

DARKTRACE

El panorama de las amenazas cibernéticas

en América Latina

2024–2026

Intrusiones impulsadas
por identidades, extorsión
habilitada por la nube y
prioridades operativas para
los defensores de la región

Contenido

02	Resumen Ejecutivo	10	Sectores y países más afectados
03	Hallazgos clave	11	Panorama por país
03	Metodología	11	Colombia
04	Panorama de amenazas y factores clave	12	Chile
04	Tecnología y expansión digital	12	México
04	Presión geopolítica y estratégica	13	Brasil
04	Madurez cibernética y limitaciones de la fuerza laboral	13	Ecuador
05	La IA y el entorno de ataque	14	Implicaciones gubernamentales, regulatorias y estratégicas
05	Colaboración regional y respuesta estatal	15	Conclusión
06	Cómo se están desarrollando los ataques en América Latina	16	Apéndice
07	Phishing, robo de credenciales y la capa de correo electrónico	16	Análisis de malware de estafas judiciales en Colombia
08	La evolución del ransomware: del cifrado de datos a la extorsión y la monetización del acceso	16	Análisis de Malware SnappyBee / DEEDRAT
08	Malware, infostealers y la economía de las credenciales	17	Blind Eagle
08	Abuso de herramientas de confianza: LOTL, VPN, RMM y SaaS	17	Hallazgos de threat hunting
10	Actividad de intrusión estratégica vinculada a intereses estatales	18	Bibliografía

Resumen Ejecutivo

Entre 2024 y principios de 2026, el panorama de amenazas cibernéticas en América Latina evolucionó de forma decisiva hacia intrusiones impulsadas por la identidad y la explotación posterior al acceso.

En toda la región, los atacantes están eludiendo cada vez más los controles perimetrales mediante el robo de credenciales, el abuso de herramientas de administración remota y al operar dentro de flujos de trabajo legítimos en la nube y de software como servicio (SaaS), en lugar de depender exclusivamente de compromisos basados en vulnerabilidades.



Este cambio refleja tanto la rápida expansión digital como los diferentes niveles de madurez en ciberseguridad. Las inversiones en nubes híbridas, pagos digitales, telecomunicaciones, servicios habilitados por inteligencia artificial y modelos de trabajo distribuidos han ampliado la superficie de ataque. Al mismo tiempo, las brechas regulatorias, la escasez de talento especializado y una visibilidad operativa limitada han permitido que actores con fines lucrativos y grupos alineados con intereses estatales amplíen sus operaciones de forma eficiente más allá de las fronteras nacionales.

Tres tendencias definen el entorno actual: el acceso mediante credenciales se ha industrializado, las operaciones de ransomware han evolucionado hacia la extorsión de datos y la visibilidad en la nube, y las técnicas Living-off-the-Land (LOTL) son cada vez más predominantes en la actividad posterior al compromiso. En conjunto, estas dinámicas permiten a los atacantes operar dentro de flujos de trabajo empresariales legítimos, priorizar la exfiltración de información sobre el simple cifrado y evadir con mayor eficacia los mecanismos de detección basados en firmas.

La telemetría de Darktrace en la región corrobora esta tendencia.

El phishing y las credenciales comprometidas continúan siendo las principales vías de acceso, representando una proporción significativa de los incidentes observados. Mientras tanto, sectores como educación, administración pública, finanzas, manufactura y logística siguen experimentando un impacto sostenido. Colombia, México, Brasil, Chile, Ecuador y Panamá reflejan distintas combinaciones de crecimiento digital, exposición sectorial y enfoque por parte de los adversarios.

Para los líderes de seguridad en América Latina, el desafío no radica únicamente en que haya más ataques, sino en que grupos motivados financieramente, operadores regionales y actores alineados con estados utilizan cada vez más la misma lógica operativa: credenciales robadas, herramientas de confianza, persistencia silenciosa y robo acelerado de datos. En este contexto, la resiliencia depende de la visibilidad sobre las identidades digitales, las plataformas SaaS, la nube y las actividades de administración remota, así como de la capacidad para detectar anomalías sutiles de comportamiento más allá de la presencia de malware.

Las organizaciones que continúen centrando su estrategia únicamente en controles perimetrales, sin reducir su exposición al robo y abuso de identidades digitales ni mejorar la visibilidad sobre la actividad posterior al acceso inicial, afrontarán un riesgo cada vez mayor. El entorno operativo actual favorece a los defensores capaces de identificar tempranamente comportamientos anómalos de usuarios, dispositivos y servicios en la nube, interrumpir rápidamente el movimiento lateral y responder de manera efectiva a incidentes basados en la extorsión.

Hallazgos clave

La **superficie de ataque de América Latina** se ha visto transformada por la rápida adopción de tecnologías digitales y servicios en la nube, la expansión de herramientas de acceso remoto y la exposición generalizada de credenciales, desplazando la superficie principal de ataque desde la infraestructura hacia las identidades digitales.

La telemetría de Darktrace muestra que el **phishing y las credenciales comprometidas** siguen siendo los vectores de acceso más comunes, mientras que la ingeniería social por correo electrónico sigue afectando tanto a los usuarios generales como a las cuentas VIP a gran escala.

La **evolución del ransomware** también redefinió las prioridades de la superficie de ataque al desplazar el enfoque hacia el acceso y la visibilidad dentro del almacenamiento en la nube y los entornos SaaS, lo que permitió a los atacantes favorecer las técnicas LOTL y herramientas nativas por encima de la ejecución tradicional de malware.

Se ha observado que **actores de amenazas** como BlindEagle (APT-C-36), SambaSpider y APT41 han sido observados atacando infraestructura crítica, instituciones financieras y entidades gubernamentales en toda América Latina.

Persisten **disparidades regionales** en el nivel de madurez en ciberseguridad, siendo las economías en desarrollo las más expuestas, debido a recursos limitados y a marcos regulatorios fragmentados.

Metodología

Este informe combina múltiples conjuntos de evidencia.

El análisis regional principal se basa en datos de clientes de Darktrace observados en América Latina durante el período 2024–2026, cubriendo casos en Colombia, México, Brasil, Chile, Ecuador y Panamá. El informe también incorpora telemetría de Darktrace / EMAIL de octubre de 2025 a marzo de 2026, así como investigaciones específicas de caza de amenazas (threat hunting) realizadas entre enero de 2025 y abril de 2026.

El informe distingue entre el comportamiento observado por Darktrace y la información contextual procedente de fuentes externas. Los conocimientos propietarios se derivan del análisis conductual de la actividad de red, nube, SaaS e identidad en lugar de depender únicamente de firmas de malware. Fuentes externas se utilizan para complementar el contexto local sobre cambios regulatorios, tendencias digitales a nivel nacional y reportes públicos sobre la actividad relevante de actores de amenazas.

Los perfiles de países se centran únicamente en mercados de importancia estratégica y con una presencia significativa en los casos analizados por Darktrace. Por lo tanto, el informe sigue enfocado en América Latina, en lugar de en la región más amplia de América Latina y el Caribe (LAC). Cuando los datos hacen referencia a subconjuntos más reducidos de la base de clientes o a telemetría específica de determinados productos, dichos períodos se indican explícitamente.

Panorama de amenazas y factores clave

El riesgo cibernético en América Latina está cada vez más moldeado por la interacción entre el rápido crecimiento digital, la dependencia de la nube, una madurez en ciberseguridad desigual y las oportunidades de monetización criminal. Esto no produce un entorno de amenaza uniforme en toda la región, pero sí crea un modelo operativo consistente para los atacantes: **obtener acceso a bajo costo, integrarse en la actividad empresarial normal y monetizar rápidamente los datos o accesos obtenidos.**

Tecnología y expansión digital

En toda América Latina, la migración continua a la nube híbrida, aplicaciones empresariales SaaS, pagos digitales, flujos de trabajo habilitados por la IA y conectividad de alta velocidad han transformado la superficie de ataque ^[1]. El problema de seguridad no es la digitalización en sí, sino la visibilidad fragmentada que a menudo la acompaña. A medida que las organizaciones amplían su presencia en entornos distribuidos y en la nube, la identidad se convierte en el tejido conectivo entre usuarios, dispositivos, aplicaciones y terceros (third parties), haciendo que la exposición y el uso indebido de credenciales sean significativamente más importantes ^[2].

