INTERPOL

INFORME DE INTERPOL DE EVALUACIÓN DE LAS CIBERAMENAZAS EN ÁFRICA - 2025

4ª EDICIÓN

MAYO DE 2025

AVISO LEGAL

ÍNDICE

Neal Jetton
Director de
Ciberdelincuencia
INTERPOL

PRÓLOGO DE INTERPOL

El continente africano se encuentra en un momento crucial de su evolución digital. Conforme la conectividad va ampliándose a nuevos lugares y la innovación digital acelera su desarrollo, también aumenta la complejidad de las ciberamenazas a las que se enfrenta la región. Estas amenazas no se detienen en las fronteras, sino que las trascienden, avanzan rápidamente y son cada vez más sofisticadas. Atacan directamente a la base sobre la que se sustenta el progreso: los sistemas financieros, los servicios públicos, las infraestructuras esenciales y, sobre todo, la confianza de la ciudadanía en el futuro digital.

Esta cuarta edición del Informe de INTERPOL de evaluación de las ciberamenazas en África ofrece una inestimable instantánea de la situación actual. Gracias a la información policial operativa recibida, la amplia participación de las fuerzas del orden y la colaboración estratégica del sector privado, en el informe se ha podido dibujar con precisión un panorama de las amenazas en constante cambio, en el que siguen predominando el *malware*, y en particular el *ransomware*, las estafas en línea (incluidas las cometidas mediante *phishing*) y las estafas a empresas por *e-mail* mediante suplantación de identidad (estafas BEC), y se pone asimismo de manifiesto la urgente necesidad de neutralizar los peligros emergentes -como las estafas basadas en inteligencia artificial, los abusos sexuales a partir de imágenes en línea y los delitos sexuales digitales, y la ciberdelincuencia como servicio-.

En INTERPOL sabemos que no existe ningún organismo ni país que puedan combatir en solitario estas amenazas. La magnitud y el ritmo progresivo de la ciberdelincuencia exigen una reacción unificada, coordinada y basada en información policial. Por mediación de las Operaciones Conjuntas contra la Ciberdelincuencia en la Region Africana, y en estrecha colaboración con AFRIPOL, estamos reforzando las capacidades operativas, aumentando la confianza entre las unidades nacionales especializadas en ciberdelincuencia y favoreciendo una cooperación transfronteriza que consiga desarticular de manera efectiva las redes de ciberdelincuentes.

En este informe se evidencian asimismo las crecientes competencias de los organismos africanos encargados de la aplicación de la ley y su mayor capacidad de adaptación. Se están produciendo avances: desde fructíferas operaciones regionales hasta nuevas reformas legislativas y esfuerzos en el ámbito de la capacitación. Con todo, aún queda mucho por hacer. Las lagunas en el ámbito de la cultura digital, la armonización legislativa, los recursos disponibles para la investigación y el acceso a las pruebas digitales siguen suponiendo una traba para una actuación policial eficaz.

Para nuestros socios -ya sean de las fuerzas del orden, la Administración pública, la industria, o la sociedad civil-, este informe es tanto una llamada a la acción como la base de toda colaboración. Solo podremos proteger el futuro digital de África si trabajamos juntos, intercambiando conocimientos y generando confianza entre los países y los sectores.

Quiero hacer extensivo mi más sincero agradecimiento a la oficina de Operaciones Conjuntas contra la Ciberdelincuencia en la Region Africana y a todas aquellas personas que han participado en la elaboración de este informe. El trabajo de todos ustedes refuerza nuestra determinación colectiva de construir un entorno digital más seguro y resistente para todos. Para terminar, quisiera dar las gracias a la comunidad de las fuerzas del orden de nuestros países miembros africanos por su entrega a la hora de combatir la ciberdelincuencia y hacer del mundo un lugar más seguro.

Embajador Jalel Chelba
Director ejecutivo
(en funciones)
de AFRIPOL

PRÓLOGO DE AFRIPOL

El continente africano se está adentrando en una era de transformación digital acelerada, que comporta unas oportunidades sin precedentes para el desarrollo económico, social e institucional de sus Estados miembros. Este impulso refleja el compromiso colectivo de agilizar la inclusión digital, mejorando los servicios públicos y promoviendo la innovación local. Pero estos importantes avances también conllevan la proliferación en el ciberespacio de unas amenazas cada vez más sofisticadas, que ponen en jaque la seguridad de los países, las infraestructuras esenciales y las empresas, y comportan un peligro para los ciudadanos africanos.

Ante la complejidad de estos retos, AFRIPOL se posiciona como la principal organización continental para elaborar una respuesta coordinada, ambiciosa y adaptada al contexto, que tome en consideración las distintas realidades africanas. Nuestro compromiso es claro: promover una soberanía digital sólida capaz de proteger eficazmente a nuestras sociedades de unas ciberamenazas cada vez más ingeniosas, que a menudo son de naturaleza transnacional y avanzan tan rápidamente como las propias tecnologías.

En 2024, AFRIPOL intensificó su labor estrechando la cooperación con INTERPOL, las estructuras regionales especializadas, los organismos nacionales dedicados a la seguridad y los socios estratégicos del sector privado. Algunas de las operaciones más importantes, como la operación Serengeti, lograron desmantelar redes delictivas sofisticadas especializadas en *ransomware*, estafas financieras, *phishing* dirigido contra objetivos concretos y ataques lanzados contra los sistemas de información públicos. Estos buenos resultados operativos ponen de relieve la importancia de la cooperación interinstitucional, el intercambio de información y una reacción coordinada a escala continental.

Paralelamente, AFRIPOL ha seguido reforzando las competencias de sus funcionarios policiales mediante programas formativos especializados y específicos, que tratan sobre ámbitos clave, como el análisis de información policial, el seguimiento de flujos financieros ilícitos, la investigación digital, la vigilancia cibernética y la protección de infraestructuras esenciales. Los acuerdos estratégicos suscritos con Kaspersky y Group-IB en 2024 constituyen un paso decisivo hacia nuestro compromiso de equipar a los Estados miembros con los recursos necesarios para prevenir incidentes graves y reaccionar a ellos, mejorando el acceso a las herramientas tecnológicas, la información policial sobre amenazas y los conocimientos internacionales.

A partir de 2025, AFRIPOL se centrará en tres prioridades estratégicas: 1) continuar reforzando la cooperación internacional y entre los países africanos para responder de manera unificada a las amenazas transnacionales; 2) ayudar activamente a los Estados miembros a aumentar sus capacidades operativas, humanas y tecnológicas; y 3) integrar sistemáticamente las innovaciones emergentes, en concreto, la inteligencia artificial y las tecnologías *blockchain* (o cadena de bloques), para anticipar los riesgos y adaptar nuestras estrategias en tiempo real.

La ciberseguridad no es una cuestión meramente técnica, sino que se ha convertido en un pilar fundamental para la estabilidad, la paz y el desarrollo sostenible en África, como se evidencia en la Agenda 2063. Atañe directamente a la soberanía digital de los países, la capacidad de adaptación de nuestras instituciones, la confianza de la sociedad y el correcto funcionamiento de nuestras economías. Es en nombre de la responsabilidad compartida, la solidaridad continental y la innovación constante como AFRIPOL renueva su compromiso para construir un ciberespacio africano seguro, inclusivo, soberano y resiliente que esté al servicio de la paz, la seguridad y el progreso colectivo.

ABREVIATURAS Y ACRÓNIMOS

AFJOC	Operaciones Conjuntas contra la Ciberdelincuencia en la Región Africana
AFRIPOL	Mecanismo Africano para la Cooperación Policial
IA	Inteligencia artificial
APK	Paquete de aplicaciones para Android
UA	Unión Africana
Estafas BEC	Estafa a empresas por *e-mail* mediante suplantación de la identidad
CEO	Director general
DDoS	Denegación de servicio distribuida
FCDO	Ministerio de Asuntos Exteriores, de la Commonwealth y de Desarrollo
GB	Gigabyte
GEPF	Fondo de pensiones de la función pública (Sudáfrica)
TIC	Tecnologías de la información y la comunicación
ASBIL	Abusos sexuales basados en imágenes en línea
SIM	Módulo de identidad del suscriptor
SMS	Servicio de mensajes cortos
TB	Terabyte
RU	Reino Unido
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

AGRADECIMIENTOS

Este informe ha sido redactado por la oficina de Operaciones contra la Ciberdelincuencia en la Región Africana con la ayuda de las operaciones Conjuntas contra la Ciberdelincuencia en Región Africana (AFJOC), y ha sido financiado por el Ministerio de Asuntos Exteriores, de la Commonwealth y de Desarrollo del Reino Unido. Toda consulta relacionada con el informe debe formularse a través de la dirección de correo electrónico AfricaDesk@interpol.int.

Este informe es la culminación de un minucioso análisis de la información recopilada a través de diversas fuentes, como los países miembros africanos y los socios de INTERPOL del sector privado (entre ellos Bi.Zone, Group-IB, Kaspersky y Trend Micro). Además, para documentar y completar el informe, y con el fin de garantizar una visión completa y matizada de los asuntos tratados en él, se ha tomado contacto con las propias unidades de INTERPOL dedicadas a la información policial y las operaciones.

Agradecemos sinceramente la participación de 43 de los 54 países miembros africanos que han cumplimentado el cuestionario de evaluación de las ciberamenazas, los cuales han aportado una información valiosa que ha servido para documentar este informe.

INTERPOL

AFJOC

Foreign & Commonwealth Office

AFRIPOL

BI.ZONE Cybersecurity

GROUP-IB

kaspersky

TREND MICRO

RESUMEN

La ciberdelincuencia se está disparando en África, y supone una amenaza para la seguridad pública, los sistemas financieros y la confianza digital. Si bien muchos países están reaccionando a ella, otros muchos todavía afrontan graves problemas estructurales que limitan su capacidad para detectar, investigar y neutralizar las ciberamenazas.

Siguen existiendo desigualdades en cuanto a las capacidades policiales. La mayoría de los países informan de un déficit en competencias investigadoras, un acceso limitado a las herramientas de criminalística digital y una infraestructura insuficiente. Pese a que varios países han creado unas unidades especializadas en ciberdelincuencia, a menudo estas funcionan con unos recursos y unos efectivos limitados.

Se están perfeccionando los marcos jurídicos, pero los avances se producen de manera irregular. Algunos países miembros han modernizado sus leyes sobre ciberdelincuencia, pero, en muchos casos, los países que han cumplimentado el cuestionario subrayan la necesidad de mejorar sus marcos jurídicos y su capacidad de investigación. Asimismo, estas leyes podrían ajustarse mejor a las normas regionales e internacionales. Estas lagunas siguen siendo una traba para los procesos judiciales y la admisibilidad de las pruebas digitales.

La coordinación transfronteriza continúa siendo un obstáculo importante. Aunque las operaciones facilitadas por INTERPOL han cosechado unos resultados destacados, los países informan de que los conductos oficiales de cooperación, como el procedimiento de asistencia judicial recíproca, son todavía lentos y apenas se recurre a ellos. Los conflictos de competencia jurisdiccional, la falta de confianza y el acceso limitado a las plataformas globales digitales complican aún más la labor policial regional.

Las amenazas emergentes evolucionan rápidamente. El uso delictivo de la inteligencia artificial, los medios sintéticos y las estafas perpetradas a través de dispositivos móviles está sobrepasando la capacidad de reacción de muchos organismos. A menudo, estas amenazas aprovechan los puntos débiles jurídicos y operativos, y han de ser combatidas mediante nuevas formas de colaboración interinstitucional e internacional.

Pero, a pesar de estos problemas, también hay señales alentadoras de progreso. Varios países miembros han reforzado sus alianzas público-privadas, han actualizado su legislación para poder perseguir de un modo más eficaz los delitos cibernéticos y han participado en fructíferas operaciones regionales. La concienciación sobre los riesgos de la ciberdelincuencia va aumentando progresivamente, y un número cada vez mayor de servicios policiales nacionales está dando prioridad a las capacidades de investigación digital.

En este informe se presentan los principales retos a los que se enfrenta África en el ámbito de la ciberdelincuencia, las amenazas emergentes predominantes y algunos ejemplos reales de barreras sistémicas y éxitos operativos. El informe termina con unas recomendaciones para mejorar las capacidades nacionales, reforzar los marcos jurídicos y procedimentales y ahondar en la cooperación internacional, todos ellos aspectos esenciales para desarrollar una capacidad de adaptación duradera.

1. INTRODUCCIÓN

La acelerada evolución digital de África está transformando las economías, la gobernanza y la sociedad. Pese a utilizar las últimas tecnologías e innovaciones, también está ampliando considerablemente el rango de ataque de los ciberdelitos. A medida que aumenta la integración digital, también lo hacen las amenazas dirigidas contra los sistemas financieros, los servicios públicos, las empresas y los usuarios finales.

Para entender mejor este panorama de riesgos en continuo cambio y poder hacerle frente, INTERPOL ha llevado a cabo una evaluación de las ciberamenazas en todo el continente africano. El informe ha sido elaborado a partir de **una encuesta detallada realizada entre los organismos africanos encargados de la aplicación de la ley, información policial operativa, información de los socios de INTERPOL del sector privado e información de fuentes públicas**. Este enfoque basado en diversas fuentes garantiza una visión fundamentada y exhaustiva de las tendencias regionales.

Esta evaluación es una continuación del Informe de evaluación de las ciberamenazas en África - 2024, y se inspira en las conclusiones del informe del año anterior. Su propósito es ofrecer una perspectiva actualizada del panorama de la ciberseguridad y hacer un seguimiento de los avances realizados a la hora de abordar los retos previamente resaltados.

La finalidad de este informe es ayudar a los organismos encargados de la aplicación de la ley, los responsables de la elaboración de políticas y las partes interesadas en el ámbito de la ciberseguridad a detectar las amenazas emergentes, colmar las lagunas en materia de capacidades y mejorar la cooperación a escala nacional y regional. La investigación de los delitos cibernéticos en todos los niveles afecta directamente a las víctimas y las víctimas potenciales ubicadas en cualquier lugar del mundo. Gracias a una labor colectiva, el futuro digital de África será más seguro.

2. EL PANORAMA CAMBIANTE DE LAS CIBERAMENAZAS EN ÁFRICA

La rápida transformación digital de África ha ampliado considerablemente la conectividad e impulsado la adopción generalizada de tecnologías, como la banca móvil, el comercio electrónico y la computación en la nube, lo que ha favorecido el crecimiento económico y la innovación[1]. Con todo, esta expansión también conlleva la aparición de retos en materia de ciberseguridad, pues las infraestructuras digitales resultan cada vez más atractivas para los ciberdelincuentes. Con más de 500 millones de usuarios de Internet en la región, muchos países todavía carecen de las medidas adecuadas en materia de ciberseguridad, lo que deja a empresas y personas expuestas a sufrir ataques cibernéticos[2]. Muchos países del continente se enfrentan a retos, como unos marcos jurídicos en fase de creación, unas inversiones limitadas en ciberseguridad y lagunas en materia de cultura digital, lo que agrava estos riesgos aún más.

