Olimpiada Internacional de Seguridad Financiera

El lado oscuro de la IA

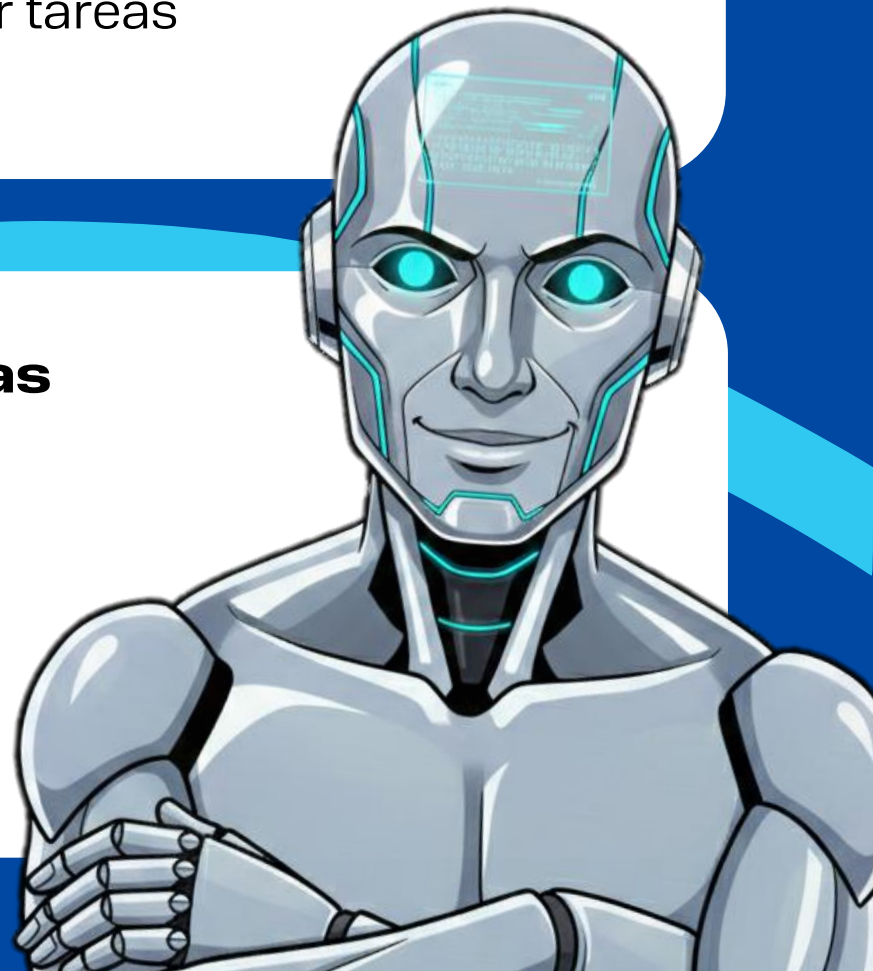
#Inteligencia artificial

Inteligencia artificial (IA)
Artificial intelligence

sistemas informáticos capaces de realizar tareas típicas de la inteligencia humana

La IA es una tecnología que permite a los sistemas

- Comprender consultas formuladas en lenguaje natural
- Analizar, procesar y encontrar datos relevantes
- Reconocer imágenes, símbolos y patrones
- Aprender de grandes flujos de datos
- Tomar decisiones y adaptarse a diferentes condiciones



¿Dónde se utiliza la IA?

Medicina y atención médica

- Tratamientos personalizados
- Desarrollo de fármacos
- Análisis de datos

Banca

- Inversiones automáticas
- Calificación crediticia y evaluación de riesgos
- Toma de decisiones rápida

Educación

- Adaptación del material al estudiante
- Identificación de lagunas de conocimiento
- Desarrollo de tareas de refuerzo

Ciencias

- Búsqueda rápida de patrones
- Aceleración de investigaciones
- Búsqueda de soluciones basada en el análisis

Protección de la ciberseguridad

Cómo la IA combate el fraude

- Detecta e intercepta esquemas fraudulentos
- Reduce la carga de las víctimas reales

Ejemplo: “Ciberabuela”, un modelo de operador móvil basado en la IA

- Se comunica con estafadores en nombre de un cliente mayor
- Distrae a los estafadores de las personas reales, desperdiciando su tiempo y recursos

El lado oscuro de la IA

Amenazas financieras

- Aumento del fraude cibernético mediante IA
- Robo de fondos y datos
- Automatización de esquemas delictivos

Zonas de riesgo especial

- Aumento del número de menores afectados
- Ataques telefónicos y de mensajes de texto (escuelas, agencias gubernamentales, operadores móviles)
- Fraude relacionado con cuentas de juegos de azar y la Certificación estatal

Operaciones sin el consentimiento del cliente

27,5
mil mill. de rublos
2024

21
mil mill. de rublos
9 meses de 2025

Robos evitados

222
mil mill. de rublos
noviembre de 2025

Oposición

- Servicio Federal de Monitoreo Financiero (Rosfinmonitoring)
- Servicio de Inteligencia Financiera de los países de la CEI
- Grupo Euroasiático sobre ALA/CFT

Blanqueo de capitales

Ciberfraude

Cuentas ficticias

transferencias múltiples, mezcla de fondos

Ofuscación de flujos financieros

Criptoplataformas

Legalización/financiación de actividades delictivas

La amenaza tiene carácter transnacional

¿Qué es una mula de dinero?

Mula de dinero (mula bancaria)

es una persona que utiliza sus tarjetas para retirar o transferir (enviar posteriormente) fondos robados.

Reclutamiento de jóvenes

A quiénes reclutan

- adolescentes a partir de 14 años
- estudiantes y escolares
- personas desempleadas

Más de 1 millón de mulas

La escala del problema en Rusia

según el Banco de Rusia

Cómo reclutan (trucos psicológicos):

- **urgencia:** “solo hoy”
- **simplicidad:** “hasta un escolar puede con ello”
- **seguridad:** “es completamente legal"
- **gradualidad:** desde pequeñas sumas hasta grandes
- **prueba social:** “cientos de personas ya están trabajando con nosotros”

Responsabilidad

Responsabilidad penal directa

se establece en la modificación del artículo 187 del Código Penal de la Federación de Rusia.