El crecimiento de las herramientas de administración remota, los modelos de externalización de TI y la prestación de servicios por parte de terceros también crea más canales de confianza que los atacantes pueden explotar después de comprometer un entorno ^{[3][4]}. Una vez que un adversario obtiene acceso válido o compromete un endpoint, las herramientas utilizadas legítimamente por la empresa suelen proporcionar suficiente alcance para mantener la persistencia, explorar el entorno y extraer datos sin desplegar malware personalizado que genera numerosas señales de detección ^[5].

Implicación de seguridad: En una región donde muchas organizaciones se están modernizando rápidamente, aunque de forma desigual, la ventaja más significativa en términos de control de seguridad proviene de una visibilidad unificada de la actividad en entornos locales (on-premises), SaaS y en la nube, especialmente en lo que respecta a usuarios, cuentas de servicio y comportamientos administrativos inusuales.

Presión geopolítica y estratégica

América Latina continúa atrayendo una combinación de actores de ciberdelincuencia con motivos financieros, operadores con intereses regionales y actividades de intrusión vinculadas a actores estatales ^{[5][6]}. Para estos últimos, sectores como telecomunicaciones, gobierno, servicios financieros, logística e infraestructura crítica representan objetivos de alto valor estratégico debido al potencial de obtención de inteligencia a largo plazo. Tanto los informes públicos como las observaciones de Darktrace apuntan a un patrón de intrusiones discretas y persistentes, más alineadas con actividades de espionaje y recolección de información que con la interrupción inmediata de operaciones.

La creciente participación de China en proyectos de infraestructura y transformación digital en distintas partes de la región añade complejidad plantea nuevos desafíos en materia de políticas públicas, especialmente en torno a cuestiones de soberanía, dependencia de proveedores y exposición estratégica ^[7]. Para los equipos de defensa, **la implicación operativa es clara: algunas intrusiones no buscan generar un impacto inmediato, sino mantener una presencia prolongada y encubierta para recopilar información de forma sostenida.** En este contexto, la capacidad de detectar anomalías sutiles y mantener visibilidad continua sobre la actividad del entorno resulta más valiosa que una estrategia centrada exclusivamente en el bloqueo de eventos aislados.

Madurez cibernética y limitaciones de la fuerza laboral

La madurez en ciberseguridad presenta importantes diferencias entre los países y sectores de América Latina ^[4]. Las organizaciones de mayor tamaño y los sectores críticos pueden contar con controles sólidos en áreas específicas, pero con frecuencia carecen de capacidades integradas de detección, procesos maduros de respuesta a incidentes y suficiente experiencia interna en seguridad de identidades y entornos en la nube ^[8].

Por su parte, las organizaciones más pequeñas y las entidades del sector público suelen enfrentar mayores limitaciones de presupuesto, personal especializado, herramientas de seguridad y supervisión de terceros ^[9]. Estas asimetrías crean condiciones favorables para el abuso de credenciales, la preparación de operaciones de ransomware y campañas de ingeniería social de bajo costo.

Por lo tanto, el desafío estratégico trasciende la tecnología. Muchas organizaciones mantienen una postura predominantemente reactiva, con capacidades limitadas para responder a incidentes de extorsión, una coordinación insuficiente entre áreas clave del negocio y una visibilidad reducida para correlacionar actividades sospechosas entre endpoints, correo electrónico, identidades y entornos en la nube. Estas brechas favorecen a los atacantes, ya que les permiten prolongar su presencia en el entorno comprometido y retrasar la necesidad de monetizar el acceso de forma inmediata.



La IA y el entorno de ataque

La proliferación de herramientas de IA generativa y agentes está transformando el panorama de amenazas de manera práctica y tangible más que teórica. La IA reduce las barreras para la ingeniería social, la traducción de contenido, la creación de señuelos, la asistencia al desarrollo de software y la escalabilidad de las campañas maliciosas. En América Latina, esto incrementa la frecuencia y sofisticación de los intentos de phishing, fraude e intrusiones automatizadas, sin modificar de forma significativa los objetivos de los atacantes ^{[8][9]}.

La implicación más importante para los defensores es la pérdida de visibilidad operacional.

A medida que los servicios legítimos de IA se integran cada vez más en los entornos corporativos, distinguir entre usos productivos y patrones de acceso potencialmente maliciosos se vuelve más complejo. Esto abre la puerta a técnicas operativas asistidas por la IA, incluida la experimentación con asistentes conectados a Internet como canales encubiertos de comunicación o infraestructura intermedia para actividades maliciosas ^{[8][10]}.

Colaboración regional y respuesta estatal

Iniciativas regionales como la colaboración con los Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT), Ciberlac, RedGEALC y otros esfuerzos de cooperación técnica demuestran que las capacidades de ciberseguridad continúan fortaleciéndose en la región ^{[11][12]}.

Sin embargo, la realidad operativa sigue siendo heterogénea. Aunque se han logrado avances en materia de estrategia, protección de datos y notificación de incidentes, el nivel de madurez y la efectividad de la implementación continúan variando considerablemente entre países y sectores ^{[11][12]}.

Para los defensores, esto implica que el cumplimiento normativo y regulatorio debe considerarse un habilitador importante, pero no una garantía de resiliencia. La resiliencia operativa sigue dependiendo de la capacidad de detección interna, la planificación y preparación para la respuesta a incidentes, así como de la capacidad para colaborar eficazmente con socios y organismos internacionales cuando se producen incidentes transfronterizos.



■ Patrones regionales:

Cómo se están desarrollando los ataques en América Latina

A través de la telemetría de Darktrace (2024 -2026), los ataques observados en América Latina siguen un patrón recurrente y claramente identificable: robo de credenciales o acceso inicial mediante campañas de phishing, seguido del abuso de herramientas legítimas y el establecimiento de mecanismos de persistencia de bajo perfil dentro de entornos corporativos. La carga útil específica, el sector afectado o el actor involucrado pueden variar, pero la lógica del ataque permanece notablemente consistente.

El panorama de amenazas en América Latina está impulsado por un ecosistema fragmentado de ransomware, el abuso generalizado de credenciales comprometidas a través de infostealers y una fuerte presencia de técnicas LOTL (Living off the Land) y herramientas de monitoreo y gestión remota (RMM).

El ransomware continúa siendo una de las amenazas más frecuentes, aunque su atribución suele ser limitada. Al mismo tiempo, los infostealers alimentan un mercado más amplio de credenciales comprometidas que sirve como punto de partida para ataques subsecuentes. A esto se suma una creciente combinación de actores patrocinados por Estados, incluidos aquellos vinculados a China y a grupos de amenazas regionales. Campañas como ByteToBreach (malware basado en la nube) y SORVEPOTEL (distribuido a través de WhatsApp por Water Saci) dirigidas a los sectores financiero y de criptomonedas evidencian la capacidad de innovación por parte del cibercrimen en la región.

Al mismo tiempo, según las observaciones de Darktrace, actividades como **SnappyBee/DEEDRAT**, vinculadas a **Salt Typhoon** en Brasil, ponen de manifiesto la continuidad de actividades de ataque alineadas con intereses estatales chinos en la región. En conjunto, estas tendencias reflejan una convergencia cada vez mayor entre el cibercrimen, los actores regionales y las operaciones con motivaciones geopolíticas.

Si bien el phishing y el uso de credenciales comprometidas continúan siendo los principales vectores de ataque en América Latina, se ha observado un aumento de nuevas variantes de ransomware, incluidas aquellas atribuidas a BlackSuit, Sauron, Medusa y Dire Wolf. Estos casos también reflejan una transición gradual desde los modelos tradicionales de cifrado de datos hacia esquemas de extorsión basados en la filtración y exposición de información robada.

Phishing, robo de credenciales y la capa de correo electrónico

En el 44% de los casos observados por Darktrace en toda la región, el malware (excluyendo el ransomware) se propagó tras el compromiso inicial de un dispositivo mediante phishing o el uso de credenciales comprometidas, lo que pone de manifiesto cómo la exposición de las identidades y las interacciones de los usuarios continúan desempeñando un papel central en las intrusiones posteriores.

Este patrón también se refleja en la telemetría de Darktrace / EMAIL recopilada en América Latina, entre octubre de 2025 y marzo de 2026:

Esto qué significa: Controles robustos de autenticación de correo electrónico, por sí solos, ya no son suficientes para mitigar el riesgo asociado al phishing moderno. Los atacantes continúan evadiendo controles basados en la confianza, adaptando sus tácticas de ingeniería social y dirigiéndose de forma reiterada a usuarios de alto valor dentro de las organizaciones.