Como consecuencia del uso generalizado de los teléfonos inteligentes, las plataformas móviles se han convertido en el objetivo principal de los ciberdelincuentes, sobre todo en aquellas regiones en las que la banca móvil se ha implantado de manera masiva. Adicionalmente, la progresiva integración de los dispositivos del Internet de las cosas en sectores tales como la agricultura, la sanidad y la fabricación entraña nuevos riesgos para la seguridad, pues muchos de ellos carecen de una protección robusta[3]. Varios países africanos -como Etiopía, Zimbabue, Angola, Uganda, Nigeria, Kenia, Ghana y Mozambique- se encuentran entre los que más ataques han recibido en 2024, según los datos sobre detección de malware procedentes del Índice Global de Amenazas Cibernéticas de la Unión Internacional de Telecomunicaciones (UIT)[4]. Esto pone de relieve la necesidad de contar con unos marcos más robustos en materia de ciberseguridad para proteger los avances digitales y garantizar una capacidad de adaptación duradera en la región[5] [6].

El Informe de INTERPOL de evaluación de las ciberamenazas en África - 2025 pone de relieve el brusco aumento de los incidentes relacionados con delitos cibernéticos en África. Más de dos tercios de los países miembros africanos de INTERPOL que han respondido a la encuesta han indicado que los delitos dependientes del entorno cibernético y los delitos facilitados por Internet representan un porcentaje medio-alto del total de todos los delitos. En concreto, los delitos cibernéticos representan más del 30 % de todos los delitos denunciados en África Occidental y Oriental, con lo que son una de las principales fuentes de preocupación en estas subregiones:

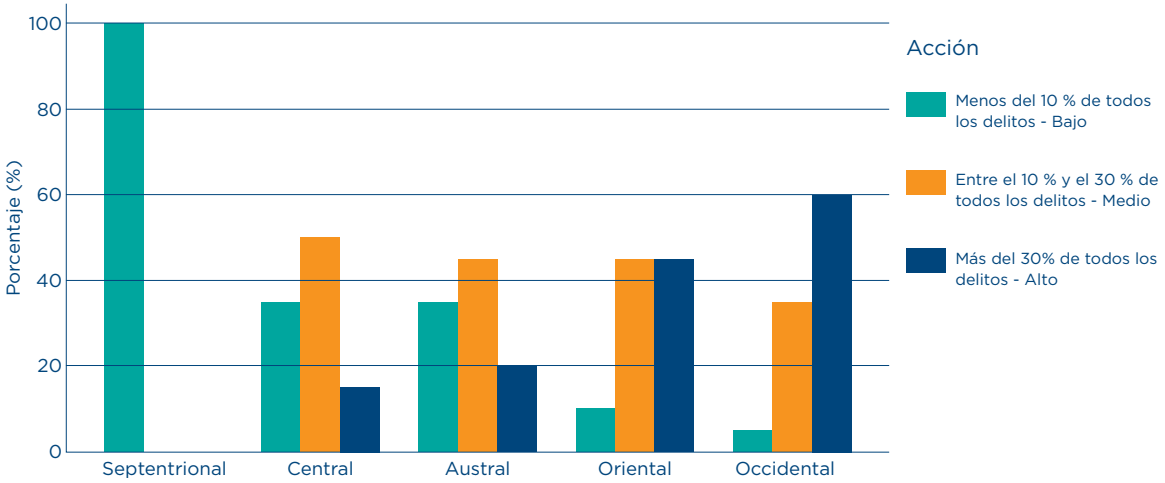


Gráfico 1: Niveles percibidos de riesgo cibernético en las regiones africanas según lo indicado por los países miembros africanos de INTERPOL en la encuesta de 2025.

1 GSMA, The Mobile Economy of the Sub-Saharan Africa (la economía móvil del África subsahariana): https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf
2 https://innovation-village.com/cybersecurity-in-africa-emerging-threats-and-solutions
3 GSMA, The Mobile Economy of the Sub-Saharan Africa (la economía móvil del África subsahariana): https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf
4 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
5 Check Point, The State of Cyber Security 2025: https://www.checkpoint.com/security-report
6 https://it-online.co.za/2024/09/13/africa-faces-urgent-cybersecurity-challenges

En ediciones anteriores del informe se indicó que los ciberdelitos más frecuentes eran los ataques de *ransomware*, los troyanos bancarios, los *stealers* (*malware*), las estafas por Internet, el *phishing*, las estafas BEC y los *software* maliciosos ofrecidos como servicio (como el *spyware* y los paquetes de *phishing*)[7]. Las estafas por Internet, y en concreto el *phishing*, siguen siendo los ciberdelitos más habitualmente denunciados por los países miembros de INTERPOL, mientras que el *ransomware* y las estafas BEC continúan siendo muy comunes. Adicionalmente, los países miembros africanos señalan como principales ciberamenazas la sextorsión digital y la suplantación de identidad.

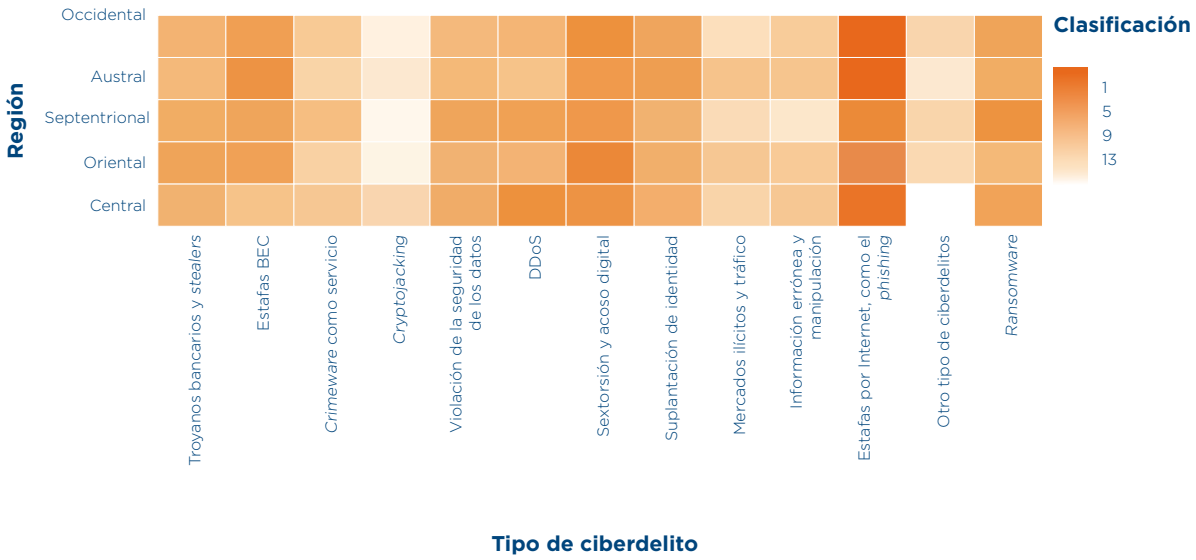


Gráfico 2: Ciberamenazas denunciadas con mayor frecuencia en los países miembros africanos de INTERPOL en 2024, según los datos de la encuesta realizada entre los organismos encargados de la aplicación de la ley.

En comparación con años anteriores, se ha observado una disminución en el número de incidentes denunciados en relación con troyanos bancarios, *stealers* de información y ciberdelincuencia como servicio. Esta tendencia podría ser indicativa de una intensificación de la labor policial, un mejor conocimiento en el ámbito de la ciberseguridad, o un cambio en las tácticas empleadas por los ciberdelincuentes, quienes optan por métodos más eficaces, como la ingeniería social y las estafas basadas en inteligencia artificial.

Muchos de los países miembros de INTERPOL de la región africana han señalado que los delitos cibernéticos cada vez producen más efectos de índole financiera y operativa, y han informado de que las amenazas más perjudiciales desde el punto de vista financiero para todas las regiones son las estafas por Internet, las estafas BEC, el *ransomware* y los ataques de denegación de servicio distribuidos (DDoS).

Entre 2019 y 2025, los incidentes cibernéticos acaecidos en el continente africano generaron unas pérdidas económicas estimadas en más de 3000 millones de dólares[8], y los sectores que más acusaron estas repercusiones fueron el financiero, el sanitario, el energético y el público[9]. Estos sectores esenciales son el objetivo principal de los ciberdelincuentes, quienes crean fallas operativas y cometen violaciones de la seguridad de los datos con importantes consecuencias financieras.

7 Informe de INTERPOL de evaluación de las ciberamenazas en África - 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

8 https://african.business/2025/02/apo-newsfeed/over-half-of-africans-fear-financial-losses-from-cybercrime-survey-finds

9 Informe de Group-IB de 2023/2024 sobre las tendencias en delitos de alta tecnología y el panorama de las ciberamenazas en Próximo Oriente y África (versión inglesa): https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-mea/

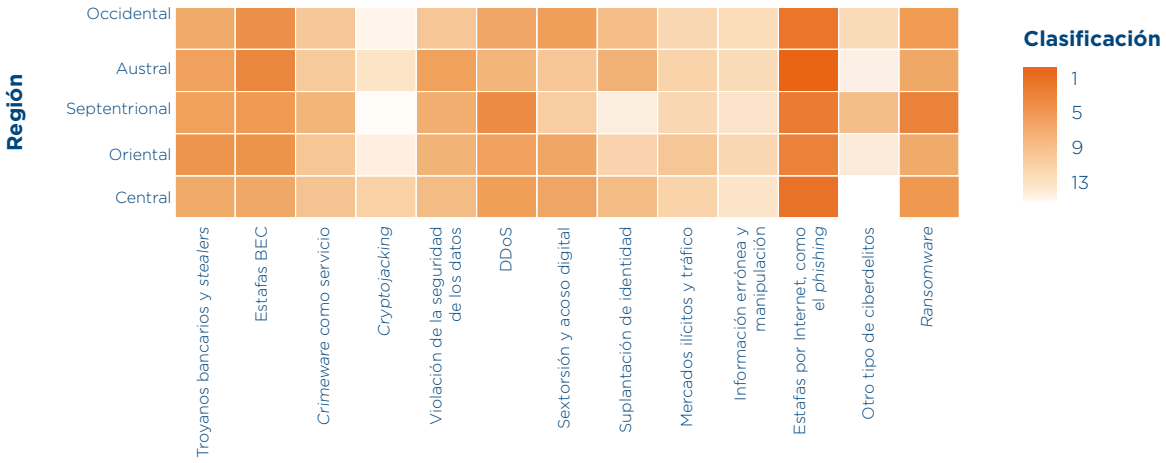


Gráfico 3: Clasificación promedio de los tipos de ciberdelitos en función de las repercusiones económicas comunicadas para cada subregión africana, según los datos facilitados por los países miembros de INTERPOL.

Según han informado los países miembros africanos de INTERPOL, los ciberdelincuentes están perfeccionando continuamente sus tácticas, y recurren a la ingeniería social, la inteligencia artificial y las plataformas de mensajería para lanzar unos ataques cada vez más sofisticados. La principal táctica utilizada por las redes nacionales e internacionales de ciberdelincuencia es explotar la vulnerabilidad humana, para lo que emplean unas técnicas avanzadas de engaño con el propósito de estafar a organizaciones y personas.

2.1 Las ciberamenazas más comunes en África en 2024

Según los resultados de la última encuesta realizada entre los países miembros africanos de INTERPOL y los socios privados[10] , así como las conclusiones de los informes regionales sobre ciberseguridad, las ciberamenazas más importantes son las estafas en línea, el *ransomware*, las estafas BEC y la sextorsión digital. En este apartado se analiza en detalle el panorama cambiante de las ciberamenazas y se destacan cuáles han sido las amenazas más frecuentes en África en 2024.

2.1.1. ESTAFAS POR INTERNET

Las estafas por Internet están experimentando un brusco repunte en varios países, ya que los ciberdelincuentes están continuamente adaptando sus métodos para explotar las vulnerabilidades con el fin de estafar a personas y empresas. Las actividades fraudulentas, como el *phishing* y las estafas sentimentales por Internet, son cada vez más sofisticadas, gracias al uso estratégico de la ingeniería social, la inteligencia artificial y la manipulación por conducto de las plataformas de medios sociales. Los países miembros de INTERPOL han señalado que este tipo de estafas por Internet son las ciberamenazas más graves a las que se ha enfrentado África en 2024 y han advertido de su frecuencia cada vez mayor y sus graves repercusiones. Este hecho ha sido confirmado por otras fuentes, incluidos los datos facilitados por los socios privados de INTERPOL.

10 Datos facilitados por cuatro socios privados de INTERPOL: Group-IB, Trend Micro, Kaspersky y Bi.Zone.

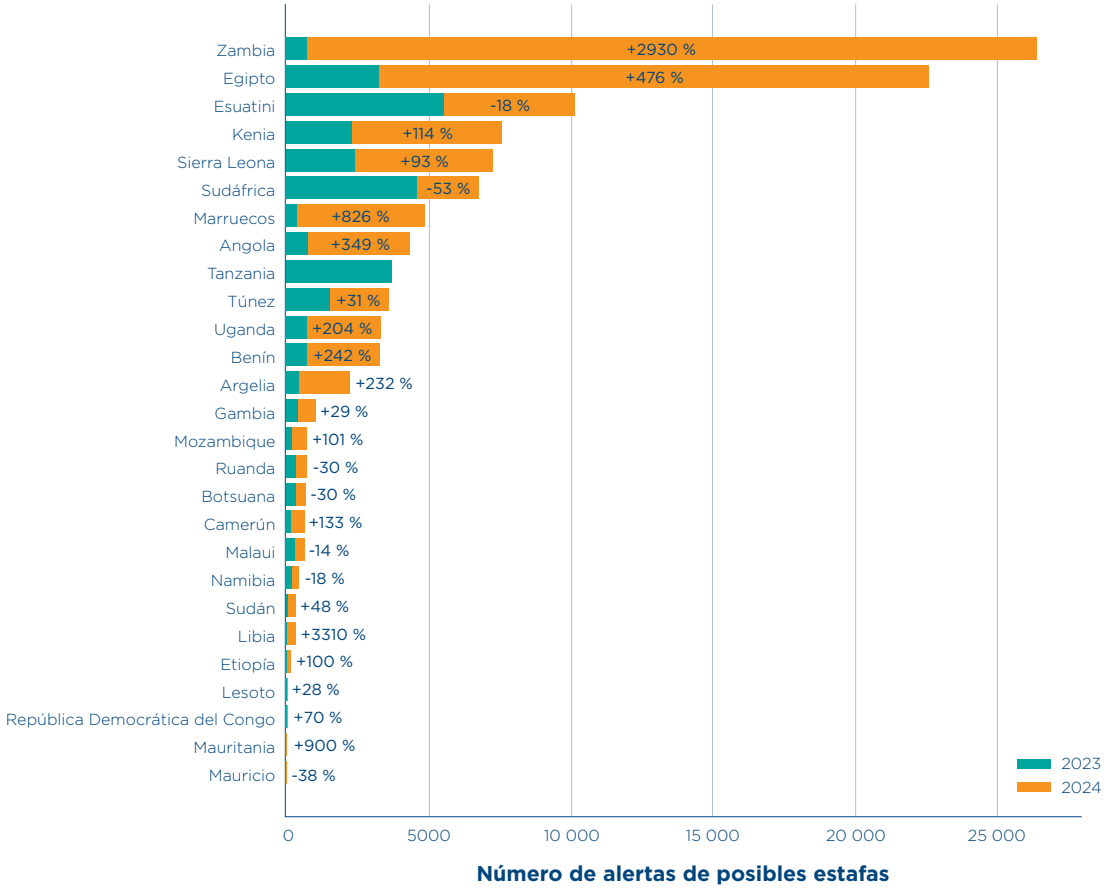


Gráfico 4: Aumento de las alertas de estafa en las regiones africanas entre 2023 y 2024, según los datos facilitados por Kaspersky.

