el Fraude Ciberasistido** cuyo marco metodológico, diseño e implementación se encuentra alineado con el “Plan Federal de Prevención de Ciberdelitos y Gestión Estratégica de la Ciberseguridad (2025 - 2027)” aprobado mediante Resolución N° 72/25 y el “Programa de Fortalecimiento en Ciberseguridad e Investigación del Ciberdelito (ForCIC)” aprobado mediante Resolución N° 19/25, ambas del registro del Ministerio de Seguridad Nacional.

Objetivo general

Establecer los ejes rectores, medidas y acciones específicas mediante un marco metodológico que permita realizar un abordaje integral de los fraudes ciberasistidos como fenómeno criminal, protegiendo los derechos y garantías reconocidos en la normativa vigente para los habitantes de la República Argentina y promoviendo un ciberespacio seguro, confiable y resiliente para todos.

Objetivos específicos

1. Prevención

a. **Concientización**
   1. Diseñar piezas gráficas y audiovisuales para difusión de las principales amenazas y tendencias identificadas
   2. Desplegar campañas de sensibilización en medios de comunicación (televisión, radios, diarios, entre otros)
   3. Difusión de los diferentes canales para recepcionar denuncias

b. **Educación**
   1. Brindar charlas formativas en espacios educativos de diferentes niveles y público en general (instituciones escolares, universitarias y centros de la tercera edad, entre otros)
   2. Participar en eventos formativos de diferentes instituciones educativas y organizaciones no gubernamentales especializadas en educación digital

c. **Desarrollo de marco normativo**
   1. Contribuir al desarrollo, diseño y redacción de normativa específica nacional y provincial
   2. Participar en foros nacionales e internacionales para contribuir de la generación de normativa específica

d. **Vinculación con organismos reguladores**
   1. Participar en mesas de trabajo con organismos reguladores de plataformas utilizadas para el fraude ciberasistido
   2. Acompañar en la implementación de requisitos mínimos normativos elaborados por los organismos reguladores

e. **Anticipación de fraudes masivos mediante esquemas piramidales**
   1. Generar alertas tempranas a la población ante la posible detección de esta modalidad de fraudes masivos
   2. Articular acciones con otros organismos a fin de investigar este tipo de actividades ilegales

2. Detección

a. **Canalización de denuncias**
   1. Actualizar los formularios de denuncias con el objetivo de maximizar la eficiencia del flujo de las denuncias recepcionadas a través de la línea 134, correo electrónico o formulario web
   2. Generar constancias de denuncia a fin de emitir el comprobante pertinente

b. **Análisis estadístico**
   1. Identificar patrones delictivos y campañas maliciosas por medio del análisis de la información proporcionada por las víctimas mediante las denuncias realizadas y otras fuentes de información
   2. Generar estadísticas y métricas que permitan capitalizar la información proporcionada por las víctimas mediante las denuncias realizadas y otras fuentes de información

c. **Procesos de detección proactiva del fraude ciberasistido**
   1. Gestionar proactivamente los indicadores de riesgo (IOR) e indicadores de ataque (IOA) detectados
   2. Proponer metodologías que permitan realizar la prevención del delito en entornos cibernéticos

d. **Capacitación a las Fuerzas Policiales y de Seguridad Federales**
   1. Diseñar capacitaciones específicas en fraudes ciberasistidos para las fuerzas policiales y de

seguridad federales
2. Promover la realización de actividades educativas conjuntas con áreas de prevención de fraudes de otros organismos del sector público y privado

e. **Coordinación con otros canales de denuncias**
1. Promover el intercambio de información estadística con otros canales de denuncias pertenecientes al Poder Judicial, Ministerio Público Fiscal, policías provinciales y de la Ciudad Autónoma de Buenos Aires
2. Establecer puntos de contacto para compartir alertas y reportes sobre nuevas modalidades delictivas en la materia

3. Respuesta

a. **Gestión de las denuncias línea 134, mail y formulario**
1. Optimizar el proceso de gestión de las denuncias con un enfoque basado en procesos
2. Articular con las fuerzas policiales y de seguridad federales el proceso de tramitación de denuncias recepcionadas

b. **Detención de transacciones indebidas**
1. Articular acciones con los entes encargados de gestionar los registros de claves bancarias uniformes (CBU) y claves virtuales uniformes (CVU) utilizadas ilícitamente para su bloqueo o congelamiento
2. Evaluar los mecanismos centralizados de reportes de CBU y CVU utilizadas ilícitamente para su bloqueo o congelamiento
3. Participar en la elaboración de mecanismos de bloqueos dinámicos de transacciones ilícitas de forma conjunta con el sector privado

c. **Proceso de respuesta del fraude Ciberasistido**
1. Gestionar el tratamiento de los indicadores de compromiso (IOC) detectados
2. Realizar el análisis del modelado de amenazas e identificar puntos de compromiso y vulnerabilidades desde lo social, tecnológico y análisis de procesos

d. **Articulación con el sector privado**
1. Generar mecanismos de colaboración permanente con el sector financiero tradicional con incidencia en la materia
2. Promover mecanismos de colaboración permanente con el sector financiero digital con incidencia en la materia
3. Promover mecanismos de colaboración permanente con proveedores de activos virtuales con incidencia en la materia
4. Fomentar mecanismos de colaboración permanente con aplicaciones informáticas establecidas en la Argentina

e. **Fortalecimiento de las capacidades de las Fuerzas Policiales y de Seguridad Federales, de las provincias y de la Ciudad Autónoma de Buenos Aires**
1. Promover el fortalecimiento y construcción de capacidades del personal que integra el Centro de Sinergia Cibernética de las Fuerzas Policiales y de Seguridad Federales (CS5)
2. Articular la derivación de denuncias recibidas a las jurisdicciones provinciales o Ciudad Autónoma de Buenos Aires mediante la red 24/7 del Programa de Fortalecimiento en Ciberseguridad e Investigación del Ciberdelito (ForCIC)

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2026.01.27 17:06:42 -03:00

Santiago Gonzalez Bellengeri
Director
Dirección de Ciberdelito y Asuntos Cibernéticos
Ministerio de Seguridad Nacional

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2026.01.27 17:06:43 -03:00