Para los equipos de defensa regionales, el factor humano sigue representando la vía de entrada más sencilla para los adversarios, pero también el punto donde una detección temprana puede reducir significativamente el impacto de una intrusión y evitar que una amenaza se extienda a toda la organización.

MÁS DE
490,000

correos electrónicos de phishing fueron detectados en toda la base de clientes de la región.



MÁS DE
19,400

En el mismo periodo, más de 19 400 utilizaron **códigos QR** como mecanismo de acceso inicial.

MÁS DE
18,400

correos electrónicos de phishing fueron enviados desde **dominios creados recientemente**.

EI 48%

fue clasificado como **spear phishing**.

EI 37%

incorporó **técnicas novedosas de ingeniería social**.

EI 70%

superó las verificaciones de autenticación DMARC.



MÁS DE
55,000

de estos fueron dirigidos a usuarios VIP, lo que representa más del **11%** de todos los correos de phishing observados.



La evolución del ransomware: del cifrado de datos a la extorsión y la monetización del acceso

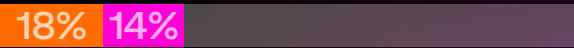
El ransomware sigue siendo una amenaza predominante en América Latina, pero cada vez resulta más impreciso considerarlo un problema centrado exclusivamente en el malware. Actividades observadas en Brasil, Chile, Colombia, Ecuador y México muestran un énfasis creciente en la obtención y explotación de accesos, el movimiento lateral, la interrupción de servicios y la exfiltración de datos, más allá del simple cifrado de endpoints. Esto se alinea con tendencias más amplias del mercado, donde el valor de la extorsión ya no se genera únicamente mediante el bloqueo de dispositivos, sino a través de la visibilidad sobre entornos de almacenamiento en la nube, plataformas SaaS y datos sensibles.

Los casos observados incluyeron atribuciones, o presuntos vínculos, con grupos de ransomware como [BlackSuit](#), Sauron, [Medusa](#), Dire Wolf, [Akira](#), [LockBit](#), [ShadowSyndicate](#) y [RansomHub](#), aunque una proporción significativa de la actividad permaneció sin atribución. Esta fragmentación tiene importantes implicaciones operativas, ya que los equipos de defensa no pueden depender de atribuciones o familias de amenazas conocidas como único medio para evaluar el riesgo. En su lugar, la prioridad debe centrarse en la detección de comportamientos comunes que preceden al despliegue del ransomware, incluidos el abuso de credenciales, la administración remota inusual, la escalada de privilegios, las actividades de reconocimiento, así como el movimiento y/o la exfiltración anómala de datos.

En toda la región de América Latina, sectores como la educación, la administración pública, la logística, la manufactura, la minería, la salud y los servicios financieros han enfrentado incidentes relacionados con cifrado malicioso, exfiltración de datos, accesos no autorizados e interrupciones operativas. En la práctica, el ransomware en América Latina se entiende mejor como una amenaza centrada en el acceso y los datos, donde el movimiento lateral y el acceso a información sensible suelen generar un impacto empresarial mayor que la carga útil utilizada en la fase final del ataque.

Sectores más afectados en América Latina:

El **sector educativo** fue el más afectado, representando el 18 % de todos los incidentes, seguido por los sectores de **administración pública** y de **información y comunicaciones**, que concentraron cada uno el 14 % de los incidentes registrados.



Los sectores de **manufactura** y comercio mayorista/minorista registraron el doble de incidentes durante la segunda mitad de 2025 en comparación con la primera, impulsados por un incremento en los casos relacionados con la propagación de malware. Esta tendencia podría estar asociada con procesos acelerados de digitalización y una mayor exposición de datos.

Malware, infostealers y la economía de las credenciales

Los casos de malware más relevantes en la región muestran una **concentración de infostealers, malware bancario, cargadores multi-etapa (multi-stage loaders) y cadenas de ataque complejas, más que cargas maliciosas puramente destructivas.**

[ViperSoftX](#) y [AtomicStealer](#) fueron observados repetidamente en Colombia y México, particularmente en el sector educativo, lo que pone de relieve la exposición persistente de entornos con capacidades de defensa más limitadas. Horabot fue identificado en México, mientras que Ecuador registró una mayor actividad de malware más compleja, incluyendo GOL-DBACKDOOR junto con [GhostSocks](#) y [Amadey](#).

En contraste, Chile y Brasil mostraron campañas más oportunistas relacionadas con la minería ilícita de criptomonedas y el robo de información, especialmente en sectores como la agricultura y la tecnología.

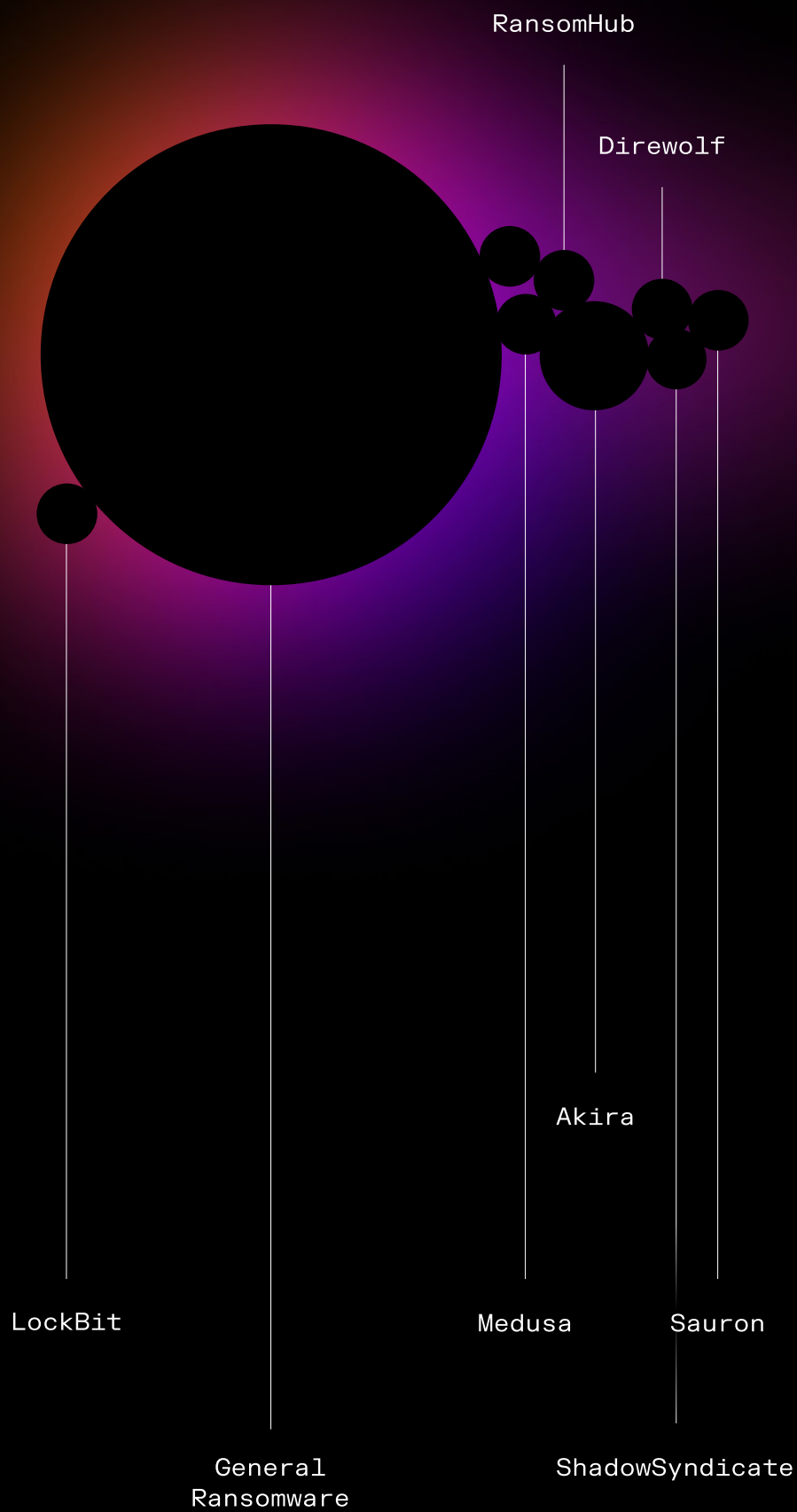
Esta actividad evidencia la creciente industrialización del robo de credenciales. Los infostealers ya no deben considerarse amenazas aisladas de bajo impacto; sostienen una economía del acceso más amplia, en la que credenciales robadas, tokens de sesión y accesos comprometidos son reutilizados, intercambiados o comercializados entre actores maliciosos. Esta dinámica acorta el camino desde la vulneración inicial hasta una intrusión más amplia, lo que facilita el fraude, la extorsión y el uso indebido de la nube o de los servicios SaaS.