El auge de las estafas por Internet está estrechamente relacionados con la aceleración de la transformación digital en África[11]. Los ciberdelincuentes aprovechan el aumento de las actividades en línea, y en particular el uso de los medios sociales, el comercio electrónico y la banca móvil, para perpetrar sus estafas. Según la información facilitada por los países miembros africanos de INTERPOL, no existe un único perfil de víctima de este tipo de delito, pues se ven afectados por él grupos de todas las edades, géneros y profesiones. Aunque algunos grupos son más vulnerables que otros -según ponen de manifiesto los datos aportados por los países miembros encuestados-, también es evidente que todos los grupos de población están en riesgo.

En 2024, el tipo de ciberamenaza más común en África han seguido siendo las estafas por Internet, mediante la técnica de *phishing*, de las que fueron víctimas personas y organizaciones de todo el continente. Los países miembros de INTERPOL han señalado al *phishing* como el mayor peligro para la ciberseguridad, por su elevada frecuencia y su amplio alcance. Según los informes de seguridad digital, el *phishing* representa el 34 % de todos los incidentes cibernéticos detectados en África[12]. Los ciberdelincuentes se sirven de esta técnica para suplantar la identidad de entidades de confianza en mensajes de correo electrónico, plataformas de mensajería, o sitios web fraudulentos, con el fin de engañar a la gente para que les facilite información confidencial, como sus credenciales de acceso, datos financieros, o datos personales[13]. Una vez obtenida, esta información facilita el acceso no autorizado, la suplantación de identidad y las estafas. La creciente sofisticación de las técnicas de *phishing* intensifica de manera notoria la vulnerabilidad de sectores esenciales, como la banca, las instituciones públicas y las telecomunicaciones.

11 GSMA, The Mobile Economy of the Sub-Saharan Africa (la economía móvil del África subsahariana): https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf

12 ESET Threat Report (Informe sobre amenazas): https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22024.pdf

13 Informe de INTERPOL de evaluación de las ciberamenazas en África - 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

Los datos arrojados por la encuesta de INTERPOL indican que las tácticas de *phishing* han evolucionado de manera considerable. Ahora, se trata de un *phishing* más personalizado y localizado, con un grado creciente de sofisticación tecnológica, con lo que se está pasando de las tradicionales estafas de correos electrónicos masivos a unos ataques de ingeniería social dirigidos a víctimas concretas. Hoy día, los ciberdelincuentes suelen suplantar la identidad de autoridades reconocidas y empresas destacadas, se aprovechan de la situación de desempleo generalizado para publicar ofertas de trabajo falsas y utilizan plataformas móviles para cometer estafas que tratan sobre premios y situaciones de emergencia. Además, las campañas de *phishing* móvil (*smishing*), *phishing* telefónico (*vishing*) y *phishing* en medios sociales se aprovechan de la confianza y los resortes emocionales de las víctimas, lo que dibuja un panorama de amenazas más amplio[14]. La posibilidad de acceder a herramientas de *phishing* a un precio asequible en mercados ilícitos favorece significativamente la proliferación de estas estafas. Los ciberdelincuentes también están integrando mensajes, audios o vídeos generados por inteligencia artificial para aumentar la credibilidad y la capacidad de persuasión de las campañas de *phishing*, adaptando el contenido de sus mensajes para reflejar el idioma local y los matices culturales[15].

Los datos facilitados por los países miembros africanos de INTERPOL ponen asimismo de relieve que los efectos del *phishing* se extienden a múltiples sectores de África, cada uno de ellos con vulnerabilidades y repercusiones distintas. Las instituciones financieras han de afrontar unas pérdidas considerables como consecuencia del robo de credenciales y la realización de transacciones no autorizadas, lo que socava la confianza del cliente y supone una traba para la inclusión digital financiera. Las empresas de telecomunicaciones se topan con problemas relacionados con la explotación de marcas, las estafas por intercambio de tarjetas SIM y las estafas masivas por SMS, lo que afecta negativamente a su reputación y su eficiencia operativa. Además, la Administración pública, las instituciones sanitarias y los centros educativos combaten las filtraciones de datos de ciudadanos, las interrupciones operativas y la caída de la confianza social, lo que resalta la necesidad de adoptar unas estrategias de neutralización robustas y adaptadas a cada sector.

En 2024 se produjo un repunte de las estafas sentimentales por Internet, que se ha convertido en una de las estafas por Internet más comunes del continente. Los estafadores utilizan unas tácticas más avanzadas y perjudiciales, alimentadas por un mayor acceso a Internet y la expansión del alcance de los medios sociales. Los datos facilitados por los países miembros de INTERPOL evidencian que, por lo general, los delincuentes toman contacto con sus víctimas por conducto de los medios sociales, los servicios de mensajería y las aplicaciones de citas en línea. El propósito de los estafadores es cultivar una relación personal aprovechándose de las vulnerabilidades, una práctica que puede consistir desde interactuar durante un breve periodo de tiempo hasta mantener un compromiso duradero durante varios años. Una vez creada la ilusión de confianza, los estafadores comienzan a manipular a sus víctimas para que les entreguen su dinero o activos de otra naturaleza.

En África, las estafas sentimentales por Internet son un motivo de preocupación generalizado y algunas regiones experimentan una incidencia mayor. En concreto, se ha descubierto que los países de África Occidental, como Nigeria, Ghana, Côte d'Ivoire y Benín, son zonas en las que las redes dedicadas a las estafas sentimentales por Internet están especialmente activas[16]. Una de las tendencias más extendidas últimamente es que los estafadores atraen en un primer momento a sus víctimas con promesas de amor, para después coaccionarlas con el fin de que inviertan dinero en estafas con criptomonedas[17].

Las estafas sentimentales por Internet se han convertido en uno de los ciberdelitos más rentables y ocasionan un daño emocional y económico considerable. En uno de las estafas nigerianas más destacadas, un único estafador consiguió amasar más de 1,9 millones de dólares estadounidenses engañando a diversas víctimas, antes de ser detenido[18]. Los datos de INTERPOL desvelan que existen numerosos casos en los que las víctimas africanas realizaron pagos a sus estafadores en repetidas ocasiones, a veces hasta agotar sus planes de pensiones o acumular deudas. Pero muchos casos siguen sin denunciarse porque las víctimas sienten vergüenza, culpa o estigma social, lo que es indicativo de que las consecuencias financieras reales son mucho mayores que las documentadas oficialmente[19]. Debido al aumento de la complejidad y el alcance de estas estafas, los organismos africanos encargados de la aplicación de la ley necesitan de manera urgente recibir formación especializada y perfeccionar sus capacidades en el ámbito forense para afrontar e investigar eficazmente esta amenaza, cada vez más extendida.

14 https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase
15 https://cltc.berkeley.edu/2025/01/16/beyond-phishing-exploring-the-rise-of-ai-enabled-cybercrime
16 https://theconversation.com/online-romance-scams-who-nigeria-and-ghanas-fraudsters-are-how-they-operate-and-why-they-do-it-247916
17 https://www.reuters.com/world/africa/almost-800-arrested-over-nigerian-crypto-romance-scam-2024-12-16/
18 https://www.interpol.int/en/News-and-Events/News/2024/Arrests-in-international-operation-targeting-cybercriminals-in-West-Africa
19 https://www.knowbe4.com/hubfs/Online-Scams+Victims-Africa-report-2024.pdf

2.1.2. *RANSOMWARE*

En 2024, los países miembros de INTERPOL señalaron el *ransomware* como una de las ciberamenazas más extendidas en el continente africano, la cual entraña un riesgo cada vez mayor para la Administración pública, las empresas y los servicios esenciales. Según los datos facilitados por los socios de INTERPOL del sector privado, el número de ataques de *ransomware* detectados mensualmente en África en 2024 fue superior al del año anterior[2]. Estos ataques son especialmente preocupantes debido a sus importantes repercusiones económicas, su capacidad para perturbar gravemente las infraestructuras críticas y el daño que pueden infligir a las organizaciones y las personas afectadas. En los informes elaborados por empresas de ciberseguridad[21] y los socios de INTERPOL del sector privado se indica que los países que mayor número de incidentes de *ransomware* experimentaron en 2024 fueron Sudáfrica y Egipto, seguidos de otras economías altamente digitalizadas, como Nigeria, Kenia, Gambia, Túnez y Marruecos. Argelia, Etiopía y otros países más pequeños, como Benín, también han denunciado importantes ataques, lo que evidencia que el *ransomware* es un reto a escala continental, sobre todo en países dotados de una infraestructura digital más desarrollada.

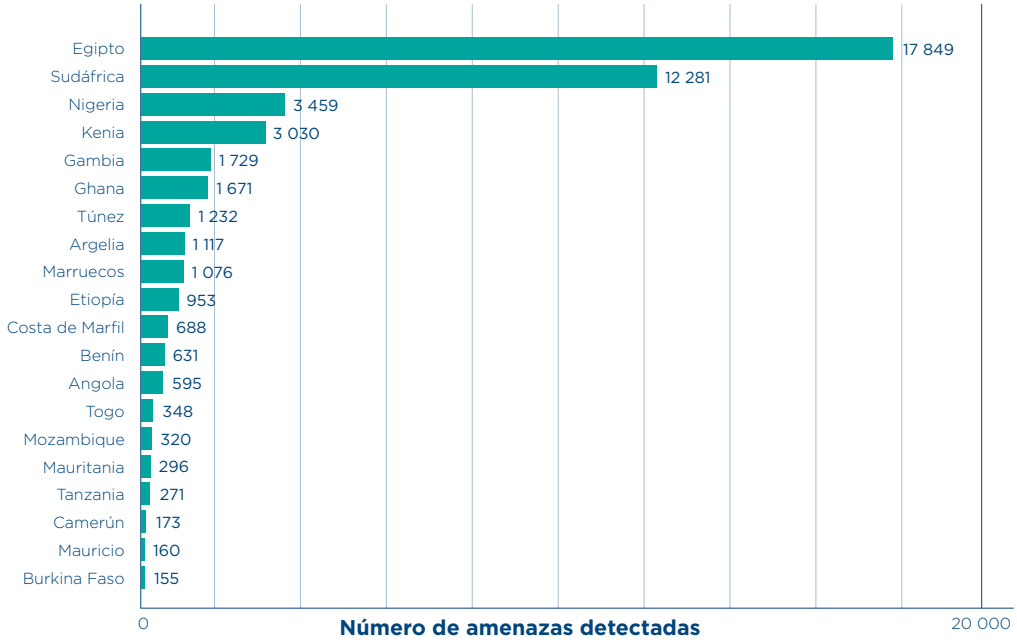


Gráfico 5: Los 20 países africanos con mayor número de amenazas de *ransomware* detectadas en 2024, según los datos facilitados por Trend Micro.

En 2024, las repercusiones económicas del *ransomware* fueron considerables en África. En algunos casos se trató de un robo directo, como el robo cibernético que sufrió en abril la empresa de tecnofinanzas nigeriana Flutterwave, en el que, según se ha informado, se desviaron unos siete millones de dólares estadounidenses[22]. En otros, se exigieron rescates de entre decenas de miles de dólares hasta millones de dólares, a menudo en criptomonedas, lo que ha conllevado importantes cargas financieras. Además, las perturbaciones provocadas por los ataques de *ransomware* han ocasionado pérdidas de ingresos, una reducción de la productividad, la paralización de la actividad comercial y unos gastos de recuperación considerables.

20 Según los datos aportados por Trend Micro en 2024.

21 https://falconfeeds.io/blogs/cyber-attacks-in-africa-a-comprehensive-analysis-of-trends-from-january-to-august-2024-206317

22 https://africa.businessinsider.com/local/markets/fintech-giant-flutterwave-loses-naira11-billion-to-security-breach

El operador eléctrico de Camerún, ENEO, interrumpió su actividad de gestión energética, mientras que la violación de la seguridad sufrida por la autoridad de carreteras urbanas de Kenia, KURA, puso en jaque datos esenciales sobre la infraestructura vial[23]. Las bases de datos públicas también se vieron afectadas, por ejemplo, como consecuencia de los *hackeos* de la autoridad de Kenia para las microempresas y las pequeñas empresas (MSEA, por sus siglas en inglés) y la Oficina Nacional de Estadísticas de Nigeria (NBS, por sus siglas en inglés) que tuvieron lugar en diciembre de 2024[24]. A finales de diciembre de 2024, el Departamento de Defensa de Sudáfrica fue víctima del grupo de *ransomware* Snatch, a resultas de lo cual perdió 1,6 TB de datos, entre ellos, los datos de contacto del presidente[25]. El sector de las telecomunicaciones se ha enfrentado a amenazas similares, como en el caso de la violación de la seguridad de los datos de la empresa Telecom Namibia a finales de 2024, en el marco de la cual quedaron comprometidos 626,3 GB de datos aproximadamente, entre los que había más de 492 000 archivos, y que afectó a más de 619 000 clientes[26]. Esta violación dejó al descubierto información confidencial sobre particulares, empresas y entidades públicas, lo que evidenció el riesgo grave que entraña tanto para la privacidad ciudadana como para la seguridad nacional[27].

Ataques de *ransomware* lanzados contra infraestructuras esenciales (% por región)

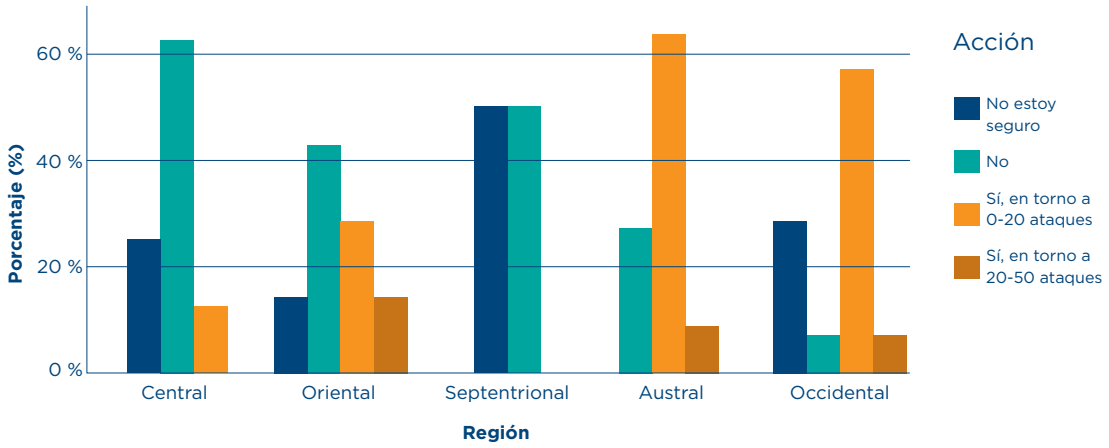


Gráfico 6: Ataques de *ransomware* lanzados contra infraestructuras esenciales por región (%), según las respuestas de los países miembros africanos de INTERPOL a la encuesta de 2024.