Sanciones penales

- Hasta **3 años** de prisión por transmitir datos bancarios
- Hasta **6 años** de prisión para los organizadores (reclutadores de mulas)

Práctica de aplicación

- En 2025, se abrió la primera causa penal contra un reclutador de mulas
- La cooperación con el Ministerio del Interior es motivo de exención de responsabilidad
- El organizador fue identificado con base en el testimonio del reclutador de mulas detenido

“Deepfakes”: una nueva amenaza

“Deepfake”

(en inglés “falsificación profunda”)

es un video, audio o foto creado por inteligencia artificial que muestra a una persona haciendo o diciendo algo que nunca ocurrió en la vida real

Cómo funciona

- Llamadas camufladas como encuestas y grabaciones de voz
- IA que copia el rostro y la voz de una persona
- Generación de *deepfakes* de voz

Unos pocos segundos de grabación son suficientes para crear un *deepfake* de voz

El primer caso sonado

2019, Reino Unido

estafadores utilizaron IA para suplantar la voz del CEO de una empresa energética

Esquema del ataque

La “voz del director” llama a un subordinado con una orden urgente de transferir fondos al proveedor

↓

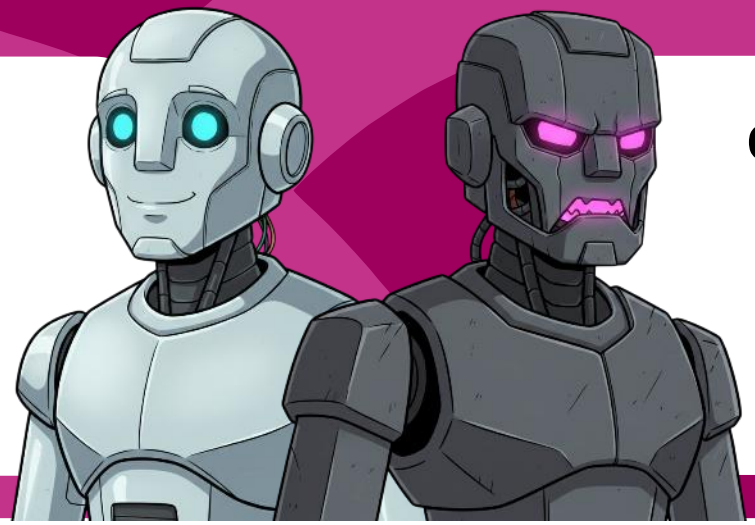
220 000 €

transferidos a la cuenta de los estafadores

Gemelo malvado (“Evil Twin”)

Idea del ataque

una red Wi-Fi falsa
que imita la real



Qué roban

- Nombres de usuarios y contraseñas
- Datos de tarjetas bancarias
- Correspondencia e historial del navegador

Cómo funciona

Clonación de red
mismo SSID, señal más potente

→

Conexión de la víctima
cafeterías, aeropuertos, centros comerciales

→

“Man-in-the-Middle”
interceptación de todo el tráfico

→

“Phishing”
página de inicio de sesión falsa

Gemelo malvado en el aeropuerto

Caso

- La estudiante se conectó a una red Wi-Fi que llevaba el nombre del aeropuerto
- La red era la primera en la lista
- El código resultó ser una contraseña de un solo uso

Errores graves

- Se ignoraron las advertencias sobre red no segura
- Se ingresó el número de teléfono
- Se ingresó el código de *Messenger*

Consecuencias

- Pérdida de acceso al *Messenger*
- Datos personales comprometidos

¡Es importante!

Los códigos de mensajería instantánea nunca se ingresan al registrarse para Wi-Fi

“IA – Phishing”