Esto qué significa: En América Latina, los infostealers deben tratarse como indicadores tempranos de compromisos potencialmente más extensos y de mayor impacto. La presencia de malware ligero puede ser una señal temprana de riesgos posteriores que van mucho más allá del equipo inicialmente comprometido y afectan identidades, datos y recursos corporativos críticos.

Abuso de herramientas de confianza: LOTL, VPN, RMM y SaaS

Una característica distintiva de la actividad observada en la región es el uso habitual y abusivo de software legítimo y de funcionalidades nativas de los sistemas operativos. Los servicios VPN, las herramientas de monitoreo y gestión remota (RMM), intérpretes de comandos, el acceso a aplicaciones SaaS a través del navegador, los componentes alojados en GitHub y mecanismos de administración en la nube aparecen de forma recurrente en los casos reportados por Darktrace. Esto refleja la tendencia más amplia de abandonar implantes maliciosos de alta visibilidad en favor de técnicas que se integran en las actividades habituales de los entornos empresariales.

Para los equipos de defensa, el desafío no radica únicamente en identificar la herramienta utilizada, sino en comprender el contexto en el que se emplea. Comportamientos administrativos inusuales, accesos fuera del horario habitual, combinaciones atípicas de aplicaciones, anomalías geográficas, intentos repetidos de autenticación fallidos y nuevas conexiones salientes suelen proporcionar las señales más valiosas. En una región donde muchas organizaciones dependen significativamente de terceros y externalizan parte de la prestación de servicios de TI, contar con visibilidad contextual basada en el comportamiento es fundamental.



Actividad de intrusión estratégica vinculada a intereses estatales

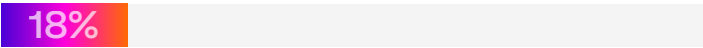
El cibercrimen motivado financieramente sigue siendo el principal desafío operativo en gran parte de América Latina [6], pero no es el único. Las observaciones de Darktrace y los informes públicos también indican una creciente influencia de actividades de intrusión alineadas con intereses chinos [7].

Estas operaciones se caracterizan por la rápida explotación de dispositivos expuestos a Internet, mecanismos de persistencia de bajo perfil, DLL sideloading, túneles DNS, infraestructura en la nube y el abuso de herramientas legítimas de gestión remota. Este patrón se refleja en la actividad relacionada con ShadowPad observada en Panamá, Colombia y Brasil, así como en la actividad de PlugX en Chile y de SnappyBee/DEE-D RAT asociada con Salt Typhoon en Brasil. Esta última fue identificada como parte del informe **Crimson Echo** de Darktrace, que utilizó análisis de comportamiento para contextualizar la actividad de intrusión vinculada a China.

Estas intrusiones son especialmente relevantes porque afectan a sectores de valor estratégico, como instituciones financieras, telecomunicaciones, organismos gubernamentales, energía, minería y funciones administrativas críticas, y porque su tiempo de permanencia tiende a ser más prolongado y discreto que el observado en las campañas de cibercrimen tradicionales. Para los defensores de la región, la principal lección es que no toda actividad de alto impacto está impulsada por la extorsión. Algunas intrusiones se comprenden mejor como operaciones estratégicas de recopilación de inteligencia que explotan las mismas brechas de visibilidad que las campañas motivadas financieramente.

Sectores y países más afectados

Dentro del conjunto de casos observados por Darktrace, el sector educativo fue el más afectado, representando el 18 % de todos los incidentes, seguido por administración pública y el sector de información y comunicaciones. Los sectores de manufactura y comercio mayorista y minorista también registraron un aumento entre la primera y la segunda mitad de 2025, lo que indica una presión creciente sobre entornos empresariales expuestos digitalmente .



Colombia es el país más afectado dentro de la base de clientes de América Latina, seguido por México, Brasil, Ecuador, Chile y Panamá. Este ranking no debe leerse como un mapa de riesgo regional completo, pero sí muestra dónde Darktrace ha visto repetidamente actividad de intrusión significativa y dónde las lecciones operativas son más relevantes.



Panorama por país

Las siguientes reseñas por país se centran en los mercados más claramente representados en los casos analizados por Darktrace y más relevantes para la combinación actual de expansión digital, exposición sectorial y comportamiento de los adversarios en la región. Cada sección está estructurada en torno al contexto del mercado, las principales amenazas, las observaciones de Darktrace, la evolución del entorno regulatorio y las implicaciones prácticas para los defensores.

Colombia

Colombia destaca tanto por el volumen de ataques como por la diversidad de los objetivos observados. El rápido crecimiento de los sectores fintech, la adopción de la nube y los servicios digitales han ampliado la superficie de ataque del país. Al mismo tiempo, la sensibilidad del sector público, la concentración de entidades financieras y la volatilidad política siguen atrayendo a una amplia gama de actores de amenaza ^[13]. Los principales centros urbanos, como Bogotá y Medellín, están utilizando cada vez más datos y la nube, lo que aumenta aún más el valor del acceso a credenciales, entornos SaaS e infraestructura híbrida ^{[14] [15] [16]}.

Los informes públicos de 2024 y 2025 indican que Colombia siguió siendo uno de los países más atacados de América Latina, particularmente en los sectores gubernamental, financiero y de salud ^[17].

Blind Eagle (APT-C-36) sigue siendo el actor de amenaza más persistente y visible del país, con múltiples campañas e intrusiones recurrentes que aprovechan phishing, documentos maliciosos, troyanos de acceso remoto (RAT) e infraestructura DNS dinámica ^{[18] [19]}. Paralelamente, el malware bancario, los brokers de acceso inicial (IAB) y los grupos de ransomware continúan explotando la importancia económica de Colombia y la desigual madurez de sus capacidades de seguridad ^{[6] [20] [21]}.

Las observaciones de Darktrace coinciden en gran medida con este panorama. En el conjunto de casos de 2024-2025, Colombia representó casi una cuarta parte de los incidentes observados en América Latina. Las actividades más comunes estuvieron relacionadas con infostealers,

malware vinculado a China y múltiples patrones asociados con Blind Eagle. Los sectores más afectados incluyeron la administración pública y la defensa, así como organizaciones de servicios financieros y aseguradoras. La concentración tanto de actividades entre el cibercrimen y las actividades de espionaje convierte a Colombia en un importante referente clave para comprender las tendencias de amenazas para el resto de la región.

Un caso de fraude dirigido contra el sistema judicial colombiano ilustra cómo la ingeniería social adaptada al contexto local continúa siendo efectiva. En esta campaña, los actores de amenaza utilizaron una notificación judicial falsa distribuida mediante un archivo adjunto para desencadenar la ejecución de código a través de PowerShell y HTA, establecer mecanismos de persistencia y comunicarse con infraestructura de mando y control (C2).

La relevancia de este caso no radica únicamente en la cadena de infección utilizada, sino también en la localización del señuelo y en la rapidez con la que los usuarios pueden ser inducidos a ejecutar contenido malicioso cuando la confianza se combina con temáticas legales, financieras o cívicas.

El entorno regulatorio colombiano continúa evolucionando, con la Estrategia Digital Nacional y el marco de protección de datos orientados a fortalecer la confianza, la gobernanza y la resiliencia digital ^{[22] [23]}. Sin embargo, al igual que en otros mercados de la región, la ambición política no se traduce automáticamente en capacidad operativa. Los equipos de seguridad aún necesitan mejorar la detección de accesos obtenidos mediante phishing, el despliegue de RAT y la actividad saliente relacionada con infraestructura C2.