Según los datos facilitados por los socios de INTERPOL del sector privado[28], en 2024 varios grupos de *hackers* actuaron en la región africana. Uno de los más destacados fue LockBit, una prolífica banda dedicada al *ransomware* como servicio (RaaS) que estuvo muy activa durante todo el año. LockBit es conocida por utilizar unos métodos abusivos de doble extorsión, consistentes en cifrar las redes de las víctimas al tiempo que las amenazan con publicar los datos robados. En febrero reclamó la autoría del ataque lanzado contra el Fondo de pensiones de la función pública (GEPF, por sus siglas en inglés) de Sudáfrica[29]. También estuvo implicada en numerosos incidentes que han tenido lugar en África Occidental[30]. Pese a que en el marco de una operación internacional las autoridades se incautaron temporalmente de los sitios que LockBit tenía en la red oscura, la banda resurgió poco después para publicar, o tratar de publicar, los datos de sus víctimas, lo que perturbó de manera significativa las operaciones y provocó graves violaciones de la seguridad de los datos[31]. Solo el ataque lanzado contra el Fondo de pensiones de la función pública de Sudáfrica afectó a millones de personas, lo que pone de manifiesto el grave peligro que encierra que LockBit siga actuando.

23 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024
24 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024
25 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack
26 https://neweralive.na/telecom-hit-by-massive-cyberattack-over-400-000-files-leaked
27 https://dailysecurityreview.com/news/namibia-ransomware-attack-sensitive-data-of-government-officials-and-citizens-leaked/
28 Según los datos aportados por BI.ZONE en 2024.
29 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack
30 https://toptechgh.com/lockbit-ransomware-member-extradited-see-attacks-on-africa
31 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack

Otro de los actores de *ransomware* más destacados, Hunters International (Hunters), ataca específicamente a empresas de telecomunicaciones, entidades públicas, e instituciones financieras de África[32]. En julio de 2024, Hunters violó la seguridad de los datos de la autoridad de carreteras urbanas de Kenia, KURA, y robó 18 GB de datos aproximadamente[33]. En diciembre actuó de nuevo, lanzando un ataque contra Telecom Namibia y filtrando información confidencial de sus clientes[34]. Hunters actúa con sigilo, extrayendo clandestinamente los datos antes de cifrar los sistemas; publica los datos de las víctimas que se niegan a pagar el rescate exigido, lo que ocasiona graves interrupciones de la actividad y erosiona la confianza social. BlackSuit, un grupo de *ransomware* dedicado a la extorsión y conocido por dirigir sus ataques contra grandes organizaciones a escala mundial, demostró su falta de escrúpulos al atacar en junio de 2024 el Servicio Nacional de Laboratorios (NHLS, por sus siglas en inglés) de Sudáfrica[35]. Este grave incidente afectó al diagnóstico de millones de pruebas médicas, forzó la anulación de cirugías esenciales y comprometió más de 1 TB de datos altamente sensibles, lo que ilustra claramente el potencial que encierra el *ransomware* para amenazar la vida de las personas y la seguridad.

2.1.3. ESTAFAS A EMPRESAS POR *E-MAIL* MEDIANTE SUPLANTACIÓN DE IDENTIDAD (estafas BEC)

Los países miembros africanos de INTERPOL han señalado que las estafas BEC son una de las ciberamenazas más importantes y que más rápido proliferan dentro del panorama general de las estafas por Internet. Según los datos facilitados por los socios de INTERPOL del sector privado[36], se ha producido un aumento brusco de los delitos cibernéticos relacionados con las estafas BEC en África, tanto por cuanto se refiere al volumen de ataques como a las repercusiones económicas. Un elevado número de autores de estafas BEC actúan desde el continente, concretamente desde África Occidental. Según los datos facilitados por los socios de INTERPOL del sector privado, la mayoría de las estafas BEC perpetradas desde el continente se llevan a cabo desde once países africanos y se concentran en Nigeria, Ghana, Costa de Marfil y Sudáfrica. En África Occidental, algunas de las redes delictivas se han convertido en empresas multimillonarias altamente organizadas que se financian mediante estafas BEC. La organización delictiva transnacional Black Axe, integrada por miles de miembros en todo el mundo, se dedica a cometer estafas financieras a gran escala gracias a las cuales ha acumulado miles de millones de dólares[37].

Según los datos facilitados por los países miembros africanos de INTERPOL, en 2024 el sector financiero fue el más atacado en los Estados miembros africanos. Las empresas dedicadas al comercio internacional y las transacciones financieras frecuentes, y aquellas dotadas de unos controles de seguridad deficientes, fueron especialmente vulnerables a los ataques BEC. Con todo, ningún sector escapa a este tipo de estafas: entidades de todos los tamaños, desde pequeñas y medianas empresas hasta grandes empresas, se han visto afectadas por este delito. Además de en bancos y en instituciones de microfinanciación, se han registrado incidentes serios en sectores como el de la importación y la exportación, el petróleo y el gas, la industria farmacéutica, el transporte y el comercio electrónico. También ha aumentado en todo el continente el número de ataques contra instituciones públicas, el sector del voluntariado y los particulares.

Es difícil obtener el número exacto de estafas BEC cometidas en África debido a que no todas ellas se denuncian; con todo, varios indicadores revelan la verdadera magnitud del problema. Solo en 2024, 19 países africanos informaron conjuntamente de 10 490 detenciones relacionadas con delitos cibernéticos, lo que sugiere que el número real de estafas BEC es considerablemente mayor, pues se estima que solo el 35 % de los ciberdelitos se denuncia oficialmente[38]. En noviembre de 2024 tuvo lugar un caso muy sonado que puso en evidencia los efectos globales provocados por las actividades llevadas a cabo por las redes africanas de ciberdelincuencia, cuando las autoridades estadounidenses condenaron a diez años de prisión a Babatunde Ayeni, un nigeriano de 33 años, por orquestar una estafa BEC a gran escala contra las transacciones inmobiliarias[39]. Ayeni y sus cómplices, quienes actuaban desde Nigeria y los Emiratos Árabes Unidos, lanzaron ataques de *phishing* para robar las credenciales de acceso al correo electrónico de abogados y agentes inmobiliarios radicados en Estados Unidos. A continuación, suplantaron la identidad de estos profesionales para redirigir el pago del cierre de hipotecas hacia cuentas fraudulentas. Más de 400 personas fueron víctimas de esta estafa, mediante la cual se sustrajeron 19,6 millones de dólares estadounidenses, que fueron desviados a cuentas controladas por los estafadores[40]. Este caso pone de manifiesto la naturaleza transnacional de las estafas BEC y el modo en el que las redes africanas de ciberdelincuencia se aprovechan de los sistemas financieros globales para estafar a personas en todo el mundo.

32 Según los datos aportados por BI.ZONE en 2024.
33 https://www.darkreading.com/cyberattacks-data-breaches/ransomware-targeting-infrastructure-telecom-namibia
34 https://magedata.ai/securefact/securefact-cyber-security-news-week-of-december-23-2024
35 https://www.bitdefender.com/en-us/blog/hotforsecurity/ransomware-attack-on-blood-testing-service-puts-lives-in-danger-in-south-africa
36 Según los datos aportados por Trend Micro en 2024.
37 https://africacenter.org/spotlight/black-axe-nigeria-transnational-organized-crime
38 https://therecord.media/orion-carbon-black-bec-scam-millions
39 https://www.justice.gov/usao-sdal/pr/nigerian-national-sentenced-ten-years-20-million-cyber-fraud-scheme
40 https://www.justice.gov/usao-sdal/pr/nigerian-national-sentenced-ten-years-20-million-cyber-fraud-scheme

Por cuanto se refiere a los *modus operandi* empleados, los países miembros africanos de INTERPOL señalan que las estafas BEC cometidas en el continente recurren a la ingeniería social, el *phishing*, la suplantación de identidad y las intrusiones en la red para manipular las transacciones financieras. Las órdenes de transferencia fraudulentas son uno de los ardides más comunes: en este caso, los ciberdelincuentes engañan a los empleados haciéndose pasar por ejecutivos, socios comerciales o funcionarios públicos para conseguir que realicen una transferencia de fondos. El fraude del CEO y el fraude de cambio de datos bancarios son las estafas más comunes, sobre todo en el sector público. El *phishing* y el robo de credenciales se utilizan habitualmente para acceder a cuentas, y algunos atacantes recurren a técnicas de ingeniería social basadas en WhatsApp haciéndose pasar por un contacto de la víctima. Los incidentes más avanzados tienen que ver con intrusiones en la red, que consisten en instalar un *malware* con el fin de vigilar los intercambios de correos electrónicos y de intervenir en los procesos de pago. En África Occidental y Austral, los delincuentes suelen utilizar dominios similares o realizar cambios menores en las direcciones de correo electrónico para engañar a las víctimas. También son habituales las estafas relacionadas con presupuestos y pagos, donde los estafadores envían a sus víctimas solicitudes fraudulentas de presupuesto o mensajes en los que les informan de que los datos bancarios han cambiado.

Según la información facilitada por los países miembros de INTERPOL, también parece que la ciberdelincuencia como servicio está favoreciendo la sofisticación de las estafas BEC. La Unidad de Delitos Digitales de Microsoft detectó un aumento del 38 % en la ciberdelincuencia como servicio en relación con cuentas de correo electrónico profesionales entre 2019 y 2022[41]. Ahora, los autores de estas amenazas disponen de kits de *phishing* ya preparados, lo que les permite ampliar el alcance de sus actuaciones de un modo eficiente. Las plataformas ilegales, como BulletProofLink, facilitan aún más la realización de campañas de estafas BEC a gran escala, al ofrecer servicios integrales, como plantillas, servicios de alojamiento y otros servicios automatizados[42]. Asimismo, estas plataformas ayudan a los delincuentes a eludir las medidas de seguridad, como las alertas de «viaje imposible», para aprovechar las IP domésticas.

Además, las estafas BEC impulsadas por la inteligencia artificial son una amenaza emergente. INTERPOL publicó una notificación morada en la que advertía de que los delincuentes estaban haciendo un uso indebido de la IA y la tecnología *deepfake* para perfeccionar las estafas[43]. La IA generativa ayuda a los estafadores a crear unos mensajes de correo electrónicos convincentes y personalizados, que reproducen el estilo y los patrones lingüísticos de personas u organizaciones concretas, mientras que la tecnología *deepfake* ya se está utilizando para suplantar la identidad de ejecutivos en llamadas telefónicas o videollamadas. La rápida evolución de la IA entraña un riesgo significativo al amplificar las estafas BEC y dotarlas de mayor autenticidad, lo que debe ser vigilado de cerca por los países miembros.

2.1.4. Sextorsión digital

La sextorsión digital se enmarca dentro de la categoría de los abusos sexuales basados en imágenes en línea, y es un tipo de delito en el que los autores utilizan imágenes sexualmente explícitas para extorsionar a sus víctimas, a quienes amenazan con difundirlas sin su consentimiento. Las imágenes pueden ser auténticas y haberse obtenido mediante coacción o engaño o haber sido compartidas de manera voluntaria, o pueden haber sido generadas por IA o manipuladas digitalmente[44]. Por lo general, la sextorsión suele producirse por motivos económicos, pero también por venganza o para coaccionar a la víctima.

Los abusos sexuales basados en imágenes en línea, y en particular la sextorsión digital, se han convertido en uno de los ciberdelitos más graves en África en 2024. Los datos facilitados por los países miembros africanos de INTERPOL demuestran un aumento considerable del número de denuncias por sextorsión digital, y más del 60 % de los países indica haber observado una intensificación de este tipo de delito. Esta tendencia probablemente es un reflejo de cambios más amplios en el entorno digital de la región. En vista del elevado porcentaje de casos que no se denuncian, sobre todo cuando se trata de delitos de esta naturaleza, lo más probable es que la verdadera magnitud sea mucho mayor. Y lo que es más importante: los datos actuales no comprenden las denuncias de víctimas de fuera de la región, lo que da a entender que la amenaza podría estar aún más extendida e interconectada a escala internacional de lo que muestran las cifras regionales.

41 Microsoft (2023): https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

42 Informe de INTERPOL de evaluación de las ciberamenazas en África - 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

43 Informe de INTERPOL de evaluación de las ciberamenazas en África - 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

44 https://www.trendmicro.com/vinfo/sg/security/definition/digital-extortion

Las crecientes repercusiones de los abusos sexuales basados en imágenes en línea quedan reflejadas en las últimas medidas de control aplicadas por las principales plataformas. A mediados de 2024, Meta eliminó más de 63 000 cuentas de Instagram y 7 000 perfiles de Facebook relacionados con acciones de sextorsión digital en Nigeria[45] [46]. A pesar de que aún no está claro cuándo fue la primera vez que se detectaron estas cuentas, la magnitud de las acciones sugiere bien un aumento acusado de la actividad delictiva, bien un aumento de la presión externa sobre las plataformas para que actúen. En ambos casos, son indicadores de una intensificación de este tipo de delito. Muchas de estas cuentas estaban vinculadas con redes de ciberdelincuencia organizada, y algunas de ellas se dedicaban a captar y entrenar a futuros delincuentes, así como a distribuir manuales para cometer delitos sexuales digitales[47] [48]. Esto apunta a una evolución táctica: la sextorsión se está convirtiendo en un arma que no se utiliza únicamente de manera aislada, sino como una táctica, una técnica y un procedimiento recurrentes dentro del ecosistema tradicional de las estafas. Algunos datos sugieren también que estas redes pueden estar conectadas con grupos de delincuencia organizada de larga data de África Occidental, si bien es necesario recabar más información para confirmar este punto[49].

Junto con los cambios en la selección de víctimas y la magnitud del delito, han aparecido nuevos vectores de amenazas. Los socios de INTERPOL del sector privado informan de un fuerte repunte de los correos electrónicos de phishing como paso previo a una campaña de sextorsión[50]. Además, han aumentado las extorsiones perfeccionadas mediante IA, en las que se utilizan imágenes explícitas -sintéticas o modificadas- para engañar a las víctimas. Los países en los que se ha registrado el mayor número de incidentes de este tipo son Marruecos, Malí, Egipto y Mauritania, lo que revela la distribución regional. La convergencia de técnicas de *phishing*, herramientas de IA y otras tácticas demuestra cómo la sextorsión se está sistematizando: ya no se trata únicamente de atacantes oportunistas, sino que este delito está cada vez está más arraigado en estructuras más amplias de estafas.