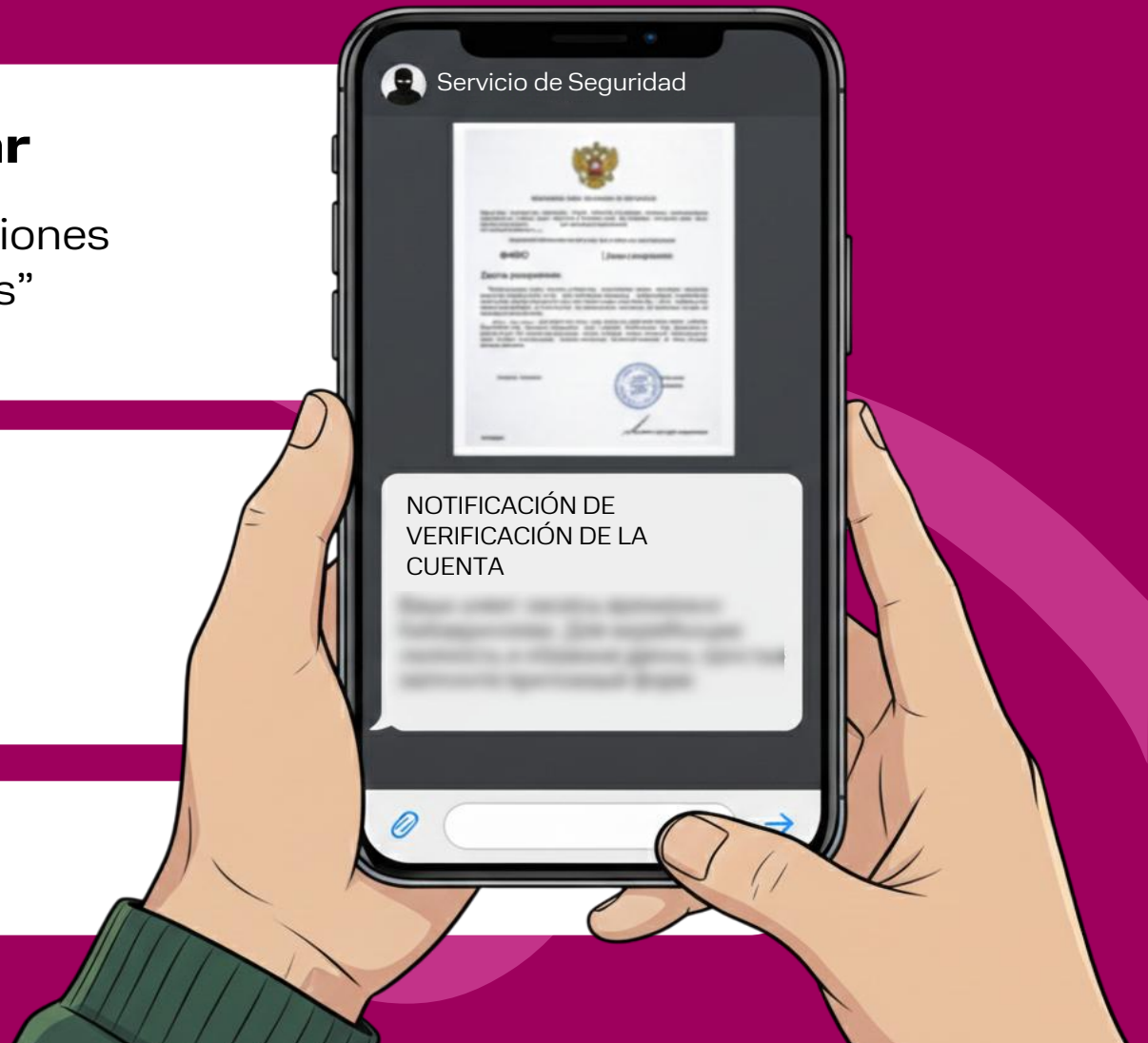
Antes de que la IA empiece a funcionar

- Analiza datos de redes sociales, sitios web y filtraciones
- Genera correos electrónicos y mensajes “perfectos”

Envía un mensaje personal

- Sin errores ni clichés
- Parece una comunicación laboral real

Consecuencia: pérdida de dinero



“Vishing” con IA

“Vishing” con IA

(en inglés: vishing = voice + phishing): phishing de voz

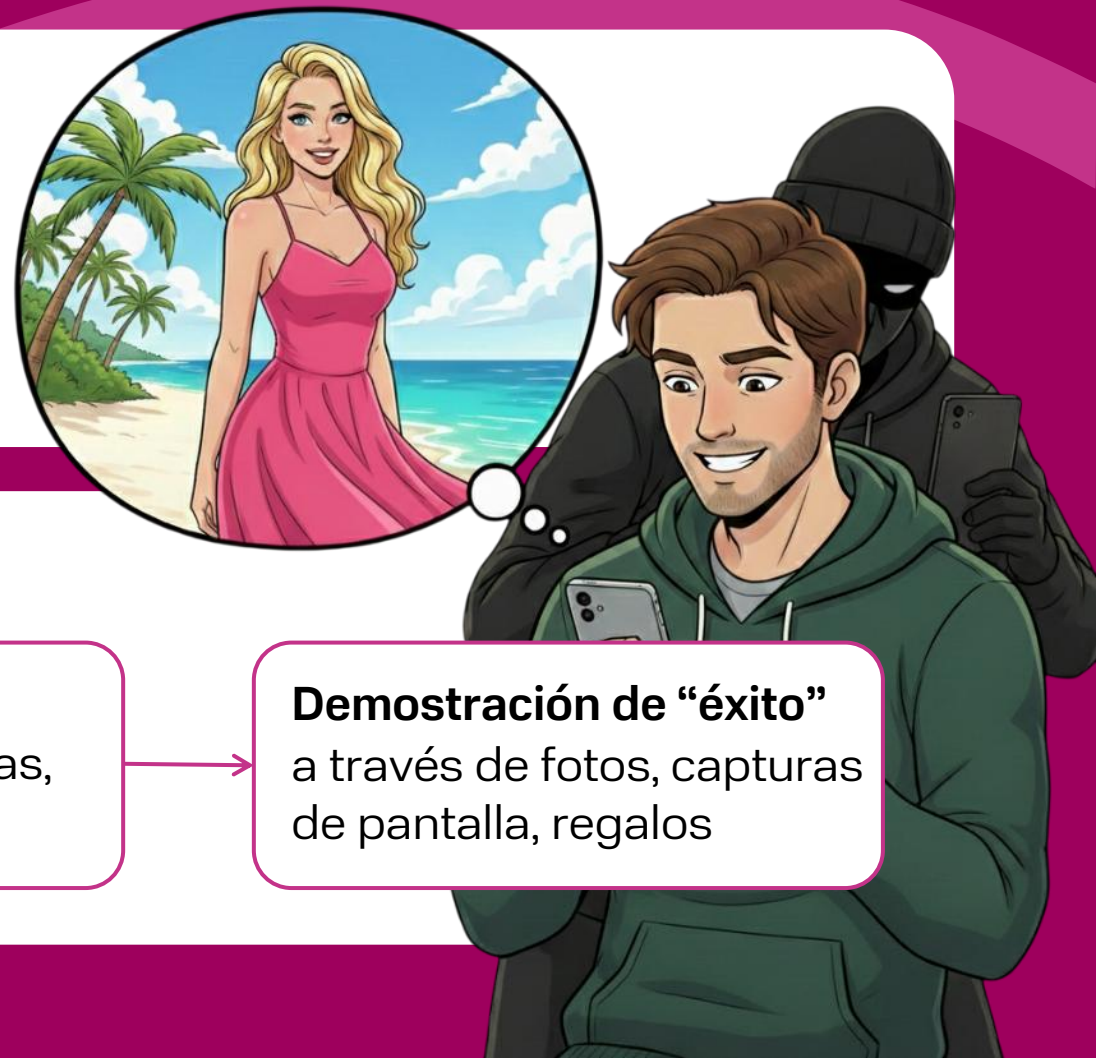
- Una versión de *deepfake* basada en voz
- La IA copia la voz en material de unos segundos de grabación
- Permite dialogar con la víctima

La IA hace que el fraude sea lo más realista posible

Estafas románticas

Idea del ataque

- La IA mantiene conversaciones con miles de personas simultáneamente
- Crea la ilusión de confianza y utiliza datos de redes sociales para personalizar las comunicaciones



Cómo funciona

Conversaciones en chats
preguntas personales, mensajes de voz

→

Llamada a invertir
apuestas, criptomonedas, pirámides financieras

→

Demostración de “éxito”
a través de fotos, capturas de pantalla, regalos

Seguridad de Wi-Fi público

Evitar la conexión a redes Wi-Fi públicas inseguras

“Evil twins” casi siempre están disponibles

Nunca introducir contraseñas y datos de tarjeta

Red Wi-Fi pública intercepta el tráfico

Utilizar únicamente sitios HTTPS

Icono de candado → la conexión está protegida mediante cifrado de extremo a extremo

Prestar atención a las advertencias

Señalan una amenaza real

Habilitar la autenticación multifactor (MFA)

Contraseña + código de un solo uso

Evitar entrar en pánico

Una forma sencilla pero confiable de protegerse de la suplantación de voz por IA

1. **Colgar** en las primeras sospechas
2. **Hacer llamada un familiar o amigo** para verificación
3. **Idear una contraseña familiar** para identificación
4. **Hacer preguntas personales**
   que solo conozcan solo personas cercanas
   (por ejemplo: “¿Cómo se llama nuestro perro?”)