Implicación para los equipos de defensa: Los equipos de seguridad en Colombia deberían priorizar la protección frente a accesos obtenidos mediante phishing y frente a comportamientos posteriores al compromiso inicial, en lugar de considerar los archivos adjuntos maliciosos como el problema principal o punto final de ataque. Dado el volumen de actividad con características asociadas a grupos de amenaza persistente avanzada (APT), resulta fundamental la detección temprana de mecanismos de persistencia, comunicaciones salientes inusuales y comportamientos administrativos sospechosos.



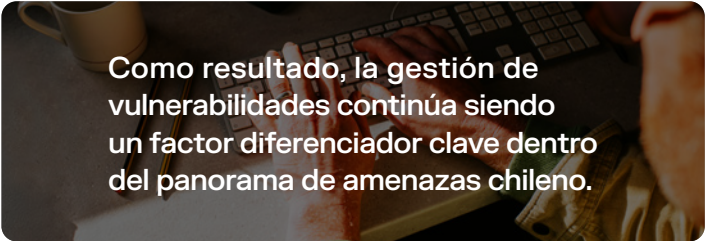
Chile

El entorno digital de Chile se caracteriza por un sólido crecimiento de la infraestructura, la expansión de la capacidad de los centros de datos, el rápido despliegue de redes 5G y una creciente adopción de servicios en la nube, lo que convierte al país en un mercado atractivo tanto para la inversión legítima como para la actividad maliciosa [24]. A medida que más servicios corporativos y procesos industriales se trasladan a entornos digitales, la exposición del país se extiende más allá de los compromisos tradicionales de endpoints y se extiende a riesgos que afectan la infraestructura, los proveedores de servicios y los sectores críticos [24].

Entre 2024 y mediados de 2026, Chile experimentó un marcado aumento de los ciberataques reportados, con actividad de ransomware, phishing y malware que afectó a organismos gubernamentales, empresas de energía, telecomunicaciones y otros sectores empresariales [6] [25]. Los reportes públicos también han destacado la actividad de actores vinculados a Horabot y campañas criminales más amplias dirigidas a entornos de habla hispana [25]. La dinámica operativa sigue siendo consistente: acceso obtenido mediante la interacción del usuario, explotación de sistemas expuestos y actividades posteriores orientadas a la extorsión.

Los datos de casos de Darktrace recopilados entre 2024 y 2026 muestran que Chile se vio particularmente afectado en el sector educativo, con incidentes relevantes relacionados con la minería ilícita de criptomonedas, ransomware e infostealers.

Casi el 50 % de los casos observados involucraron la explotación de vulnerabilidades de hardware o software, incluida la explotación asociada a Cleo y el abuso de herramientas como Atera y Splashtop. Esto diferencia en cierta medida a Chile de otros países donde el robo de credenciales y el phishing dominan las vías de acceso inicial de forma más marcada .



Chile también es uno de los mercados más activos en materia de desarrollo regulatorio. Su Política Nacional de Ciberseguridad, la creación de la Agencia Nacional de Ciberseguridad (ANCI), los requisitos reforzados de notificación de incidentes y un marco de protección de datos significativamente actualizado apuntan a un entorno regulatorio en constante maduración [26] [28]. Sin embargo, el avance normativo no elimina la necesidad práctica de fortalecer la gestión de parches, fortalecer la detección temprana de indicadores previos al ransomware y aumentar la visibilidad sobre entornos educativos, tecnológicos y de servicios críticos.

Implicación para los equipos de defensa: Las organizaciones en Chile deben seguir priorizando la gestión de vulnerabilidades y la aplicación oportuna de parches, pero estos esfuerzos deben complementarse con capacidades de monitoreo conductual capaces de detectar las etapas iniciales del ransomware, la escalada de privilegios y el movimiento lateral. Los primeros indicadores de compromiso suelen manifestarse mucho antes de que un ataque alcance su fase más disruptiva.

México

El papel de México como un importante centro de manufactura, logística, subcontratación y servicios digitales lo convierte en uno de los mercados cibernéticos más estratégicos de América Latina [27] [28]. El crecimiento continuo de los servicios de TI, la inversión en la nube, las iniciativas de ciudades inteligentes y la transformación digital impulsada por la IA amplían tanto la escala como la diversidad de los sistemas expuestos [27] [28] [29]. Al mismo tiempo, aumenta la dependencia de proveedores externos, lo que crea vías adicionales para el compromiso de la cadena de suministro y las intrusiones vinculadas a terceros de confianza [27] [28] [29].

Los informes públicos indican que México sigue siendo uno de los países más atacados de la región, enfrentando de forma recurrente la presión por parte de grupos de ransomware, malware bancario con fines financieros, ataques a la cadena de suministro y campañas de phishing atribuidas, en parte, a actores vinculados a Estados o alineados con intereses estratégicos [6].

El tamaño del país, su relevancia industrial y su integración con las cadenas de suministro norteamericanas lo convierten en un objetivo atractivo tanto para los ciberdelincuentes como para las operaciones orientadas al espionaje. **Aproximadamente el 43 % de las organizaciones mexicanas han reportado ataques relacionados con la cadena de suministro**, los cuales aprovechan las relaciones de confianza existentes entre empresas, socios comerciales y proveedores para ser explotadas como vectores de acceso [29].



Las observaciones de Darktrace sitúan a México entre los países más afectados dentro del conjunto de datos de 2024-2025. La actividad observada incluyó exfiltración de datos, ransomware, intrusiones en entornos SaaS y accesos no autorizados, siendo los sectores de manufactura, comercio mayorista y minorista, transporte y almacenamiento algunos de los más afectados.

El caso de Water Sapi resulta particularmente ilustrativo de cómo los grupos regionales de cibercrimen están adaptando sus técnicas de distribución al comportamiento de los usuarios locales. En este caso, señuelos distribuidos a través de WhatsApp, la descarga de instaladores, componentes alojados en GitHub y comunicaciones externas sospechosas se combinaron para conformar una cadena de intrusión probablemente motivada por fines financieros dentro del sector financiero.

El entorno político de México también está evolucionando, con iniciativas recientes en materia de ciberseguridad y una mayor participación del sector público en la definición de arquitecturas y prácticas de gestión de riesgos [30] [31]. Como parte de estos esfuerzos, el gobierno mexicano introdujo el Plan Nacional de Ciberseguridad 2025-2030, una estrategia integral que reconoce a la IA y las tecnologías en la nube tanto como áreas de exposición como herramientas clave para combatir y mitigar las amenazas cibernéticas, además de fortalecer las defensas nacionales [29] [30] [31]. Sin embargo, el desafío operativo sigue siendo inmediato: una economía grande e interconectada, con amplias dependencias externas, una madurez desigual de las capacidades de seguridad entre proveedores y una exposición continua al robo de credenciales y al abuso de accesos legítimos.

Implicación para los equipos de defensa: Las organizaciones mexicanas deben priorizar la seguridad de los entornos SaaS, la protección de credenciales y el monitoreo de vías de acceso externas y conexiones con terceros. Cuando los atacantes pueden desplazarse a través de socios, proveedores de servicios o plataformas de colaboración, la detección temprana de actividades anómalas resulta esencial.

Brasil

La escala de Brasil, su sistema financiero, la digitalización del sector agrícola, el crecimiento de los centros de datos y la inversión en infraestructura de IA lo convierten tanto en un líder regional en innovación como en un objetivo cibernético prioritario [32][33][34]. Los servicios financieros críticos, el ecosistema PIX, la conectividad del sector agrotecnológico y las amplias dependencias de servicios en la nube y telecomunicaciones amplían el abanico de oportunidades de intrusión disponibles tanto para los ciberdelincuentes como para los actores estratégicamente motivados [34][35][36]. La actividad de amenazas en Brasil abarca malware bancario, ransomware, robo de credenciales, campañas distribuidas a través de WhatsApp, ecosistemas de brokers de acceso inicial (IAB) y operaciones de espionaje alineadas con intereses estatales [37][38]. Los reportes públicos identifican de forma consistente al país como un mercado de alto valor para el malware financiero y el ransomware, mientras que las observaciones de Darktrace indican que Brasil también merece una atención significativa debido a la actividad vinculada a China o alineada con intereses chinos en sectores estratégicos.