Si bien mucha de la actividad conocida en relación con los abusos sexuales basados en imágenes en línea que ha tenido lugar en las plataformas de Meta ha estado dirigida contra víctimas adultas, los organismos encargados de la aplicación de la ley han alertado de un preocupante aumento del número de casos que afectan a adolescentes de ambos sexos, incluidos algunos de fuera de la región africana[51] [52]. Esta aparente variación en los datos demográficos de las víctimas y en el alcance geográfico, que se está ampliando, puede ser indicativa de un cambio de estrategia. También plantea cuestiones esenciales en torno a las motivaciones que promueven la sextorsión digital. Aunque el objetivo principal es la extorsión económica, habitualmente amenazando con difundir imágenes explícitas, en algunos casos parece que las motivaciones se basan en la manipulación psicológica, las coacciones, o la voluntad de causar un daño reputacional. En estos casos, los delincuentes pueden aprovecharse de las vulnerabilidades de sus víctimas para hacerse con el control, en lugar de para obtener una ganancia económica. Las víctimas sufren un impacto psicológico considerable. En Sudáfrica, las autoridades informaron de un aumento en el número de víctimas adolescentes, mientras que una víctima adulta se suicidó tras un incidente de sextorsión[53]. En Egipto, una plataforma de apoyo digital recibió más de 250 000 denuncias de sextorsión, la mayoría de ellas presentadas por mujeres y niñas[54] [55]. Estas cifras evidencian una crisis latente pero generalizada, en la que los delincuentes explotan a menudo el miedo, el estigma y el malestar emocional como métodos de control.

Para responder a esta creciente amenaza, los organismos africanos encargados de la aplicación de la ley han intensificado sus esfuerzos, también potenciando la coordinación internacional, la cooperación transfronteriza y la colaboración con plataformas del sector privado. Con todo, las limitaciones persistentes de capacidades, las dificultades en materia de competencia jurisdiccional y los retrasos a la hora de acceder a los datos transfronterizos siguen suponiendo una traba para las investigaciones. Dado que tanto los delincuentes como las víctimas trascienden las fronteras nacionales, los marcos de aplicación de la ley experimentan dificultades para seguir el ritmo.

45 https://www.npr.org/2024/07/24/nx-s1-5050709/meta-sextortion-scams-nigeria-facebook-instagram
46 https://www.reuters.com/world/africa/facebook-removes-63000-accounts-nigeria-over-sextortion-scams-2024-07-24/
47 https://tuxcare.com/blog/sextortion-scams-63k-instagram-account-in-nigeria-removed
48 https://www.theverge.com/2024/7/24/24205236/meta-nigeria-financial-sextortion-scam
49 https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook.pdf
50 Según los datos aportados por Trend Micro en 2024.
51 https://www.reuters.com/world/africa/facebook-removes-63000-accounts-nigeria-over-sextortion-scams-2024-07-24/
52 https://businesstech.co.za/news/internet/790431/extortion-syndicates-targeting-boys-in-south-africa
53 https://www.theguardian.com/uk-news/article/2024/aug/21/how-west-africas-online-fraudsters-moved-into-sextortion
54 https://allafrica.com/stories/202408190082.html
55 https://www.reuters.com/article/technology/feature-egyptian-women-find-help-online-to-fight-sextortion-threats

3. TENDENCIAS DE LAS CIBERAMENAZAS Y REFLEXIONES SOBRE SU INCIDENCIA EN LAS DISTINTAS SUBREGIONES AFRICANAS

En el continente africano, las tendencias de las ciberamenazas siguen por lo general un patrón similar, según el cual las estafas por Internet, el *ransomware*, las estafas BEC y la sextorsión digital se consideran las ciberamenazas más graves. Con todo, la naturaleza y la magnitud de estas amenazas varía de una subregión a otra, debido a las diferencias por cuanto se refiere a la infraestructura digital, las capacidades policiales y las tácticas empleadas por los ciberdelincuentes. En este apartado se examinan las tendencias y la evolución en el ámbito cibernético en África Occidental, África Oriental, África Austral, el Norte de África y Africa Central, y se presentan una serie de reflexiones sobre cómo se manifiesta la ciberdelincuencia en cada una de estas regiones.

3.1 África Occidental

- Nigeria, Ghana, Costa de Marfil y Senegal acumulan un alto porcentaje de la economía digital y la actividad cibernética de África Occidental[56].
- Estos países no solo son centros de innovación tecnológica y de servicios financieros, sino también objetivos de gran interés para las ciberamenazas que están transformando el ecosistema general de ciberseguridad de la región.
- Las estafas BEC siguen siendo una de las ciberamenazas más perniciosas desde una perspectiva económica, y los grupos radicados en África Occidental lanzan ataques contra empresas de todo el mundo.
- Los ataques de *ransomware* siguen siendo una de las principales ciberamenazas, en particular aquellos perpetrados siguiendo el modelo *ransomware* como servicio, y se lanzan contra organizaciones africanas para probar nuevos tipos de *malware*[57]. Por lo general, este tipo de ataque se realiza aplicando un modelo de doble extorsión, consistente en cifrar los datos al tiempo que se amenaza a las víctimas con publicar información delicada si no pagan el rescate exigido.
- Los ataques DDoS continúan siendo motivo de gran preocupación en la región. En la primera mitad de 2024, Ghana registró 4 753 incidentes DDoS, los cuales llegaron a alcanzar máximos de 314 Gbps, lo que convierte al país en uno de los principales objetivos de este tipo de ataques en África[58].
- Las estafas con monederos instalados en teléfonos móviles han experimentado un fuerte aumento. Los estafadores aplican tácticas de ingeniería social para secuestrar cuentas y solicitar fondos de emergencia a contactos desprevenidos. Las estafas con dinero móvil, que comprenden el SIM *swapping* (duplicación fraudulenta de la tarjeta SIM) y hacerse pasar por un empleado de una empresa de telecomunicaciones, están muy extendidas, mientras que el robo de identidad favorece el aumento de las estafas relacionadas con inversiones, apuestas y compras por Internet.
- Las estafas sentimentales por Internet están en auge, y las víctimas son chantajeadas con información delicada. Una de las últimas tendencias consiste en que los estafadores atraen en un primer momento a sus víctimas con promesas de amor y, después, las coaccionan para que inviertan dinero en estafas con criptomonedas.

56 https://arxiv.org/html/2402.01649v1
57 https://www.darkreading.com/cyberattacks-data-breaches/criminals-test-ransomware-africa
58 https://toptechgh.com/ghana-hit-with-4753-ddos-attacks-netscout-threat-intelligence-report-1h-2024

3.2 África Oriental

- Los países de África Oriental (Kenia, Uganda, Tanzania, Ruanda y Etiopía) están estableciéndose rápidamente como centros tecnológicos y financieros, y esto insufla un impulso considerable a la transformación digital. Pero estos avances los convierten en objetivos cada vez más atractivos para las ciberamenazas, lo que resalta la necesidad de contar con unos marcos robustos en materia de ciberseguridad.
- Etiopía ha sido el país que más ciberataques recibió de todo el mundo en 2024, y ocupa el primer puesto a escala mundial en detección de malware[59].
- Las infraestructuras esenciales, como las instituciones públicas, los servicios financieros, e importantes proyectos de desarrollo, son un blanco frecuente.
- El SIM *swapping* ha aumentado de manera considerable en Uganda y Tanzania. Los delincuentes se aprovechan de las vulnerabilidades de las redes móviles adquiriendo tarjetas SIM de sustitución, a menudo mediante engaños o con la connivencia de personas de una empresa con acceso legítimo a información interna, lo que les permite secuestrar el número de teléfono de sus víctimas.
- La sextorsión digital es una ciberamenaza en auge en África Oriental. A menudo, los delincuentes utilizan material comprometedor para extorsionar a sus víctimas, en particular a mujeres y jóvenes.

3.3 África Central

- Los ciberataques lanzados en África Central suelen aprovecharse de la protección deficiente de las infraestructuras y de unos sistemas obsoletos.
- Entre los ciberdelitos denunciados con mayor frecuencia siguen figurando las estafas de ingeniería social, en las que los delincuentes utilizan determinadas artimañas, como oportunidades falsas de empleo y estafas sentimentales por Internet, para aprovecharse de víctimas desprevenidas.
- Las instituciones financieras son cada vez más vulnerables a las estafas BEC y las intrusiones en la red. Camerún y Gabón han informado de un aumento significativo de los ciberataques lanzados contra las instituciones financieras, que han ocasionado importantes pérdidas económicas.

3.4 África Austral

- África Austral es conocida por disponer de uno de los ecosistemas de ciberseguridad más avanzados del continente, donde países como Sudáfrica, Namibia y Botsuana realizan importantes inversiones para concienciar en materia de ciberseguridad, elaborar unos marcos jurídicos exhaustivos y dotarse de tecnologías de seguridad basadas en la IA.
- Los ciberdelincuentes han adoptado herramientas basadas en la IA para crear sofisticadas suplantaciones ultrafalsas de voz y vídeo, lo que en 2024 provocó un aumento considerable del número de ataques de *vishing* que imitaban a directores generales y proveedores[60].
- La ingeniería social sigue siendo una de las tácticas más habitualmente empleadas en muchos incidentes cibernéticos, y a menudo se utiliza como punto de partida del ataque. Los ataques de *phishing* por SMS (*smishing*) se lanzan específicamente contra clientes bancarios, para lo que se envían mensajes engañosos con el fin de comprometer las cuentas de usuarios.
- Los ciberdelincuentes de África Austral aprovechan cada vez más las nuevas tendencias en el ámbito de las tecnofinanzas, como la banca digital y las criptomonedas. El *cryptojacking* aumenta progresivamente, y las instituciones financieras informaron de que este tipo de incidentes había aumentado considerablemente a lo largo de 2024.

59 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024/

60 https://qtatech.com/en/article/why-are-cyberattacks-increasingly-targeting-african-financial-institutions?srsltid=AfmBOoqghmt5QRlVko-UqiSdks8zjt99y1nHYR24zzh1vf63gxMYTk2a

3.5 Norte de África

- En 2024, los países del Norte de África, como Egipto, Argelia, Marruecos, Túnez y Libia, se enfrentaron a un panorama de ciberamenazas cada vez más complejo, influido por las tendencias globales en materia de ciberdelincuencia y la dinámica geopolítica regional.
- Egipto y Marruecos fueron los países de África que más ataques recibieron, debido a la amplia penetración de Internet en sus territorios y a su condición de grandes economías. Egipto acumuló aproximadamente el 13 % de todos los ciberataques lanzados en el continente en 2024, y ocupa el segundo lugar después de Sudafrica.[61]
- La ingeniería social sigue siendo el sostén de muchos incidentes cibernéticos ocurridos en el Norte de África, que abarcan desde estafas básicas hasta ataques altamente sofisticados. Las empresas fueron un blanco común de los correos electrónicos de *phishing* redactados en el idioma local para aumentar su autenticidad. Las estafas de la lotería y las inversiones son los delitos más frecuentes; se han denunciado muchos casos relacionados con mensajes de WhatsApp que prometen un premio fraudulento u oportunidades de inversión fraudulentas en criptomonedas.

ÁFRICA CENTRAL	ÁFRICA ORIENTAL	NORTE DE ÁFRICA	ÁFRICA AUSTRAL	ÁFRICA OCCIDENTAL
El bajo nivel de cultura digital y una débil infraestructura dejan a la región en una posición vulnerable. • En Camerún los ciberincidentes casi se multiplicaron por dos en 2024. • Las estafas con criptomonedas y con ingeniería social van en aumento. • Las entidades financieras se enfrentan a un número creciente de estafas BEC y de ataques contra las redes, pero la mayoría de los casos no se resuelven debido a una capacidad limitada en materia de ciberseguridad.	La expansión digital evoluciona a un ritmo más rápido que la preparación en materia de ciberseguridad. • En 2024 Etiopía ocupó el primer puesto a escala mundial por el número de detecciones de *malware*, cuyos ataques pusieron en peligro infraestructuras esenciales. • Las estafas de SIM *swapping* van en aumento en Uganda y Tanzania. • La sextorsión y el acoso en línea, especialmente dirigidos contra las mujeres y los jóvenes, son un fenómeno cada vez más común.	En 2024 los ciberataques experimentaron un brusco aumento, impulsados por la tensión geopolítica y la expansión digital. • Egipto y Marruecos figuraron entre los países africanos más afectados, produciéndose en Egipto un 13 % de todos los ataques. • Las estafas mediante ingeniería social y *phishing*, perpetradas a menudo a través de WhatsApp y de inversiones falsas, están muy extendidas.	Región de África en la que la ciberseguridad está más desarrollada, pero que se encuentra todavía asediada por la ciberdelincuencia. • En 2024 se dispararon los casos de *deepfakes* y *vishing* basados en la IA. • Sudáfrica sigue siendo un objetivo destacado de los delincuentes, en particular en el ámbito de las finanzas y de la Administración. • Los ataques de *cryptojacking* y *smishing*, que se aprovechan de la expansión de las tecnofinanzas, están muy extendidos.	La rápida expansión de los servicios digitales -especialmente el dinero móvil y los medios sociales- ha hecho de África Occidental un punto crítico de la ciberdelincuencia. • Las estafas BEC y los ataques con *ransomware* son los delitos predominantes, y varios grupos radicados en Nigeria, como Black Axe y Operaǝr, son líderes mundiales en el ámbito de las estafas. • A principios de 2024 Ghana registró cerca de 5 000 ataques DDoS, que se centraron en gran medida en el sector de las telecomunicaciones. • Las estafas con monederos instalados en teléfonos móviles y las estafas sentimentales por Internet van en aumento, a menudo en relación con tramas de criptomonedas falsas. • El *phishing* potenciado por la IA y los *deepfakes* son amenazas crecientes.

Cuadro 1: Panorama de las tendencias de las ciberamenazas y reflexiones sobre su incidencia en las distintas subregiones africanas.

61 https://global.ptsecurity.com/analytics/cybersecurity-threatscape-for-african-countries-q1-2023-q3-2024

4. RETOS A LA HORA DE COMBATIR LA CIBERDELINCUENCIA EN ÁFRICA

4.1 Marcos jurídicos y normativos fragmentados

La ciberdelincuencia avanza más rápido que los sistemas jurídicos concebidos para acabar con ella. El 65 % de los países informa de que el año pasado sus legislaciones en materia de ciberdelincuencia no se actualizaron, y más del 75 % de los países considera que sus marcos jurídicos y sus capacidades de investigación han de ser mejoradas, lo que indica claramente que existen vacíos legales de carácter sistémico[62].

Para hacer frente a estos retos, existen varios instrumentos internacionales y regionales que ofrecen un marco para reforzar la legislación en materia de ciberdelincuencia:

- **Convenio de Budapest sobre la Ciberdelincuencia[63]:** Ofrece unas directrices exhaustivas, como el artículo 19, que describe las facultades para el acceso y la incautación de datos. Hasta la fecha, solo seis países africanos lo han ratificado.
- **Convención de las Naciones Unidas contra la Ciberdelincuencia[64]:** Tiene por finalidad reforzar la cooperación internacional para combatir la ciberdelincuencia y está recibiendo un apoyo cada vez mayor en África.
- **Convención de Malabo de la Unión Africana[65]:** Dedicada a la ciberseguridad y la protección de los datos personales. Con todo, hasta la fecha tan solo ha sido ratificada por quince Estados miembros de la Unión Africana.

Estas lagunas resaltan la creciente necesidad de armonización con los marcos jurídicos internacionales, una cuestión que se aborda con mayor detalle en el capítulo 6.

4.2 Limitaciones en materia de capacidades y competencias

Unas leyes estrictas son solo parte de la solución; la mayoría de los países también tienen dificultades para aplicarlas. Según los resultados de la encuesta, el **90 % de los países que han respondido** afirman que sus capacidades policiales o de investigación han de ser mejoradas ligera o considerablemente.