Practicar la higiene digital

Cómo evitar que la IA clone su voz

- **Cerrar el acceso a las redes sociales** (solo para amigos)
- **Evitar compartir copias públicas** de la voz
  (estados en *Messenger*, redes sociales, transmisiones)

Controlar el estado emocional

- Cualquier información que provoca emociones fuertes y requiere una acción inmediata puede ser un engaño
- Hay que hablar de la situación con los seres queridos

La mejor arma es el pensamiento crítico

Ojo: las agencias gubernamentales (el Banco Central de la Federación Rusa, el Servicio Federal de Seguridad y el Servicio Federal de Impuestos) no resuelven “asuntos importantes” por teléfono

Evitar contactos sospechosos

Cómo actuar en el caso de encontrarse con una estafa

- **Cesar la conversación** cuando se mencione dinero, apuestas o criptomonedas
- **Pensar de manera crítica**
- **Bloquear** al estafador
- **No transferir dinero** a alguien que no conozca en persona
- **Si es necesario,** denunciarlo a las autoridades y a la administración de la plataforma

Estafas románticas son un juego de confianza,

y la meta es su dinero

Mulas: intermediarios en planes criminales financieros

Qué es una mula bancaria

- Es una persona que acepta el dinero robado
- Transfiere o retira dinero para los reclutadores de mulas
- Entregan una tarjeta con acceso a la banca *online*

Mulas son parte del delito penal

“Adquisición o transferencia de una tarjeta por personas que no sean clientes del banco”
Por esta infracción, un ciudadano puede ser condenado a penas de prisión de hasta seis años y multado.

Artículo 187 del Código Penal ruso, “Manejo Ilícito de Fondos de Pago”

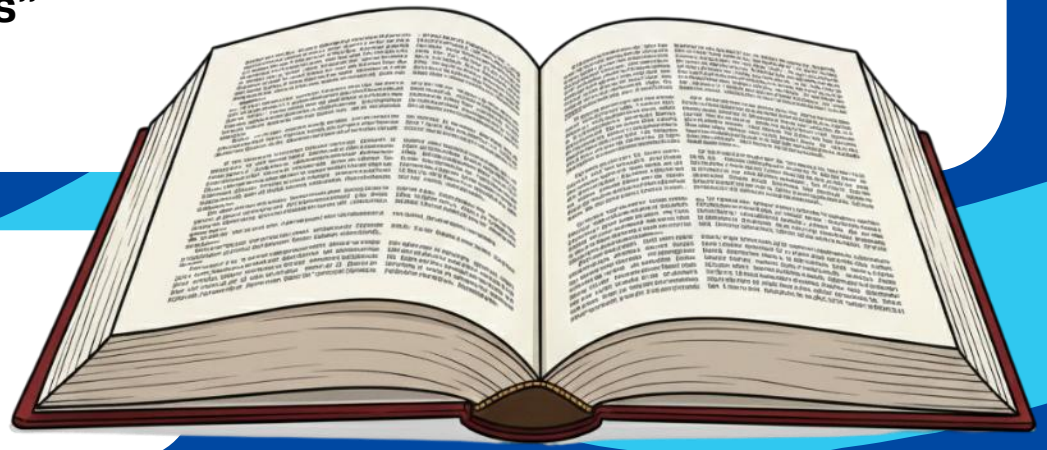
Número de mulas en Rusia

> 1 millón
de clientes mulas bancarias

~ 20 %
adolescentes inconscientes de las consecuencias

Las mulas bancarias son parte importante de la cadena delictiva del blanqueo de capitales

pueden ser procesados en virtud del artículo 174 del Código Penal ruso, **“Legalización (blanqueo) de fondos u otros bienes adquiridos por otras personas mediante medios delictivos”**



Son fundamentales la concienciación y la precaución

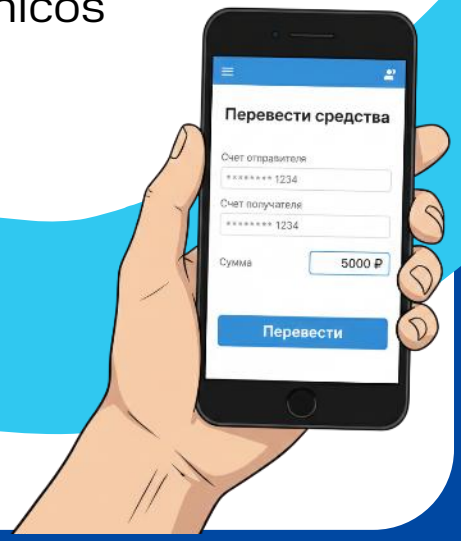
⇆Clasificación de mulas según funciones✕

Ingresadores

- aceptan efectivo →
- lo ingresan en sus cuentas→
- lo transfieren a otros participantes

Transitarios

- reciben transferencias →
- las redirigen a otras cuentas o monederos electrónicos