Dentro de los casos observados por Darktrace entre 2024 y 2025, Brasil mostró actividad recurrente en los sectores agrícola y financiero, incluyendo malware, intrusiones relacionadas con SaaS y campañas de infostealers. El caso SnappyBee/DEEDRAT es particularmente significativo puesto que ilustra cómo un actor de amenaza vinculado a China pudo aprovechar una **vulnerabilidad en Citrix NetScaler**, la VPN SoftEther, actividad de beaconing y comportamientos de exfiltración de datos para llevar a cabo una operación de espionaje a largo plazo contra una organización brasileña del sector tecnológico. Esto representa un perfil de riesgo distinto al del malware bancario predominante en la región, aunque explota muchas de las mismas brechas de visibilidad. Puede encontrarse un análisis más detallado sobre la actividad vinculada a China en el informe Crimson Echo de Darktrace. El informe **The State of Cybersecurity in the UK, US and Brazil Healthcare Sectors** de Darktrace identifica un modelo de amenaza específico para Brasil en el que los ciberatacantes tienen cada vez más en el punto de mira tanto a pacientes como a proveedores de servicios de cirugía estética, utilizando datos médicos altamente sensibles para fines de coerción directa y extorsión económica. En este contexto, los actores de amenaza priorizan la monetización a nivel del paciente, y no únicamente al nivel institucional, utilizando información robada para facilitar esquemas de extorsión dirigidos, en lugar de depender exclusivamente de la interrupción operativa característica del ransomware tradicional.

Este enfoque refleja una adaptación deliberada a la economía del sector sanitario brasileño y al comportamiento de los pacientes, donde la sensibilidad en torno a la privacidad y la fragmentación de la seguridad en muchas clínicas generan condiciones favorables para la doble extorsión, tanto contra individuos como contra proveedores de servicios.

El entorno regulatorio y estratégico de Brasil continúa evolucionando mediante la política nacional de ciberseguridad, los requisitos establecidos por la Ley General de Protección de Datos Personales (LGPD) y diversas propuestas orientadas a fortalecer la supervisión institucional [39][40][41][42]. Sin embargo, los equipos de defensa deben operar en un entorno en el que el cibercrimen y el espionaje convergen cada vez más alrededor de las identidades digitales, los servicios en la nube y las vías de acceso basadas en herramientas legítimas y de confianza.

Implicación para los equipos de defensa: El peso de los sistemas financieros de Brasil, su infraestructura a gran escala y su transformación digital estratégica lo convierten en un objetivo prioritario tanto para actores de ciberdelincuencia como para operaciones de espionaje. El abuso de credenciales, los accesos remotos anómalos, los comportamientos inusuales asociados a servicios VPN y los movimientos anómalos de datos deben considerarse indicadores operativos de alta prioridad.



Ecuador

Ecuador refleja una faceta diferente, aunque igualmente reveladora, del panorama regional de amenazas. La infraestructura digital del país ha estado marcada en gran medida por su dependencia de las telecomunicaciones, una conectividad rural desigual y los esfuerzos continuos por ampliar los servicios digitales [43][44][45]. A medida que mejora la conectividad y crecen el comercio electrónico, la digitalización gubernamental y la prestación de servicios en línea, la madurez de las capacidades de seguridad no siempre evoluciona al mismo ritmo.

Los reportes públicos han destacado la actividad de ransomware, filtraciones de datos, exposición causada por amenazas internas y ataques de denegación de servicio distribuido (DDoS) que afectan a organismos gubernamentales y servicios críticos [46][47][48][49]. Como resultado, el panorama de amenazas en Ecuador se caracteriza menos por el volumen de ataques y más por los desafíos relacionados con la resiliencia, la visibilidad y las consecuencias de contar con una profundidad defensiva limitada en sectores clave.

El conjunto de casos observados por Darktrace en Ecuador es menor que el de Colombia o México, pero mantiene una alineación general con las tendencias nacionales de amenazas. La mitad de los casos observados involucró ataques basados en malware dirigidos al sector de transporte y almacenamiento, mientras que otros incidentes incluyeron abuso de WinReg y exfiltración de datos que afectaron a organizaciones de los sectores de manufactura y salud. La actividad de malware multietapa, incluido GOLDBACKDOOR y otros componentes relacionados, sugiere que incluso un volumen de casos relativamente bajo puede revelar riesgos significativos asociados con la persistencia y la explotación posterior por parte de los atacantes.

El entorno regulatorio ecuatoriano continúa madurando mediante iniciativas como la Estrategia Nacional de Ciberseguridad, el desarrollo de su régimen de protección de datos personales y el debate continuo sobre la IA y la regulación de datos [50][51][52]. Sin embargo, para muchas organizaciones, especialmente aquellas con visibilidad limitada y equipos de seguridad de menor tamaño, el desafío sigue siendo fundamentalmente operativo: establecer líneas base de comportamiento, monitorear actividades anómalas y mantener una adecuada preparación para la respuesta a incidentes.

Implicación para los equipos de defensa: Dado que la visibilidad suele ser limitada en numerosos entornos, las organizaciones en Ecuador deberían priorizar el monitoreo básico y la detección de anomalías, especialmente aquellas relacionadas con actividad de malware, abuso del registro del sistema, las comunicaciones salientes inusuales e intentos de exfiltración de datos.

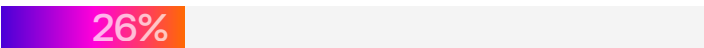
Implicaciones gubernamentales, regulatorias y estratégicas

La regulación de la ciberseguridad en América Latina continúa avanzando, pero la realidad operativa sigue reza-gada. Muchos países han introducido leyes más estrictas de protección de datos, estrategias nacionales de ciberse-guridad, requisitos de notificación de brechas de seguridad y mecanismos de supervisión para infraestructuras críticas [53][54][55] [56] [57]. Sin embargo, la aplicación, la coordinación y las capacidades corporativas siguen siendo inconsistentes, y la brecha entre la ambición política y la ejecución efectiva de la seguridad continúa siendo significativa [1] [6].

Esto es relevante porque el entorno de amenazas evoluciona más rápido que los marcos de cumplimiento normativo. Las organizaciones ya enfren-tan robo de credenciales, extorsión y abuso de herramientas legítimas y de confianza, independientemente de que los marcos regulatorios hayan madurado plenamente en áreas como la supervisión de entornos en la nube, la respuesta transfronteriza a incidentes o los riesgos asociados con la IA. En términos prácticos, una regulación más estricta no se traduce automáticamente en un SOC más maduro, una capacidad de respuesta a incidentes mejor preparada o una visibilidad integral sobre entornos de identidad y nube.

Los desafíos operativos siguen siendo evidentes en toda la región. El crecimiento digital a menudo ha superado la inversión en seguridad, mientras que muchas organizaciones continúan enfrentando escasez de talento, responsabilidades fragmentadas, requisitos limitados de divulga-ción de incidentes y una débil coordinación entre los sectores público y privado [56][57].

Las organizaciones afrontan una brecha considerable entre la ambición tecnológica y la madurez de sus capacidades de seguridad. Mientras tanto, los ciberataques en la región registran incrementos de hasta un 26 % anual, y el gasto empresarial en TI e infraestructura digital en América Latina se proyecta en casi 118,000 millones de dólares, mientras que los presupuestos de seguridad continúan creciendo a un ritmo significativamente menor [1] [59].



Según el Foro Económico Mundial, el 65 % de las organizaciones en América Latina carecen de las competencias críticas necesarias para alcanzar sus objetivos de seguridad, y una proporción significativa reporta una grave escasez de profesionales especializados en respuesta a incidentes e ingeniería DevSecOps [56]. **Solo el 12% de los líderes de TI encuestados manifiestan un alto nivel de confianza en sus equipos de ciberseguridad [56].**



Estas limitaciones afectan no solo la prevención, sino también la velocidad de respuesta, la calidad de las in-vestigaciones y la capacidad de compartir información defensiva de manera oportuna entre sectores y países.

La soberanía de los datos y la dependencia estratégica también son cada vez más relevantes. La inversión en infraestructura extranjera, la con-centración de servicios en la nube y la dependencia de los proveedores de telecomunicaciones complican las cuestiones relacionadas con el control de los datos y la respuesta a incidentes. Para algunas organizaciones, especialmente aquellas que operan en sectores regulados, esto añade una dimensión de gobernanza a un desafío técnico ya de por sí complejo. La visibilidad sobre dónde residen los datos, quién puede acceder a ellos y con qué rapidez puede investigarse la actividad sospechosa constituye ahora un requisito estratégico, y no simplemente una obligación de cumplimiento normativo.