Estas son algunas de las limitaciones más comunes:

- **Necesidades en materia de formación:** El 95 % indica que la formación es inadecuada, irregular o que depende de donantes.
- **Limitaciones en materia de recursos:** 95 % de los países.
- **Acceso a herramientas especializadas:** 95 % de los países.
- **Lagunas en competencias técnicas:** 74 % de los países.
- **Lagunas en infraestructuras:** 72 % de los países.
- **Barreras operacionales:** El 58 % se topa con obstáculos de índole burocrática, jurídica o institucional que impiden que las investigaciones sean eficientes.

A pesar del aumento del número de casos, la mayoría de los países siguen careciendo de la infraestructura esencial para combatir la ciberdelincuencia:

- **Un 30 %** dispone de un sistema para denunciar incidentes.
- **Un 28 %** utiliza un sistema de gestión de casos.
- **Un 19 %** dispone de una base de datos de información policial sobre ciberamenazas.
- **Un 29 %** lleva un repositorio de pruebas digitales.

Además, existen pocas instituciones nacionales dotadas del personal o el equipamiento necesarios para reaccionar en tiempo real. Las tecnologías basadas en la nube utilizadas para la comisión de delitos, las plataformas de cifrado de mensajes y las investigaciones internacionales a menudo superan el alcance técnico y procedimental de los equipos nacionales.

62 Encuesta de INTERPOL de evaluación de las ciberamenazas

63 https://www.coe.int/en/web/cybercrime/the-budapest-convention

64 https://www.unodc.org/unodc/es/cybercrime/convention/text/convention-full-text.html

65 Convenio de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (Convenio de Malabo) https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

4.3 Amenazas emergentes y tácticas cambiantes

Un porcentaje cada vez más alto de los ciberdelitos cometidos en África utiliza nuevas herramientas y tácticas, en particular aquellas que recurren a la IA, los medios sintéticos y la desinformación. Estas amenazas cambiantes avanzan a un ritmo más rápido que el de la capacidad de muchos organismos nacionales para detectarlas, investigarlas o contenerlas.

- ***Deepfakes* generados con la IA y extorsión**

  En varios países los delincuentes han utilizado vídeos falsos o han clonado voces para extorsionar a sus víctimas. Estas herramientas basadas en la IA permiten realizar suplantaciones de identidad convincentes, manipulación emocional y chantaje, y, además, no suele ser necesario tener unas habilidades técnicas avanzadas para utilizarlas.
- **Campañas de desinformación**

  Algunos organismos han informado de casos en los que se han utilizado noticias falsas, imágenes manipuladas y cuentas falsas de medios sociales para sembrar el pánico, provocar disturbios o dañar la reputación. Estos ataques están dirigidos por lo general contra la confianza, y utilizan como arma los canales de información pública.
- **El auge de las infraestructuras de ataque preconfiguradas**

  Cada vez es más habitual utilizar servicios de alojamiento *bulletproof* como complemento de las soluciones de ciberdelincuencia como servicio, gracias a lo cual los delincuentes poco cualificados tienen acceso a kits de *phishing*, cargas maliciosas y a una automatización escalable alojada en una infraestructura diseñada para evitar su eliminación.

A pesar de la rápida evolución de estas amenazas, el 86 % de los organismos encuestados no han incorporado todavía la IA a sus actuaciones policiales[66]. Mientras los atacantes aprovechan la IA para ampliar el alcance de sus actividades y perfeccionar sus engaños, muchos organismos nacionales corren el riesgo de quedarse atrás como consecuencia de esta deficiencia en materia de capacidades.

4.4 Limitaciones de la cooperación transfronteriza y el intercambio de información policial

La ciberdelincuencia traspasa las fronteras de manera habitual, si bien la mayoría de los países africanos encuentran dificultades para colaborar a escala internacional. De acuerdo con las respuestas aportadas a nuestra encuesta, el 86 % de los organismos sostiene que sus capacidades en materia de cooperación transfronteriza necesitan mejorar y el 44 % indica que necesitan mejorar considerablemente.

Se ha informado de varias limitaciones importantes:

- **Lentitud de las actuaciones oficiales:** La tramitación de actuaciones como las solicitudes de asistencia judicial recíproca o de extradición es a menudo demasiado lenta con respecto a la diligencia exigida para reaccionar eficazmente a los delitos cibernéticos, lo que pone de manifiesto la necesidad de adoptar unos marcos de cooperación más flexibles y racionalizados.
- **Diferencias jurídicas y procedimentales:** Cuando se trabaja con distintos países, las diferencias en materia de legislación, normativa sobre pruebas digitales y reglamentos sobre la privacidad de los datos generan fricciones. Estas cuestiones jurídicas se abordan con mayor detalle en el apartado 4.1.
- **Creación de redes operativas y generación de confianza:** Algunos países tienen dificultades para saber quiénes son sus homólogos extranjeros o para ponerse en contacto con ellos, y en ocasiones la comunicación establecida o los marcos de coordinación en tiempo real son limitados, lo que a veces puede provocar que se pierdan oportunidades para actuar de manera conjunta.
- **Acceso limitado a plataformas y datos alojados en el extranjero:** Los organismos indican tener dificultades para obtener información de plataformas o proveedores de servicios con sede en el extranjero, en particular cuando se trata de casos en los que están implicados ciudadanos de otras nacionalidades o en los que intervienen infraestructuras radicadas en otros países.

A pesar de estas barreras, las últimas operaciones coordinadas en el marco del proyecto AFJOC de INTERPOL evidencian que, cuando existen unos conductos fiables y unos protocolos conjuntos, la reacción regional a los delitos cibernéticos puede ser rápida y eficaz.

66 Encuesta de INTERPOL de evaluación de las ciberamenazas.

4.5 Obstáculos para la creación de alianzas público-privadas y responsabilidad de las plataformas:

En las investigaciones de delitos cibernéticos es cada vez más habitual recurrir a la cooperación con socios del sector privado, y en particular a plataformas tecnológicas, proveedores de telecomunicaciones, e instituciones financieras. Con todo, la mayoría de los organismos africanos encargados de la aplicación de la ley se encuentran con importantes obstáculos a la hora de forjar estas relaciones.

- **Conductos de interacción poco definidos:**

  A menudo, a los organismos les resulta complicado obtener acceso a datos de empresas como Meta, TikTok y Snapchat y hacen alusión a la falta de contactos directos, unos tiempos de respuesta lentos y la poca claridad de los procedimientos existentes. Al no existir acuerdos oficiales o puntos de contacto, lo habitual es que las peticiones experimenten retrasos o sean ignoradas.
- **Escasa preparación institucional:**

  Son pocos los países que han suscrito con empresas privadas un memorando de entendimiento o un acuerdo para el intercambio de datos. De igual modo, muchos organismos carecen de las capacidades técnicas o jurídicas para formular unas peticiones efectivas y legítimas.
- **Falta de compromiso por parte de los sectores de las telecomunicaciones y las tecnofinanzas:**

  A pesar de que los proveedores de telecomunicaciones y de servicios financieros tienen un rol preeminente en el ámbito del fraude y las estafas -como el SIM *swapping* o el uso indebido del dinero móvil-, en las estrategias nacionales sobre ciberdelincuencia apenas se cuenta con ellos.

→ Según los datos consignados en el cuestionario, el 89% de los países africanos consideran que su cooperación con el sector privado necesita mejorar considerable o ligeramente[67].

A medida que aumenta el número de infraestructuras digitales bajo el control de entidades privadas, la capacidad de actuación de las fuerzas del orden va a depender cada vez más de factores como la obtención de acceso, la generación de confianza y una cooperación estructurada, ninguno de los cuales puede dejarse al azar.

67 Encuesta de INTERPOL de evaluación de las ciberamenazas.

5. CAMBIOS POSITIVOS EN EL PANORAMA DE LA CIBERSEGURIDAD EN ÁFRICA

África ha progresado considerablemente en el ámbito de la ciberseguridad, gracias a las reformas jurídicas, los avances en materia forense, las iniciativas para concienciar a la sociedad, la cooperación regional, y la adopción de nuevas tecnologías. Estos avances evidencian su creciente compromiso con la lucha contra la ciberdelincuencia y el refuerzo de la seguridad digital en todo el continente.

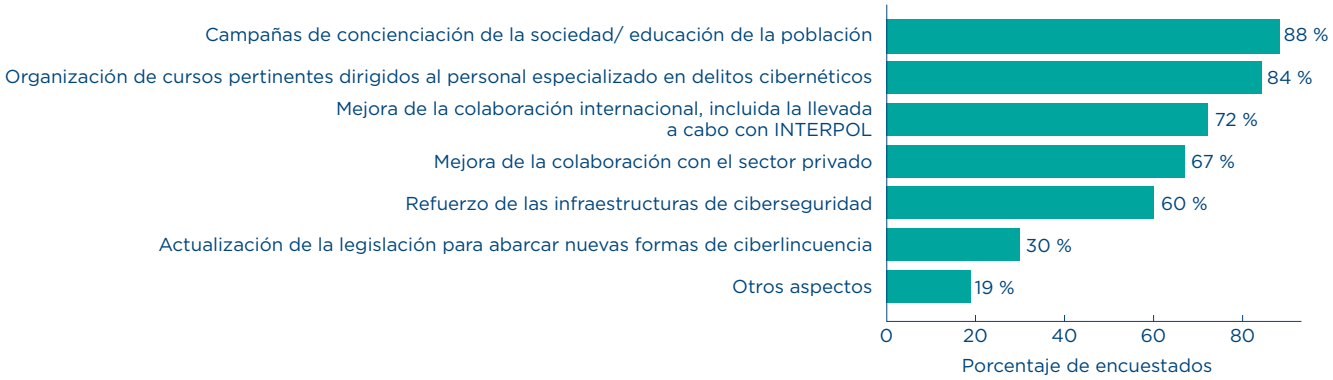


Gráfico 8: Medidas para prevenir la ciberdelincuencia adoptadas por los organismos africanos encargados de la aplicación de la ley en 2024.

5.1 Refuerzo de los marcos nacionales en materia de ciberdelincuencia

En 2024, varios países africanos actualizaron sus marcos jurídicos para combatir la ciberdelincuencia, lo que es ilustrativo de un compromiso creciente con la seguridad digital.

- **Túnez** se convirtió en marzo de 2024 en el septuagésimo país ensuscribir el Convenio de Budapest sobre la Ciberdelincuencia, y armonizó su ordenamiento jurídico con la normativa internacional para facilitar la cooperación transfronteriza a la hora de luchar contra los delitos cibernéticos.
- **Nigeria** promulgó la ley sobre ciberdelincuencia (represión, prevención, etc.) (modificada) de 2024, por la que actualizó la ley de 2015 en esta materia. Entre las principales modificaciones destacan la creación de unos equipos sectoriales de respuesta ante emergencias informáticas, la clarificación de las disposiciones sobre ciberacoso, y la introducción de un impuesto sobre ciberseguridad para financiar iniciativas nacionales[68].
- **Gambia** presentó ante el Parlamento su primera ley específica en materia de ciberdelincuencia (2023), lo que constituye un paso fundamental hacia la formalización de su planteamiento para combatir la ciberdelincuencia[69].
- **Guinea-Bisáu** elaboró su estrategia nacional en materia de ciberseguridad en 2024[70]; también ha logrado avanzar significativamente en su labor general de transformación digital En enero de 2025 el Gobierno presentó oficialmente la estrategia nacional para la transformación digital, concebida con la finalidad de mejorar el desarrollo económico, la gestión de los datos, la gobernanza, y los servicios públicos[71].
- **Burkina Faso** aprobó la ley n.º 014-2024/ALT en julio de 2024, por la que se introducen mejoras en la protección de los sistemas informáticos y el cifrado de las respuestas a las ciberamenazas, como el *ransomware* y las estafas por Internet[72].

Estos esfuerzos legislativos son indicativos de que la región está predispuesta a armonizar la legislación en materia de ciberseguridad con la normativa internacional, que comprende el Convenio de Budapest y la Convención de las Naciones Unidas contra la Ciberdelincuencia.

68 https://placng.org/i/documents/cybercrimes-prohibition-prevention-etc-amendment-act-2024/
69 https://mocde.gov.gm/ministry-of-communications-and-digital-economy-of-the-gambia-embarked-on-a-two-day-retreat-to-discuss-the-cybercrime-bill-2023/
70 Encuesta de INTERPOL de evaluación de las ciberamenazas.
71 https://unu.edu/egov/news/digital-transformation-project-guinea-bissau-egov-undp
72 https://www.mdenp.gov.bf/fileadmin/user_upload/storages/documents/administratifs/loi_014_systeme_d_information.pdf

5.2 Ampliación de las capacidades institucionales y técnicas

En los últimos 18 meses, los países africanos han realizado avances significativos hacia la mejora de sus capacidades para reaccionar a los delitos cibernéticos. La inversión en unidades especializadas e infraestructuras digitales forenses y el desarrollo de capacidades han sido determinantes a la hora de reforzar las investigaciones y la aplicación de la ley.

- Según las respuestas aportadas a la encuesta[73], **el 67 %** de los países participantes indican haber organizado en 2024 iniciativas de capacitación en el ámbito de los delitos cibernéticos, mientras que el **44 %** informa de la creación de unidades de ciberdelincuencia o la ampliación de las unidades existentes en este ámbito.
- **Argelia:** A finales de 2023, Argelia inauguró una nueva sede nacional para su unidad central de ciberdelincuencia y amplió las operaciones a sus 58 provincias. Ahora, las unidades están organizadas por funciones (vigilancia, apoyo técnico e investigaciones), lo que agiliza las actuaciones policiales. La formación continua refuerza estas reformas estructurales[69] [74].
- **Seychelles:** Los servicios policiales de Seychelles han recibido un paquete de herramientas digitales y equipos de formación, que han sido ofrecidos por el Gobierno británico[75], y un laboratorio forense digital, donado por el Gobierno chino[76], y todo esto en los últimos 18 meses, poco después de haber creado en 2023[77] la unidad especializada en ciberdelincuencia. La finalidad es que estas nuevas herramientas ayuden a perfeccionar las investigaciones de delitos cibernéticos y mejoren la calidad del tratamiento de las pruebas digitales.
- **Benín:** El Gobierno creó el Centro Nacional de Ciberdelincuencia (Centre National d'Investigations Numériques, CNIN) con la finalidad de centralizar todas las investigaciones de delitos cibernéticos y las actividades de criminalística forense[78]. En agosto de 2024, el CNIN anunció la desarticulación de una de las principales redes de ciberdelincuencia en Comè, lo que demuestra su eficacia operativa[79].
- **Togo:** De acuerdo con su estrategia nacional sobre ciberseguridad para el periodo de 2024 a 2028, Togo está consolidando sus actuaciones frente a la ciberdelincuencia creando una entidad unificada de control[80], ha abierto un nuevo laboratorio forense digital[69] y sigue invirtiendo en formación técnica para sus investigadores.
- **Congo:** A finales de 2024, el Gobierno organizó un curso especializado dirigido a miembros de la judicatura y las fuerzas del orden, en el que se trataron cuestiones tales como la recogida de pruebas y las técnicas de investigación de delitos cibernéticos[81].