Sacadores

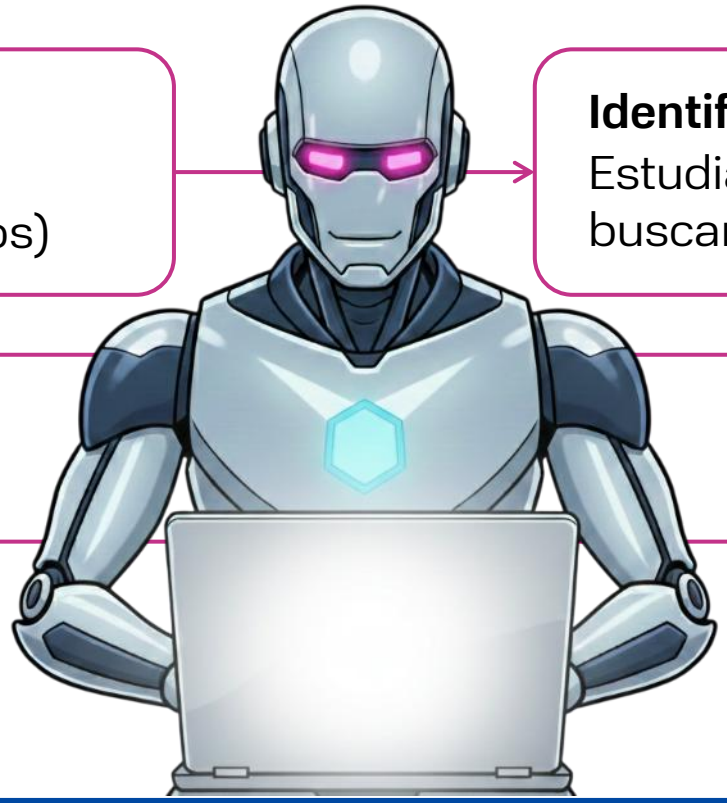
- retiran el dinero en efectivo a través de cajeros automáticos →
- lo entregan a los organizadores

Reclutamiento de mulas con la IA

Cómo funciona

Redes neuronales y el NLP
analizar fuentes abiertas
(redes sociales, foros, mercados)

Identificación de grupos vulnerables
Estudiantes, desempleados, quienes buscan dinero fácil



Evaluación del perfil psicológico
publicaciones, estilo de comunicación → sugestibilidad, avaricia

Contacto inicial
chatbots, uso de avatares *deepfake*

“Trabajo sencillo”

Escenario típico

- No se requiere experiencia ni formación
- Trabajo desde casa, 2-3 horas al día
- Se requiere tarjeta bancaria o banca *online*

Uno se hace mula bancaria y cómplice de un delito sin darse cuenta

“Transferencia errónea”

Cómo funciona

Una transferencia “accidental” la recibe la víctima → **Una llamada pidiendo** un reembolso urgente a la cuenta “correcta” → **Transferencia de dinero** a la cuenta de estafadores

La mejor solución

- Contactar al banco inmediatamente
- Seguir sus instrucciones estrictamente

SMS de: número desconocido
Transferencia entrante: 50 000 rublos

Me equivoqué. Por favor, reenvíeme el dinero a este número

“Administrador de la Lotería”

Cómo reclutan

- Ofrecen un “trabajo técnico”
- Se debe distribuir los premios en efectivo entre los “ganadores”

Qué pasa en realidad

- La persona contratada se hace mula de dinero
- El dinero en la tarjeta es el dinero robado a otras víctimas
- Las transferencias se registran como “ganancias”, pero se dirigen:
  - a otras mulas o testaferros
  - directamente a los estafadores

Papel clave de la mula

- Fragmenta y “depura” el flujo delictivo
- Dificulta el rastreo del plan criminal por parte de los bancos y las fuerzas del orden

Reclutamiento por redes sociales

Cómo encuentran víctimas

- La IA analiza las redes sociales: publicaciones sobre búsquedas de empleo, participación en sorteos
- Se seleccionan personas vulnerables

Coartada típica

- “Administrador de Pagos”
- Asistente de un bloguero o *streamer*
- Voluntario que acepta donaciones

Cómo reclutan

- Se usa una cuenta “activa” con fotos robadas.
- Los mensajes ofrecen un trabajo a tiempo parcial, asistencia o un proyecto “social”
- Se enfatiza la legitimidad del trabajo
- Se solicitan transferencias de dinero a través de una tarjeta personal

Ninguna organización legítima utiliza la tarjeta de una persona al azar

Responsabilidad penal en Rusia

Artículos que establecen sanciones para mulas bancarias

- **Artículo 174 del Código Penal de la Federación Rusa,** “Legalización (blanqueo) de fondos u otros bienes adquiridos por otras personas mediante medios delictivos”
- **Artículo 187** “Circulación ilegal de instrumentos de pago”
- **Artículo 159** “Fraude”

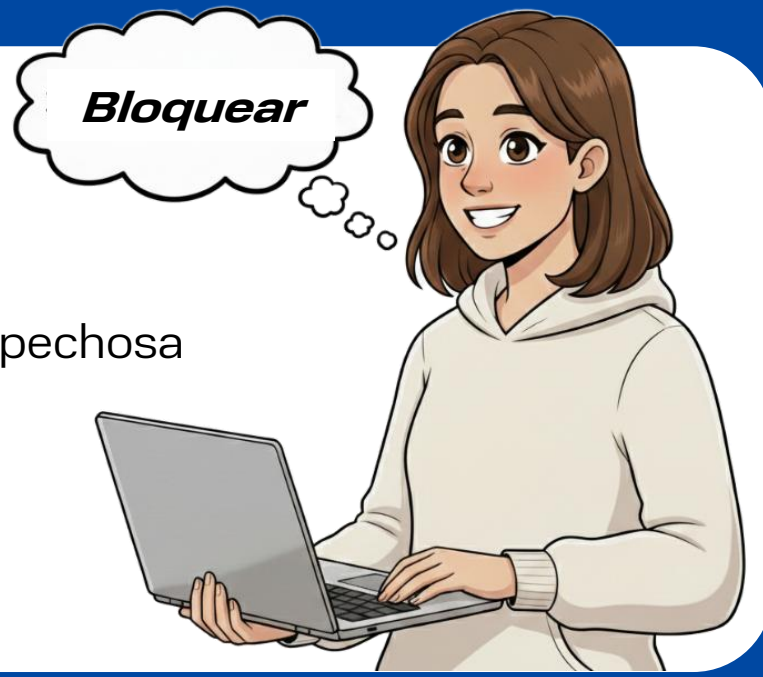
Lo más importante:

- **Ser mula** no es un trabajo sencillo sino **un delito**
- Tanto **los organizadores** como **los participantes** tienen responsabilidad

Normas de seguridad

Si hay signos de reclutamiento de mulas, es necesario:

- Cesar inmediatamente todo contacto con estafadores
- Evitar transferir nada, aunque se recibiera una transferencia sospechosa
- Bloquear la tarjeta y contactar al banco
- Guardar la correspondencia, los datos de los estafadores
- Contactar a las agencias policiales