Al mismo tiempo, el progreso es tangible. Brasil, Chile, Colombia, Ecuador y México están avanzando hacia modelos de gobernanza más sólidos mediante enfoques distintos, ya sea a través de la implementación de mecanismos de notificación de incidentes, políticas nacionales, el forta-lecimiento de la protección de datos, iniciativas de confianza cero (zero trust) o la creación de instituciones especializadas en ciberseguridad [52] [57][58][60]. Estos avances deben interpretarse como bases sobre las cuales las organizaciones pueden construir capacidades resilientes, y no como sustitutos de la resiliencia interna.

¿Qué significa esto?: Para las organizaciones que operan en América Latina, el cumplimiento regulatorio por sí solo no equivale a seguridad. La resiliencia efectiva depende de contar con capacidades internas de detección, preparación para la respuesta a incidentes, una gobernanza sólida en torno a las identidades digitales y la exposición a la nube, así como de la capacidad de coordinarse de manera ágil entre las áreas legales, técnicas y ejecutivas.

Conclusión

El panorama de amenazas cibernéticas en América Latina ya no se define principalmente por campañas ruidosas, centradas en exploits (explotación de vulnerabilidades) y el uso intensivo del malware. Actualmente, la región enfrenta ahora un entorno más complejo e híbrido, en el que el robo de credenciales, el abuso de entornos SaaS, los infostealers, la extorsión habilitada por la nube y los mecanismos de persistencia de bajo perfil ocupan un lugar central tanto en las operaciones del cibercrimen como en la actividad de intrusión estratégica.

Tres prioridades emergen con claridad para los líderes de seguridad. En primer lugar, reducir la exposición relacionada con la identidad mediante una mayor protección de credenciales, la detección del abuso de cuentas y un control más eficaz de las cuentas privilegiadas y de servicio. En segundo lugar, mejorar la visibilidad sobre los entornos SaaS, la nube y las herramientas de administración remota, de modo que las actividades posteriores al acceso puedan detectarse antes de derivar en pérdida de datos o extorsión. En tercer lugar, fortalecer la preparación mediante planes de respuesta basados en escenarios, especialmente para compromisos derivados de campañas de phishing, fases de preparación de ransomware y movimientos de datos sospechosos.

Para los líderes de seguridad en América Latina, la prioridad no consiste únicamente en defenderse de manera más eficaz, sino en adaptarse a la forma en que ocurren los ataques en la actualidad. El compromiso de identidades, el abuso de entornos SaaS y la persistencia discreta definen el entorno operativo actual. Las organizaciones capaces de detectar anomalías de comportamiento de forma temprana, reducir su exposición a credenciales y responder rápidamente a actividades posteriores al acceso estarán mejor posicionadas para gestionar el riesgo en la región.

Apéndice

El apéndice proporciona detalles técnicos adicionales que respaldan los estudios de caso seleccionados referenciados en el informe principal.

■ Apéndice A.

Análisis de malware de estafas judiciales en Colombia

En este caso, el actor de amenaza disfrazó un malware como una notificación judicial legítima colombiana denominada "Radicado Judicial.pdf.lnk". El archivo de acceso directo ejecutó PowerShell de forma silenciosa, eludió las restricciones de ejecución y creó una ruta de preparación (staging path) para un archivo HTA en la carpeta del directorio temporal del sistema. Posteriormente, la cadena de ataque utilizó un mecanismo de descarga similar a wget para obtener adicional desde una ubicación remota y ejecutarlo mediante mshta.exe.

El componente HTA mostró una notificación judicial falsa mientras un script VBScript establecía en segundo plano una carga maliciosa oculta de PowerShell. Esta carga recopiló información del sistema comprometido, obtuvo detalles del host y de las soluciones antivirus instaladas, y estableció mecanismos de persistencia mediante tareas programadas, elementos de inicio automático y claves del registro. La clave de registro "iRaNKfje" y una tarea programada denominada "qbbxljYk" fueron utilizadas para mantener la ejecución continua del malware en el sistema afectado.

Posteriormente, el malware se conectó con la infraestructura de comando y control (C2) alojada en love.negro[.]ink, enviando información del sistema comprometido y realizando consultas periódicas en busca de nuevas instrucciones. Entre las capacidades identificadas se encontraban la ejecución de expresiones PowerShell, la entrega y ejecución de archivos adicionales, la recopilación de información sobre las ventanas activas del sistema, la descarga de contenido remoto y la capacidad de eliminarse a sí mismo. El uso de un agente de usuario (useragent) personalizado, solicitudes HTTP POST dirigidas a un endpoint no estándar y técnicas de identificación (fingerprinting) del host mostraban un comportamiento claramente alineado con actividades de comando y control (beaconing) en lugar de corresponder a comportamientos legítimos de usuarios o aplicaciones autorizadas.

Entre los indicadores seleccionados asociados con organizaciones colombianas comprometidas se identificaron 45.83.31[.]136, 172.94.9[.]23 y love.negro[.]ink:4448. El caso demuestra la eficacia continua de señuelos legales y administrativos altamente localizados, combinados con ejecución basada en scripts y mecanismos de persistencia simples pero efectivos.

■ Apéndice B.

Análisis de Malware SnappyBee / DEEDRAT

SnappyBee consiste en un archivo DLL de carga y un archivo de datos cifrado que contiene código malicioso. Habitualmente se ejecuta mediante carga lateral de DLL (DLL sideloading) dentro de una aplicación legítima y firmada digitalmente, incluyendo software asociado con productos de seguridad, con el fin de reducir la visibilidad de la ejecución maliciosa. Entre los nombres de muestra observados se incluyen DgApi.dll e lmfsbDLL.dll.

Cuando se carga, la DLL utiliza DllMain para interceptar (hook) la función StartServiceCtrlDispatcherW y redirigir la ejecución hacia el cargador. Una vez activado, el malware localiza un archivo de datos como dbindex.dat, asigna memoria para alojarlo, descifra el shellcode mediante RC4, marca la región de memoria como ejecutable e inicia un proceso adicional de desempaqueado por etapas (staged unpacking). En fases posteriores resuelven funciones de la API mediante recorridos del PEB (Process Environment Block) basados en valores hash, con el fin de evitar almacenar directamente los nombres de funciones sensibles y dificultar el análisis.

La carga útil principal posteriormente descifra y carga en memoria funcionalidades similares a complementos (plugins) y establece comunicaciones con la infraestructura de comando y control (C2), proporcionando al operador un amplio control sobre el sistema comprometido. En campañas reportadas anteriormente, Salt Typhoon ha utilizado SnappyBee para mantener la persistencia y desplegar herramientas posteriores como DEMODEx. El caso brasileño analizado en este informe demuestra la relevancia de estas técnicas y procedimientos para los sectores estratégicos de América Latina y para entornos con infraestructura crítica expuesta.

Blind Eagle

Indicadores y Tácticas, Técnicas, Procedimientos (TTPs)

Los indicadores seleccionados incluyeron el agente de usuario Microsoft-WebDAV-MiniRedir/10.0.19045, la dirección IP 62[.]60[.]226[.]112, la ruta de la carga útil hxxp[.]/62[.]60[.]226[.]112/file/3601_2042.exe, el endpoint de DNS dinámico 21ene[.]jip-ddns[.]com y el nombre de host diciembrenota-senclub[.]musicalarga[.]com.

Los TTP observados y reportados incluyeron compromisos mediante navegación (drive-by compromise), explotación de aplicaciones expuestas a Internet (public-facing applications), archivos adjuntos de spear phishing, ejecución de Visual Basic y PowerShell, comunicaciones tipo beaconing hacia dominios y direcciones IP poco frecuentes, uso de puertos no estándar, transferencia de herramientas hacia entorno comprometido (ingress tool transfer), comportamiento asociado a la generación de dominios (DGA), técnicas de suplantación (masquerading), exfiltración de datos a través de canales de comando C2 y exfiltración hacia servicios de almacenamiento de texto o plataformas en la nube.

Hallazgos de threat hunting

Las actividades de threat hunting (caza de amenazas) de Darktrace para este informe se centraron en dos enfoques complementarios: el perfilado basado en actores utilizando el Modelo Diamante para el Análisis de Intrusiones (Diamond Model of Intrusion Analysis) y las investigaciones basadas en hipótesis construidas en torno a TTP recurrentes, comportamientos esperados e infraestructura conocida. El objetivo no fue elaborar perfiles exhaustivos de los actores de amenaza, sino evaluar si los reportes públicos y las observaciones previas de Darktrace se traducían en actividades reales y relevantes para la región dentro de la base de clientes.