Estos avances son ilustrativos de un cambio de mayor calado en todo el continente, el cual ha pasado de responder de una manera fragmentada o puntual a los ciberdelitos a luchar contra ellos de un modo más estructurado, con mejores recursos y apoyándose cada vez más en la tecnología. La inversión continua en infraestructura, la capacitación del personal policial y la coordinación interinstitucional serán clave para sostener e incrementar estos avances.

73 Encuesta de INTERPOL de evaluación de las ciberamenazas.
74 https://www.horizons.dz/?p=74105
75 http://www.seychellesnewsagency.com/articles/19082/British+government+donates+digital+tech+to+Seychelles+Police+Force+for+better+training+and+results
76 http://www.seychellesnewsagency.com/articles/19616/China+gifts+Seychelles+Police+Force+digital+forensic+lab+to+help+deal+with+cybercrime
77 https://www.nation.sc/articles/16639/cybercrime-unit-in-the-offing--by-vidya-gappy
78 https://cybersecuritymag.africa/benin-renforce-lutte-contre-cybercriminalite-avec-creation-du-cnin
79 https://cybersecuritymag.africa/index.php/le-cnin-demantele-un-vaste-reseau-de-cybercriminels-come-au-benin
80 https://www.togofirst.com/en/justice/2805-14118-togo-to-set-up-single-center-to-fight-cybercrime
81 https://www.wearetech.africa/en/fils-uk/news/tech/congo-hosts-cybersecurity-training-for-judicial-and-law-enforcement

5.3 Potenciar la capacidad de adaptación cibernética mediante iniciativas de concienciación ciudadana

El 88 % de los países africanos indican haber organizado en 2024 campañas de sensibilización o iniciativas educativas para prevenir la ciberdelincuencia, que pasan a ser la medida de prevención más extendida de todo el continente.

Por lo general, estas iniciativas están dirigidas a los grupos más vulnerables (como los estudiantes, los jóvenes, los propietarios de pequeñas empresas y ciudadanos sénior) y para su ejecución se utilizan diversos métodos de comunicación, como la radio y la televisión nacionales, los medios sociales, las alertas por SMS y las actividades escolares.

1. Campañas escolares y para jóvenes
Uno de los objetivos estratégicos de muchos países sigue siendo dirigirse a los sectores más jóvenes de población para promover la seguridad en línea, concienciar sobre el ciberacoso, e impulsar la cultura digital.

- **Esuatini:** El Ministerio de Tecnologías de la Información y la Comunicación, con la colaboración de la Comisión de Comunicaciones de Esuatini y la UNESCO, organizó en los colegios varias sesiones informativas sobre ciberseguridad[82] [83] [84].
- **Sudáfrica:** El Instituto de Profesionales de las Tecnologías de la Información de Sudáfrica (IITPSA, por sus siglas en inglés), por conducto de su Grupo de interés especial por la ciberseguridad (SIGCyber), organizó en Puerto Elizabeth el primer tribunal simulado sobre ciberseguridad. Los estudiantes de secundaria presentaron sus argumentos sobre un caso ficticio de ciberacoso ante un tribunal de jueces, con el objetivo de profundizar su comprensión sobre los daños digitales y las soluciones normativas en el ámbito escolar[85].
- **Marruecos:** Los servicios policiales han organizado programas informativos en las escuelas en colaboración con el Ministerio de Educación, y, en mayo de 2024, más de 2,1 millones de personas asistieron a la jornada de puertas abiertas de la Dirección General de la Seguridad Nacional en Agadir, en la que se organizaron exposiciones sobre delitos cibernéticos, participaron estudiantes de 845 colegios y se presentó la plataforma E-Blagh para denunciar delitos cibernéticos.[86] [87]
- Las organizaciones de la sociedad civil, como Child Online Africa[88] y Better Internet for Kids[89], organizan iniciativas (como el día de la seguridad en Internet en África, el concurso sobre seguridad y bienestar en línea y la semana de la cultura digital) dirigidas a colegios, padres, e instituciones religiosas.

2. Participación de los medios de comunicación de masas y los medios sociales
A fin de maximizar el alcance de sus iniciativas, los países recurren cada vez más a las plataformas de medios sociales y tradicionales para difundir mensajes de prevención de los delitos cibernéticos.

- **Ghana:** En octubre de 2024, la autoridad de ciberseguridad inauguró el mes nacional de la concienciación sobre la ciberseguridad bajo el lema «Combatir la información errónea y la desinformación en una democracia digital resiliente - Nuestra responsabilidad colectiva». Esta iniciativa consistió en una campaña mediática a escala nacional, la organización de foros regionales y actividades de educación pública para fomentar la resistencia digital antes de las elecciones nacionales[90].
- **Ruanda:** En el mes de octubre de 2024 la autoridad nacional de ciberseguridad llevó adelante la campaña anual «Tekana Online». Esta iniciativa utilizó la televisión, la radio y los medios sociales para instruir a las personas, las familias y las organizaciones sobre las mejores prácticas contra las ciberamenazas como las estafas en línea, el *ransomware* y el *phishing*[91].
- **INTERPOL:** En diciembre de 2024, INTERPOL lanzó la campaña #ThinkTwice en sus plataformas de medios sociales. El objetivo de la campaña era concienciar sobre las amenazas en Internet (como el *ransomware*, el *phishing* y las estafas con IA generativa) y animar a los usuarios a tomar decisiones informadas en línea[92].

82 https://independentnews.co.sz/10470/local-news/cybersecurity-awareness-initiative-hits-schools/
83 https://www.facebook.com/story.php?id=100069400350741&story_fbid=850193827303955&
84 https://www.swazilandnews.co.za/fundza.php?nguyiphi=7578&
85 https://www.itweb.co.za/article/iitpsa-sigcyber-raises-awareness-on-cyber-bullying-at-inaugural-moot-court-event/6GxRKqYQrnmqb3Wj
86 https://www.mapnews.ma/fr/actualites/social/jpo-de-la-dgsn-un-nombre-record-de-2120000-visiteurs
87 https://en.hespress.com/85374-moroccan-police-launches-new-platform-e-blagh-to-combat-cybercrime.html
88 https://www.childonlineafrica.org/
89 https://better-internet-for-kids.europa.eu/en/saferinternetday/supporter-listing/africa-safer-internet-day
90 ncsam.csa.gov.gh
91 https://cyber.gov.rw/updates/article/ncsa-launches-cybersecurity-and-data-protection-awareness-campaign/
92 https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Una-campana-de-INTERPOL-alerta-sobre-la-ciberdelincuencia-y-otros-delitos-financieros

3. Concienciación comunitaria y compromiso cultural

Las campañas localizadas que emplean el idioma y los canales culturales conocidos son especialmente eficaces en las comunidades rurales y desatendidas.

- **Chad:** Las autoridades de Yamena crearon unos programas informativos sobre delitos cibernéticos en los que participaron artistas locales y emisoras privadas de radio. Se trata de una decisión estratégica en un país con unos índices de alfabetización dispares, donde muchas comunidades se comunican oralmente. Se emplearon las lenguas locales y mensajes culturalmente familiares para instruir a los residentes sobre las estafas en línea, lo que ayudó a llegar a comunidades a las que no se puede acceder fácilmente por medio de contenidos escritos o digitales[93].
- **República Democrática del Congo:** Cada mes, los servicios policiales organizan actos públicos para devolver los teléfonos robados a sus propietarios legítimos. Esta iniciativa, organizada en colaboración con el organismo regulador nacional de telecomunicaciones y el Ministerio Fiscal, se ha difundido ampliamente y su finalidad es desincentivar la compra de teléfonos de segunda mano. Estos dispositivos suelen estar relacionados con algún tipo de ciberdelito, como la suplantación de identidad, la extorsión, o la difamación. La campaña ha ayudado considerablemente a concienciar a la población y ha contribuido a reducir la incidencia de estos delitos[93].

4. Canales de distribución institucionales e intersectoriales

Algunas de las campañas de sensibilización más extendidas de África se organizan por conducto de estructuras coordinadas en las que participan diversos ministerios, organismos encargados de la aplicación de la ley y grupos de la sociedad civil. Estas alianzas institucionales aumentan el alcance, la coherencia de los mensajes y la credibilidad.

- **Argelia:** Las unidades argelinas especializadas en la lucha contra la ciberdelincuencia han colaborado estrechamente con el Ministerio de Educación, el Ministerio de Correos y Telecomunicaciones y las organizaciones de la sociedad civil para lanzar campañas de sensibilización. Estas iniciativas han estado dirigidas a diversos públicos, y se han llevado adelante periódicamente en varias plataformas, como la radio, la televisión, los medios sociales, los foros públicos y los anuncios. Las autoridades han verificado su eficacia controlando las interacciones en medios sociales, siguiendo el aumento de las denuncias de ciberdeiltos y verificando la adopción generalizada de conductas preventivas por parte de la ciudadanía.

5.4 Refuerzo de las operaciones policiales

En 2024, los países africanos evidenciaron el aumento de su capacidad operativa y de la cooperación internacional, en particular a través de dos operaciones de alto nivel contra la ciberdelincuencia coordinadas por INTERPOL.

- **La operación Serengeti** , llevada a cabo entre septiembre y octubre de 2024, es hasta la fecha una de las actuaciones policiales más importantes acometidas en el continente contra la ciberdelincuencia. Estuvo coordinada por INTERPOL y AFRIPOL, y en ella participaron 19 países africanos. Se saldó con más de 1 000 detenciones, el desmantelamiento de 134 000 infraestructuras en línea maliciosas y la identificación de más de 35 000 víctimas. Las autoridades investigaron a operadores de *ransomware*, autores de estafas BEC, extorsionadores digitales y redes especializadas en estafas de inversión. Se estima que las pérdidas económicas relacionadas con las tramas delictivas desarticuladas en el marco de la operación ascienden a 193 millones de dólares estadounidenses a escala global. Los socios del sector privado, entre ellos varios proveedores de servicios de Internet, brindaron su apoyo a la operación ayudando con el cierre de infraestructuras y la protección de plataformas digitales[94].
- **La operación Red Card**, llevada a cabo entre octubre de 2024 y marzo de 2025 en el marco del proyecto AFJOC, reunió a las unidades especializadas en ciberdelincuencia de Costa de Marfil, Benín, Togo, Ruanda, Sudáfrica, Zambia y Nigeria. Logró desarticular una red dedicada a las estafas de préstamos en línea analizando dominios, archivos APK y perfiles de medios sociales. La información aportada por el sector privado nutrió los informes sobre ciberdelincuencia, que fueron fundamentales para detectar las infraestructuras delictivas e identificar a los autores de las amenazas[95].

Combinadas, estas operaciones ponen de manifiesto la creciente capacidad de los países africanos para participar en complejas investigaciones transfronterizas sobre ciberdelincuencia, facilitadas por una coordinación más estrecha, unos marcos de intercambio de información policial más sólidos y una colaboración público-privada más activa.

93 Encuesta de INTERPOL de evaluación de las ciberamenazas

94 https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Una-operacion-importante-contra-la-ciberdelincuencia-permite-detener-a-1-006-sospechosos

95 https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2025/Mas-de-300-personas-detenidas-en-una-operacion-de-los-paises-africanos-para-poner-un-alto-a-las-ciberamenazas

6. RECOMENDACIONES Y CONCLUSIONES

Para atajar las amenazas, las deficiencias de capacidades y los retos sistémicos señalados en esta evaluación, INTERPOL propone las siguientes recomendaciones estratégicas a los organismos encargados de la aplicación de la ley, los responsables de la elaboración de políticas, los organismos regionales y los socios internacionales. Estas recomendaciones están basadas en los comentarios de los países miembros, la información operativa y las tendencias observadas, y su finalidad es servir de orientación para la aportación de unas mejoras sostenibles, prácticas y coordinadas a la capacidad de respuesta de África frente a los delitos cibernéticos.

Las recomendaciones se han organizado en seis ámbitos temáticos:

- Refuerzo de las capacidades nacionales
- Mejora de los marcos jurídicos y normativos
- Mejora de la cooperación regional e internacional
- Ampliación del alcance de la prevención y la sensibilización
- Consolidación de las alianzas público-privadas
- Utilización de las nuevas tecnologías para prevenir la ciberdelincuencia

6.1 Refuerzo de las capacidades nacionales

Los organismos africanos encargados de la aplicación de la ley han de recibir apoyo para desarrollar unas capacidades operativas, técnicas, e institucionales que les permitan detectar, investigar y neutralizar eficazmente los delitos cibernéticos. A pesar de que muchos países han realizado avances, aún existen disparidades en el continente. A continuación se enumeran algunos de los ámbitos prioritarios:

- creación y ampliación a escala nacional de unidades especializadas en ciberdelincuencia, dotadas de personal suficiente, un cometido y recursos técnicos;
- inversión en cursos sobre delitos cibernéticos dirigidos a investigadores, analistas, fiscales y jueces, que cubran, entre otros, los ámbitos de la criminalística digital, el análisis de *malware*, la inteligencia de fuentes abiertas y el seguimiento de flujos financieros;
- garantía de un acceso duradero a herramientas modernas de investigación, como *software* de criminalística digital con licencia y un almacenamiento seguro de pruebas digitales;
- creación y puesta en funcionamiento de equipos nacionales y sectoriales de respuesta a incidentes informáticos, dotados de protocolos claros para la coordinación interinstitucional;
- retención de funcionarios especializados en ciberdelincuencia ofreciéndoles unas trayectorias y unos incentivos profesionales claros, a fin de reducir la fuga de talento y garantizar la eficacia a largo plazo.

La inversión sostenida en capacidades nacionales es la base de un ecosistema eficaz y autónomo de respuesta a los delitos cibernéticos.

6.2 Mejora de los marcos jurídicos y normativos

Las actuaciones para combatir eficazmente los delitos cibernéticos dependen de la existencia de unos marcos jurídicos sólidos, actualizados y aplicables. Con todo, muchos países africanos siguen lidiando con lagunas normativas que limitan sus capacidades para perseguir a los ciberdelincuentes, acceder a pruebas que se encuentran fuera de sus territorios, o cooperar a escala internacional.

Para atajar estas cuestiones, INTERPOL recomienda:

- agilizar la aprobación y la aplicación de unas leyes nacionales exhaustivas en materia de ciberdelincuencia, armonizadas con las normas internacionales y que traten sobre los delitos dependientes del entorno cibernético y los delitos facilitados por Internet;
- garantizar el reconocimiento legal y la admisibilidad de las pruebas digitales, incluidas las recogidas en otros países;
- armonizar las definiciones y los procedimientos jurídicos de los distintos países, para reducir la fragmentación jurídica y potenciar la eficacia de la cooperación regional;
- ratificar y aplicar los convenios internacionales y regionales, como el Convenio de Budapest sobre Ciberdelincuencia, el Convenio de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (Convenio de Malabo) y la Convención de las Naciones Unidas contra la Ciberdelincuencia;
- definir unos conductos legales claros para acceder oportunamente a los datos alojados en plataformas radicadas en el extranjero, mediante tratados de asistencia judicial recíproca o marcos de divulgación de emergencia.

Las reformas legales son un paso necesario para generar confianza en la capacidad de las fuerzas del orden y garantizar que se rinden cuentas por las actividades de ciberdelincuencia. Estos esfuerzos deben ir acompañados de una inversión en iniciativas de capacitación judicial y especialización en el ámbito procesal.