Todas las ofertas de “dinero fácil” son sospechosas

especialmente si requieren información personal o acceso a tarjetas bancarias

Historia y rasgos característicos

Qué es criptomoneda

- Dinero digital independiente del banco
- Funciona sobre la tecnología *blockchain,* tabla de transacciones descentralizadas

3 de enero de 2009

se generó el primer bloque de la red Bitcoin

Crecimiento fenomenal en valor

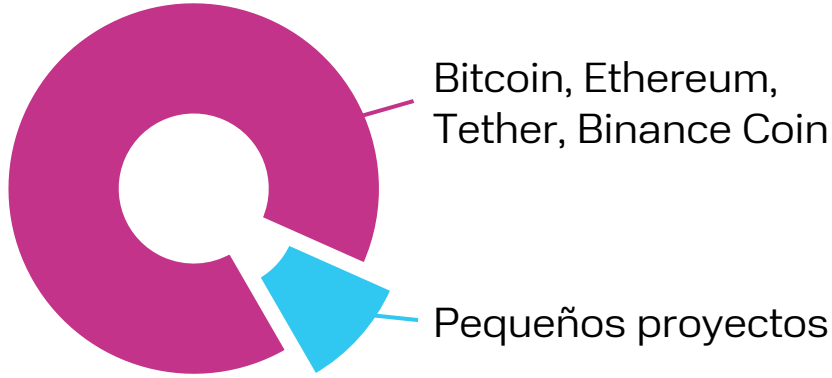
2009 1 ¢

2025 126 200 $

Rendimiento pasado ≠ rendimiento futuro

Principales criptoactivos

año 2026

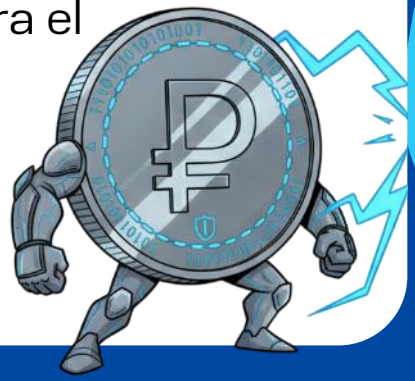


Rublo digital vs Criptomoneda

Rublo digital

- Complementa fondos en efectivo y no monetarios
- Se controla por el Banco Central de la Federación de Rusia, acceso mediante aplicaciones móviles y banca en línea.
- Es obligatorio procedimiento KYC para protegerse contra el fraude y el blanqueo de capitales.

Activo estatal y controlado



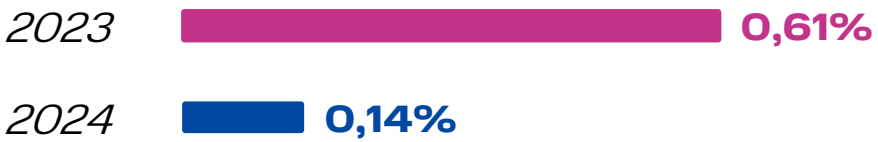
Criptomoneda

- Es descentralizada: sin control estatal ni bancario.
- Se utiliza como activo o propiedad, no siempre es de curso legal.
- Es seudónima: está vinculada a una dirección de billetera pública, lo que supone riesgos de seguridad.

Activo descentralizado con alta volatilidad

Criptomonedas y fraude

Porcentaje de transacciones delictivas



Entidades con indicios de actividad ilícita

Según el Banco Central de la Federación Rusa

3346
enero–junio de 2024

4183
enero–junio de 2025

Usos delictivos

- Drogas, juegos de azar, robo de propiedad intelectual
- Lavado de dinero, esquemas piramidales
- Las criptomonedas son una forma de atraer fondos e inversiones con la promesa de ganancias rápidas

Las criptomonedas son convenientes para los jóvenes

pero son una herramienta para el fraude, ante todo cuando se utiliza IA para su adopción masiva.

Triángulo fraudulento P2P

Cómo funciona

Anuncio falso
Venta a un precio inferior al del mercado

→

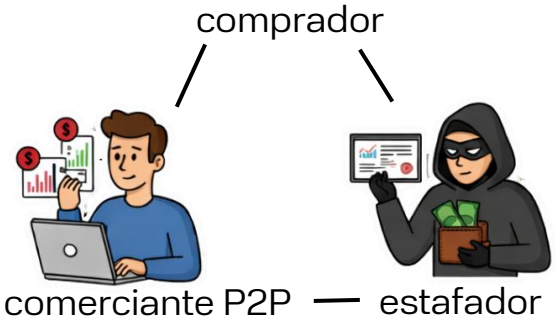
Sustitución de datos
Tarjeta del *trader* P2P, no la del comerciante

→

Transferencia de dinero al *trader*
Compra de criptomonedas a estafadores

Cómo reducir los riesgos

- Consultar las calificaciones y el historial de sus contrapartes
- Elegir métodos de pago populares y verificados
- Vender productos solo a través de plataformas verificadas



Fraude de la criptomoneda SQUID

Qué pasó

- El *token* Squid se prometió para usarse en un juego en línea basado en una popular serie de televisión
- **En 2 días: +44 000 %, precio: 2860 $**
- Cayó a cero al poco tiempo
- **Los estafadores retiraron más de 3 mill. de $,** más de 40 000 inversores afectados

Señales de peligro

- El *token* no se puede vender
- No cotiza en grandes plataformas
- Errores del sitio web

¡Ojo!