6.3 Mejora de la cooperación regional e internacional

Dada la naturaleza intrínsecamente transnacional de la ciberdelincuencia, ningún país puede combatir esta amenaza en solitario. La cooperación regional y global es un elemento necesario para llevar adelante las investigaciones transnacionales, desmantelar las infraestructuras de los autores de las ciberamenazas, e intercambiar información policial en tiempo real.

Para reforzar la capacidad de respuesta colectiva, INTERPOL recomienda:

- ratificar y aplicar los convenios internacionales sobre ciberdelincuencia, como la Convención de las Naciones Unidas contra la Ciberdelincuencia y el Convenio de Budapest sobre Ciberdelincuencia, al objeto de agilizar las investigaciones transfronterizas y la extradición de los ciberdelincuentes;
- reforzar los mecanismos de intercambio de información policial entre los países africanos intensificando la participación en el proyecto AFJOC y en otros programas regionales e internacionales sobre ciberdelincuencia;
- institucionalizar los mecanismos de investigación transfronteriza, incluidos los procedimientos formales destinados al intercambio de pruebas, la remisión de casos y la realización de investigaciones paralelas;
- utilizar las plataformas de comunicación segura, como el sistema I-24/7 de INTERPOL, para establecer una rápida coordinación policial transfronteriza;
- dar apoyo a las operaciones conjuntas y a los equipos especiales integrados por varios países, organizados con el objeto de desarticular las redes de ciberdelincuencia que actúan en la región.

INTERPOL y AFRIPOL reiteran su compromiso con facilitar una cooperación estructurada dentro de África y con los socios globales. Sellar una colaboración duradera será fundamental para colmar las lagunas en el ámbito de la aplicación de la ley y luchar contra los grupos de ciberdelincuencia organizada que actúan más allá de las fronteras nacionales.

6.4 Ampliación de la prevención y de la sensibilización del público

A pesar de que las capacidades técnicas y las herramientas legales son fundamentales para combatir la ciberdelincuencia, la prevención sigue siendo la medida más rentable y la línea de defensa más flexible. En muchos de los ciberdelitos cometidos en África (como el *phishing*, las estafas por Internet y las estafas sentimentales por Internet) se emplean tácticas de ingeniería social y se aprovecha el bajo nivel de conocimientos digitales.

Para reforzar los esfuerzos en materia de prevención, INTERPOL recomienda:

- lanzar campañas de sensibilización dirigidas a un público concreto, en particular a grupos de alto riesgo, como los jóvenes, las mujeres, las pequeñas y medianas empresas (pymes) y los nuevos usuarios de Internet;
- integrar la formación sobre ciberseguridad en los planes de estudio de los colegios, la formación profesional y los programas de aprendizaje para adultos;
- promover unas prácticas esenciales de ciberhigiene, como el uso de una contraseña segura, la autenticación multifactor y la denuncia de mensajes sospechosos;
- animar a las víctimas a denunciar cualquier incidente, reforzando la confianza en las fuerzas del orden y garantizando la confidencialidad, sobre todo en casos de sextorsión o de estafas por Internet;
- involucrar a las organizaciones locales de la sociedad civil, como los grupos de mujeres y las redes de jóvenes, para que ayuden a difundir mensajes de prevención de un modo pertinente desde el punto de vista cultural.

Mediante la transmisión de los conocimientos necesarios para que las personas y las comunidades estén capacitadas para reconocer y evitar las ciberamenazas, los países pueden disminuir el número de víctimas, reducir el número de objetivos de los ciberdelincuentes y aliviar la carga investigadora de las fuerzas del orden.

6.5 Profundización de las alianzas entre los sectores público y privado

Las investigaciones de ciberdelitos dependen a menudo de los datos, las infraestructuras y la información en poder de entidades del sector privado, como proveedores de telecomunicaciones, entidades financieras, plataformas de medios sociales y empresas de ciberseguridad. Con todo, las fuerzas del orden de África siguen encontrando obstáculos para recibir información pertinente y apoyo técnico de estos actores.

Para crear un ecosistema más colaborativo, INTERPOL recomienda:

- establecer conductos de cooperación entre las fuerzas del orden y las principales partes interesadas del sector privado, lo que también incluye la creación de marcos para un intercambio de datos seguro y legítimo;
- crear unos foros nacionales y regionales de coordinación en materia de ciberdelincuencia que reúnan a organismos reguladores, investigadores, fiscales y actores del sector privado, o incorporarse a los ya existentes (por ejemplo, el Grupo de INTERPOL de Especialistas en Ciberdelincuencia), para sincronizar prioridades e intercambiar información policial;
- facilitar el acceso oportuno a las pruebas digitales alojadas en plataformas mundiales, mediante acuerdos jurídicos actualizados, protocolos técnicos y conductos de comunicación fiables;
- aprovechar los conocimientos y la infraestructura del sector privado en ámbitos tales como la información sobre amenazas, el análisis de *malware* y la respuesta a incidentes;
- fomentar la aportación de recursos del sector privado –por ejemplo, cursos, manuales y programas de mentoría dirigidos al personal de sector público– a las iniciativas de desarrollo de capacidades.

Al promover la confianza y la coordinación operativa entre los sectores público y privado, los países pueden desbloquear capacidades esenciales y agilizar la desarticulación de las redes de ciberdelincuencia.

6.6 Utilización de las nuevas tecnologías para prevenir la ciberdelincuencia

Así como las ciberamenazas evolucionan, también han de hacerlo las herramientas y las estrategias utilizadas para combatirlas. La inteligencia artificial, el aprendizaje automático, el análisis de datos y la automatización encierran nuevas oportunidades para que las fuerzas del orden anticipen, descubran y neutralicen las actividades ciberdelictivas a gran escala. Con todo, la adopción de estas tecnologías sigue siendo desigual entre los países de África.

Para promover una actuación policial más proactiva y basada en datos, INTERPOL recomienda:

- tratar de utilizar las herramientas de IA y aprendizaje automático para detectar técnicas de *phishing* y anomalías y clasificar las pruebas digitales;
- crear unas capacidades nacionales y regionales de análisis de datos para rastrear patrones de delitos cibernéticos y apoyar el control de amenazas en tiempo real;
- invertir en infraestructuras seguras basadas en la nube para labores de gestión de casos, criminalística digital, e intercambio de información entre países;
- probar herramientas de automatización en el seno de los organismos encargados de la aplicación de la ley para la recogida de pruebas, la respuesta a incidentes y el control de redes;
- elaborar unos marcos éticos y jurídicos que promuevan un uso responsable de las nuevas tecnologías en el ámbito de las investigaciones sobre delitos cibernéticos, inspirándose en las iniciativas sobre inteligencia artificial emprendidas por el Centro de Innovación de INTERPOL.

Las nuevas tecnologías abren el camino para que las actuaciones policiales sean más ágiles, inteligentes y flexibles, pero solo si se aplican con cautela y con las garantías necesarias.

ACERCA DE INTERPOL

INTERPOL es la organización policial internacional más grande del mundo. Su cometido consiste en prestar ayuda a los organismos encargados de la aplicación de la ley en los 196 países miembros de la Organización para luchar contra todas las formas de delincuencia transnacional. Trabaja para ayudar a la policía de todo el mundo a afrontar los crecientes desafíos que plantea la delincuencia del siglo XXI, ofreciendo una infraestructura de apoyo técnico y operativo de alta tecnología. Nuestros servicios incluyen formación específica, apoyo especializado para la investigación policial, bases de datos especializadas y conductos de comunicación policial protegida.

EXPECTATIVAS DE INTERPOL: MAYOR COMUNICACIÓN POLICIAL PARA UN MUNDO MÁS SEGURO

Las expectativas de INTERPOL consisten en lograr un mundo en el que todos los profesionales de los organismos encargados de la aplicación de la ley puedan recurrir a la Organización para transmitir, intercambiar y consultar de forma segura información policial esencial cuando y donde lo necesiten, y garantizar así la seguridad de los ciudadanos de todo el planeta. La Organización proporciona y promueve constantemente soluciones innovadoras y de vanguardia para afrontar los retos mundiales en materia policial y de seguridad.

SOBRE EL PROGRAMA DE INTERPOL CONTRA LA CIBERDELINCUENCIA

En una era digital dinámica, en la que más de la mitad de la población mundial está expuesta al riesgo potencial de la ciberdelincuencia, el Programa Mundial de INTERPOL contra la Ciberdelincuencia presta apoyo a la comunidad internacional encargada de la aplicación de la ley. Nos consagramos a desarrollar y liderar una respuesta global para prevenir, detectar, investigar y neutralizar la ciberdelincuencia con el objetivo último de ayudar a los países miembros a combatir eficazmente la ciberdelincuencia transnacional.

La Estrategia Mundial contra la Ciberdelincuencia de INTERPOL se centra en cuatro objetivos principales:

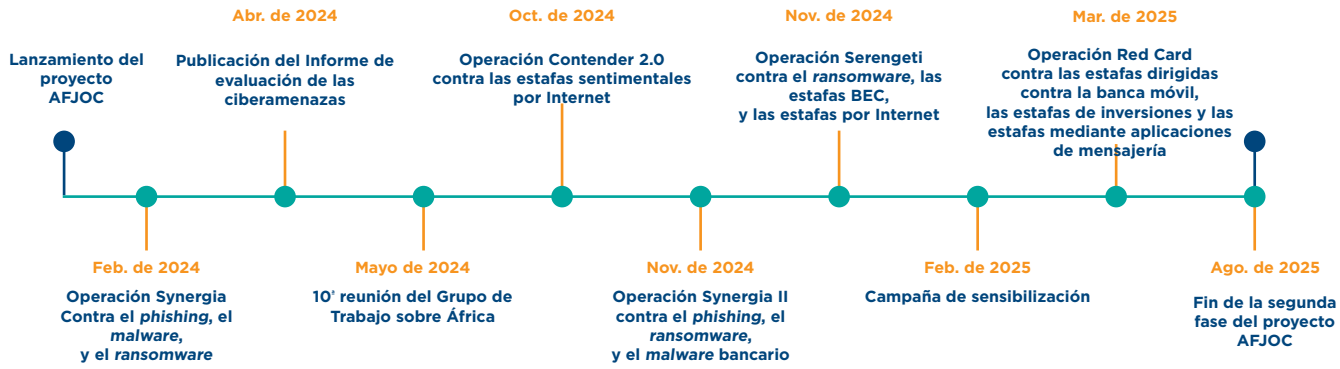
- Permitir un enfoque proactivo y ágil en materia de prevención y la neutralización de la ciberdelincuencia, mediante el desarrollo de un conocimiento profundo del panorama de las amenazas de la ciberdelincuencia a través del intercambio y análisis de información policial.
- Prevenir, detectar, investigar y neutralizar eficazmente la ciberdelincuencia, que causa daños importantes a escala nacional, regional y mundial, aportando para ello liderazgo, coordinación y apoyo a los países miembros en las actividades operativas transnacionales.
- Apoyar el desarrollo de las estrategias y capacidades de los países miembros en la lucha contra la ciberdelincuencia mediante el cultivo de alianzas abiertas, inclusivas y diversas y la creación de confianza en el ecosistema mundial de la ciberseguridad.
- Promover el papel y las capacidades de INTERPOL en la configuración de la seguridad mundial mediante la participación en foros internacionales en el ámbito de la ciberdelincuencia.

Ponemos en práctica nuestra estrategia y objetivos mediante un modelo de prestación de servicios sencillo y constructivo, que consta de tres pilares básicos:

- Respuesta a las amenazas de la ciberdelincuencia: hacer frente a las ciberamenazas inmediatas y emergentes con una respuesta rápida y coordinada.
- Operaciones sobre ciberdelincuencia: aplicar unas estrategias operativas coordinadas de alcance regional y mundial para combatir eficazmente la ciberdelincuencia.
- Desarrollo de capacidades cibernéticas: mejorar las estrategias y capacidades mediante proyectos y plataformas innovadores.

Estos pilares se sustentan en nuestra amplia red de alianzas público-privadas, que fomenta la colaboración y aprovecha los conocimientos colectivos para luchar contra la ciberdelincuencia.

Si desea más información, póngase en contacto con la Dirección de Ciberdelincuencia de INTERPOL en la siguiente dirección: EDPS-CD@interpol.int



ACERCA DE LA OFICINA DE INTERPOL DE OPERACIONES CONJUNTAS CONTRA LA CIBERDELINCUENCIA EN LA REGION AFRICANA

AFJOC es una iniciativa de INTERPOL destinada a reforzar la capacidad de los organismos nacionales africanos encargados de la aplicación de la ley para prevenir, detectar, investigar y neutralizar la ciberdelincuencia. Para lograrlo, es preciso:

- la recopilación y el análisis de información sobre actividades de ciberdelincuencia;
- la realización de actividades coordinadas basadas en información policial;
- la promoción de la cooperación y las buenas prácticas entre los países miembros africanos.

La fase 1 de la iniciativa fue financiada por el Ministerio de Asuntos Exteriores, de la Commonwealth y de Desarrollo del Reino Unido y se desarrolló de 2021 a 2023. La segunda fase, que cuenta con el apoyo del mismo organismo del Reino Unido, se basa en los logros de la primera y tiene por objeto seguir mejorando las capacidades de los organismos nacionales encargados de la aplicación de la ley en África.

Actividades del proyecto

- Apoyo analítico e información policial: recibir información policial correcta y proporcionada a tiempo es vital en cualquier respuesta policial a la ciberdelincuencia. Nuestros informes sobre ciberdelincuencia son un recurso importante, y ofrecen información sobre ciberamenazas dirigidas contra determinados países o regiones.
- Desarrollo de la capacidad nacional y de los recursos para combatir la delincuencia: las plataformas colaborativas como la Plataforma Colaborativa sobre Ciberdelincuencia y la Plataforma de Intercambio de Información sobre la Ciberdelincuencia permiten establecer comunicaciones seguras e intercambiar datos sobre las operaciones.
- Marco operativo conjunto: este marco permite abordar las amenazas de ciberdelincuencia mediante la colaboración entre organismos encargados de la aplicación de la ley, el sector privado y otras organizaciones internacionales e intergubernamentales.
- Apoyo a las operaciones y coordinación: nuestras operaciones ayudan a desmantelar las redes delictivas que se esconden detrás de la ciberdelincuencia.
- Campañas de sensibilización: estas campañas promueven buenas prácticas cibernéticas y están dirigidas a personas y empresas en África.
- Reuniones de grupos de trabajo para jefes de unidad: estos actos reúnen a los representantes de casi todos los países africanos con el fin de abordar los retos regionales en el ámbito de la ciberdelincuencia y de reforzar la colaboración operacional mediante reuniones paralelas y debates estratégicos.

Nuestra Oficina de Operaciones contra la Ciberdelincuencia en la Region Africana es la responsable de la ejecución del proyecto AFJOC. Esta Oficina trabaja en estrecha colaboración con las entidades interesadas más importantes de la región, en particular el Mecanismo Africano para la Cooperación Policial de la Unión Africana, AFRIPOL, las comunidades policiales y el sector privado.

Datos de contacto

Operaciones Conjuntas contra la Ciberdelincuencia en la Region Africana
AfricaDesk@interpol.int

INTERPOL

INTERPOL HQ

@INTERPOL_HQ

INTERPOL

INTERPOL HQ

INTERPOL_HQ