- Antes de invertir hay que verificar la información disponible sobre los creadores del proyecto
- Precaución y pensamiento crítico = protección contra el fraude financiero

Pirámide Bitconnect

Cómo funciona

- **Se hace pasar** por una plataforma de trading de criptomonedas con inteligencia artificial
- **Promete grandes ganancias** con un riesgo mínimo
- **Programa de referidos:** 7-15 % de los depósitos de nuevos miembros

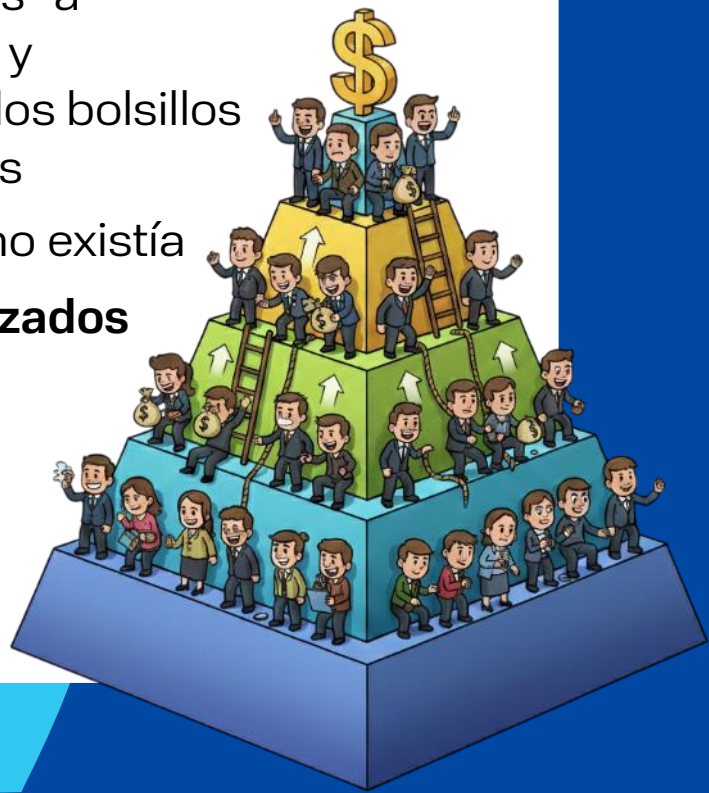
Consecuencias

- Inversores afectados de más de **40 países**
- Más de **17 mill. de $** de pérdidas

Mecanismos de engaño

- Dinero de nuevos inversores → pagos de "ganancias" a antiguos inversores y bonificaciones → a los bolsillos de los organizadores
- El robot de trading no existía

Ingresos altos garantizados
+
bonificaciones por referencias
=
una clara señal de estafa financiera



Pirámide financiera Finiko

Cómo funciona

- **Eliminación de deudas** mediante inversiones
- Uso de modelos matemáticos e IA para reducir riesgos
- Oportunidad de comprar un apartamento o un coche **al 35% de su precio**
- **Depósitos con una rentabilidad del 20-30% mensual**

Rasgos característicos

- Todas las operaciones se realizaban en bitcóin y en la criptomoneda Tether
- Se prohibía recargarse con dinero fiduciario
- La popularidad del esquema creció gracias a grandes ofertas “ventajosas”

Ingresos altos + incapacidad de usar dinero regular = una clara señal de fraude

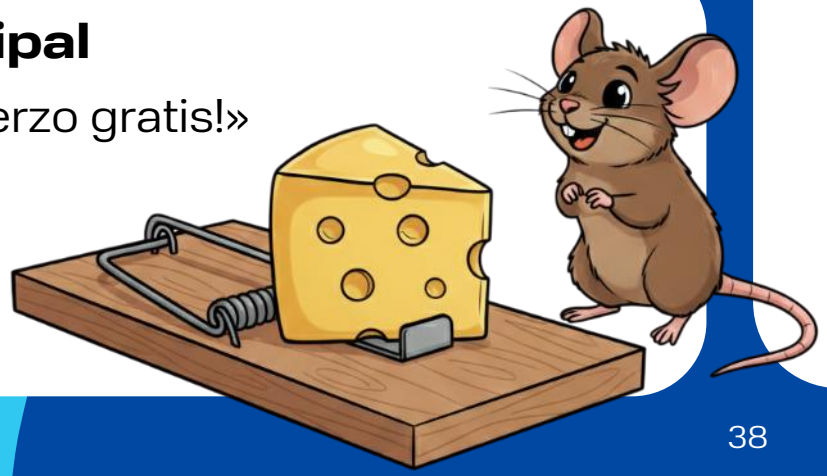
Normas de seguridad

Verificar la legalidad

- Todas las instituciones financieras deben contar con la licencia del Banco Central de la Federación Rusa
- Sitio web de verificación: *cbr.ru/inside/warning-list*

Regla principal

«¡No hay almuerzo gratis!»



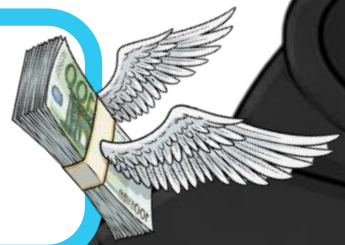
Indicios de pirámides financieras

- Promesas poco realistas de rentabilidad varias veces superior al mercado
- Programa de referidos
- Falta de licencia y documentación
- Publicidad agresiva y urgencia (“¡Solo hoy!”)
- Falta de transparencia: ausencia de información sobre la dirección, el registro oficial
- Aceptación de efectivo o criptomonedas sin documentación

El objetivo principal de los atacantes

es hacer que la víctima baje la guardia y deje de pensar de manera crítica

Los esquemas cambian, pero
la idea sigue siendo la misma



Tiendas y sitios web de phishing

Cómo funciona

Los estafadores hacen copias de sitios web de tiendas, aerolíneas, bancos, etc.

Ofrecen productos, paquetes de viajes con descuento, atrayendo a la víctima

Normas de seguridad

Realizar compras a través de aplicaciones oficiales

No hacer clic en enlaces de correos electrónicos

Asegurarse de que el sitio utilice **https** y no http.

Una tarjeta separada para compras en línea

Ver errores en el texto y el nombre del sitio

Utilizar *software* antivirus

Entrega de flores y “Gosuslugi”

Cómo funciona

Llamada del “servicio de entrega”

se pide decir el código de “confirmación” del SMS

→

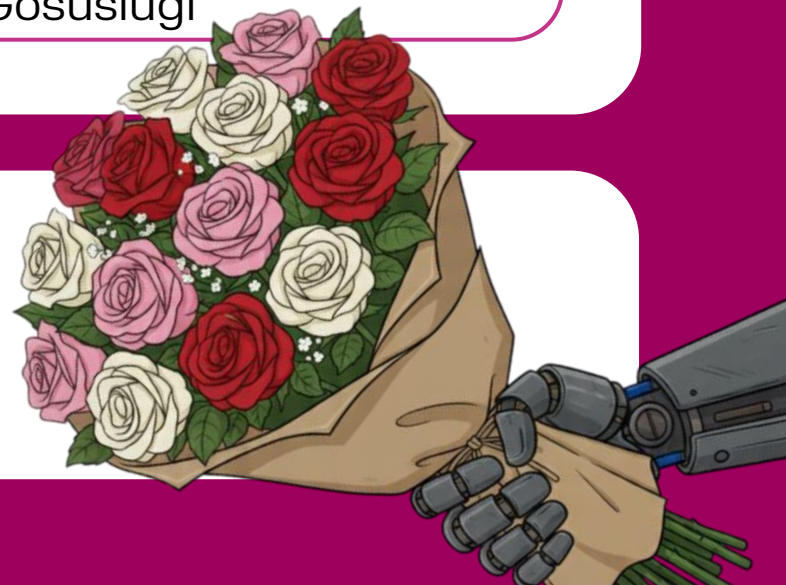
Llamada de “Roskomnadzor”

denuncian una situación presuntamente insegura

→

La segunda llamada del “servicio de seguridad”

se finge ayudar a restaurar el acceso a “Gosuslugi”



Normas de seguridad

- Nunca decir códigos de SMS; son códigos para microcréditos
- Cuestionar la situación: ¿Se esperaba la entrega? Si no, es una estafa

⇆ Bloqueo de tarjetas mediante la IA ✕

Cómo funciona

Llamada al banco de un "cliente"
Proporcionan información personal y utilizan IA para imitar voz

→

Bloqueo de tarjetas
Motivos: pérdida, robo, etc.

→

Amenazas a la víctima
Exigen dinero

Normas de seguridad

Llamar al banco únicamente al número oficial

No transferir dinero bajo ninguna circunstancia

Contar a todos los familiares sobre el fraude

Problema global

Población adulta del mundo

57 %
se enfrentó al fraude

54 %
sufrió pérdidas al comprar en línea

48 %
sufrió fraudes de inversión

Consecuencias psicológicas

69 %
experimenta un estrés severo

14 %
experimenta deterioro en las relaciones familiares

17 %
experimenta pérdida de autoconfianza

La mejor defensa es el pensamiento crítico y la alfabetización digital

- Casi una de cada cuatro personas que se consideran cautelosas siguen perdiendo dinero
- Los estafadores perfeccionan constantemente sus tácticas, y la vigilancia básica ya no es suficiente

Olimpiada Internacional de Seguridad Financiera

Las tareas de la olimpiada se basan en los siguientes programas:

Escolares

- Matemáticas
- Informática
- Ciencias Sociales

Estudiantes universitarios

- Relaciones Internacionales, Estudios Regionales Extranjeros
- Economía, Finanzas, Seguridad Económica
- Matemáticas, Seguridad Informática
- Jurisprudencia

Premios y beneficios

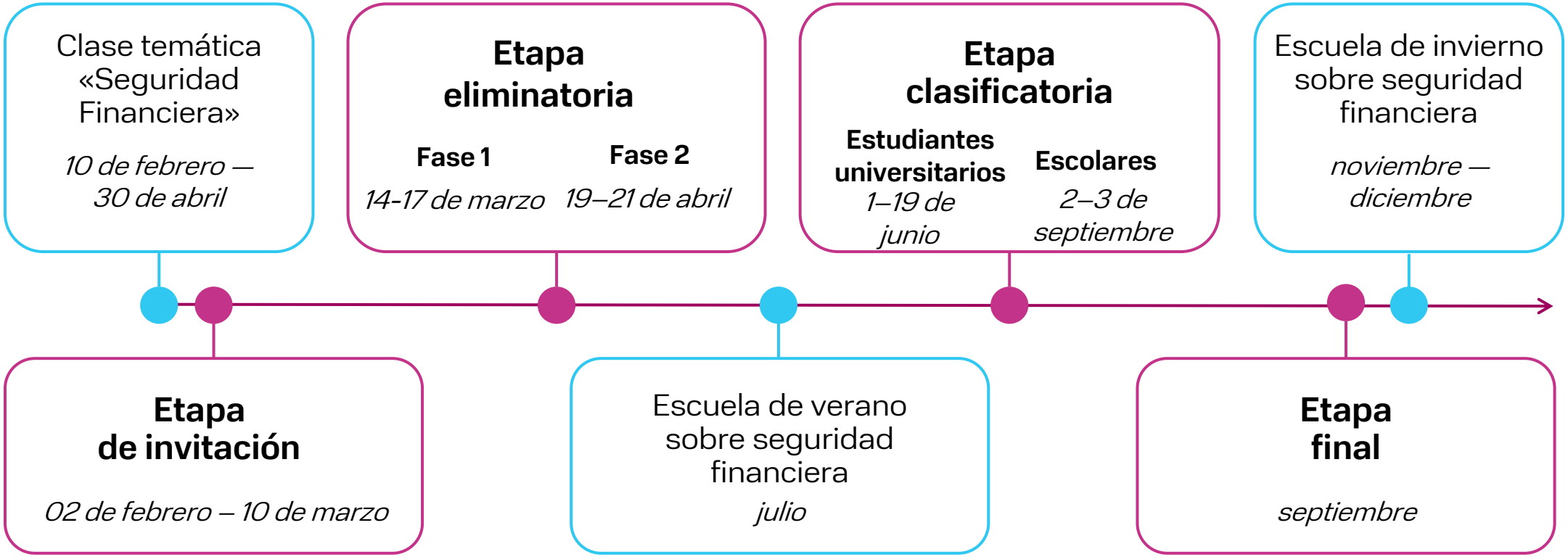
✓ **Beneficios de admisión a las universidades** del Instituto Internacional de Redes (Grado, Máster, Doctorado)

✓ **Oportunidad de hacer prácticas** en Rosfinmonitoring y otras organizaciones

rosfinolymp.ru

Olimpiada Internacional de Seguridad Financiera

sodrujestvo.org



Socios

SERVICIO FEDERAL
DE MONITOREO
FINANCIERO

MINISTERIO
DE EDUCACIÓN
DE LA FEDERACIÓN
DE RUSIA

MINISTERIO
DEL INTERIOR
DE LA FEDERACIÓN
DE RUSIA

РУДН

MINISTERIO DE CIENCIA
Y EDUCACIÓN SUPERIOR
DE LA FEDERACIÓN DE RUSIA

МУМЦУМ

содружество

ПСБ

ЦЕНТР
МЕЖОЛИМПИАДНОЙ
ПОДГОТОВКИ