BLIND EAGLE (APT-C-36)

Hipótesis: Se esperaba que Blind Eagle continuara utilizando correos electrónicos de phishing y archivos señuelos (lure files) que, finalmente, proporcionan acceso mediante VBScript, PowerShell y troyanos de acceso remoto (RAT), apoyándose en infraestructura de DNS dinámico y canales habituales de comando y control (C2) para mantener la persistencia y facilitar la exfiltración de datos.

Procedimiento: Darktrace combinó indicadores conocidos, convenciones esperadas de nomenclatura de archivos, infraestructura de DNS dinámico y lógica basada en el Lenguaje de Consulta de Eventos (EQL) para identificar comportamientos repetitivos a lo largo de la cadena de ataque dentro de la base de clientes. Asimismo, se utilizaron modelos existentes de Darktrace para identificar tareas programadas sospechosas, descargas de malware y conexiones salientes poco frecuentes con el objetivo de detectar posibles actividades maliciosas relacionadas.

Lo que observamos: Darktrace observó comunicaciones recurrentes con infraestructura vinculada a Remcos y múltiples endpoints de DNS dinámico asociados con patrones conocidos de VBScript. Dos cadenas de ataque completas incluyeron exfiltración de datos hacia endpoints de paste[.]ee, mientras que otros casos reflejaron comportamientos en etapas iniciales o intermedias fuertemente alineadas con las tácticas, técnicas y procedimientos (TTPs) utilizados por Blind Eagle durante 2025 y principios de 2026.

Por qué es importante: Estos hallazgos refuerzan la persistencia de las cadenas de intrusión impulsadas por phishing en América Latina y muestran cómo herramientas de bajo costo pueden reutilizarse a gran escala en distintos sectores y países. Para los defensores, el éxito continuo de estas técnicas destaca la necesidad de monitorear la ejecución de scripts, la

creación de tareas programadas, las conexiones salientes poco frecuentes y los comportamientos anómalos de descarga iniciados por los usuarios.

EARTH ALUX

Hipótesis: O Earth Alux exploraría sistemas vulnerables expuestos a Hipótesis: Se esperaba que Earth Alux explotara sistemas vulnerables expuestos a Internet, utilizara mecanismos de ejecución de bajo perfil (low-noise execution) y canales de comando vinculados a servicios en la nube, para finalmente exfiltrar datos mediante almacenamiento controlado por el atacante o a través de canales encubiertos.

Procedimiento: Debido a la limitada disponibilidad de indicadores públicos, Darktrace adoptó un enfoque basado en TTP y con un uso reducido de indicadores de compromiso (IOC-light). La investigación se centró en actividades sospechosas relacionadas con dispositivos expuestos a Internet, conectividad externa inusual, posibles comunicaciones de C2 y la exfiltración hacia destinos de almacenamiento en la nube.

Lo que observamos: La investigación se centró en patrones de comportamiento en lugar de una única firma de malware, o familia específica, reflejando cómo los actores avanzados reducen la eficacia de los indicadores basados en infraestructuras estáticas. El enfoque basado en el comportamiento sigue siendo el método más eficaz para detectar campañas sigilosas que explotan sistemas expuestos a Internet y servicios legítimos, dificultando su identificación mediante indicadores tradicionales.

Por qué importa: La relevancia de Earth Alux para América Latina radica en el propio modelo de ataque: la explotación de infraestructura expuesta, seguida de persistencia sigilosa y exfiltración vinculada a la nube. Este patrón resulta directamente aplicable a organizaciones de la región que amplían servicios accesibles desde Internet sin realizar inversiones equivalentes en capacidades de detección y monitoreo en la nube.

USO DE IA GENERATIVA / AGÉNTICA

Hipótesis: Los actores de amenaza podrían experimentar con asistentes de IA que incorporan capacidades de navegación web o recuperación de información (retrieval) como posibles canales de comunicación encubiertos, utilizando solicitudes estructuradas para ocultar información sensible y facilitar la entrega indirecta de instrucciones operativas por parte de los atacantes.

Procedimiento: Darktrace correlacionó la cadena de ataque descrita públicamente como "IA como proxy de C2" con comportamientos potencialmente observables a nivel de red y plataforma. Posteriormente, utilizó lógica (Event Query Language) EQL y modelos de detección para identificar accesos sospechosos a servicios de IA como OpenAI, Perplexity, DeepSeek, Copilot, Gemini, Claude, Grok, Janitor AI y Flow XO especialmente cuando dichas actividades estaban acompañadas por indicadores asociados a beaconing, comportamientos similares a algoritmos de generación de dominios similar a DGA (DGA-like) o posibles señales exfiltración de datos.

Lo que observamos: La investigación se centró en identificar combinaciones anómalas entre el acceso saliente a servicios de IA y otros indicadores que podrían sugerir actividades de comando y control (C2) o exfiltración de datos por etapas preparatorias. Aunque esta área continúa siendo emergente, su relevancia aumenta a medida que las plataformas de IA se integran cada vez más en los entornos empresariales y pasan a formar parte de los flujos de trabajo cotidianos.

Por qué importa: Aunque estas técnicas siguen siendo en gran medida experimentales, el uso de IA como facilitador de comunicaciones C2 demuestra cómo los actores de amenaza pueden aprovechar servicios legítimos para ocultar actividad maliciosa y dificultar aún más la diferenciación entre comportamientos legítimos y actividades sospechosas. A medida que la adopción de herramientas de IA se acelera, las organizaciones necesitarán una comprensión más sólida del contexto de uso, incluyendo qué servicios se utilizan, quién los utiliza y cómo se relacionan esos accesos con otros eventos de seguridad relevantes.

Bibliografía

- [1] [En línea]. Disponible: <https://edgeuno.com/2026-connectivity-ai-edge/>
- [2] [En línea]. Disponible: <https://identitymanagementinstitute.org/identity-threats-reshaping-cybersecurity/>
- [3] [En línea]. Disponible: <https://diesec.com/2026/04/legitimate-tool-abuse>
- [4] [En línea]. Disponible: <https://www.darkreading.com/threat-intelligence/latin-americas-cyber-maturity-lags-threat-landscape>
- [5] [En línea]. Disponible: <https://www.crowdstrike.com/en-us/blog/2025-latam-threat-landscape-report-deep-dive>
- [6] [En línea]. Disponible: <https://www.recordedfuture.com/research/latin-america-and-the-caribbean-cybercrime-landscape>
- [7] [En línea]. Disponible: <https://www.csis.org/analysis/chinas-expanding-interests-latin-america-development-leverage-coercion-and-crime>
- [8] [En línea]. Disponible: <https://privatebank.jpmorgan.com/latam/en/insights/markets-and-investing/ideas-and-insights/the-cybersecurity-imperative-latin-americas-challenge-and-opportunity>
- [9] [En línea]. Disponible: <https://blog.checkpoint.com/security/securing-latin-america-in-2025-how-ai-and-cyber-threat-intelligence-are-reshaping-the-cyber-security-landscape>
- [10] [En línea]. Disponible: <https://www.redgealc.org/contenido-general/noticias/colombia-realizo-cumbre-de-inteligencia-artificial>
- [11] [En línea]. Disponible: <https://www.redgealc.org/contenido-general/noticias/idforo>
- [12] [En línea]. Disponible: <https://www.redgealc.org/contenido-general/noticias/se-presentaron-avances-de-idlac-en-washington-dc>
- [13] [En línea]. Disponible: <https://www.galileo-ft.com/blog/whats-driving-colombias-fintech-revolution-in-2025-data-driven-market-analysis>
- [14] [En línea]. Disponible: <https://alcor.com/software-development-colombia>
- [15] [En línea]. Disponible: <https://www.trade.gov/country-commercial-guides/colombia-information-and-communication-technology-ict>
- [16] [En línea]. Disponible: <https://www.datacubereseach.com/colombia-cloud-computing-market>
- [17] [En línea]. Disponible: <https://www.ventasdeseguridad.com/en/news/latest-news/431-enterprises/25510-colombia-accounts-for-one-out-of-every-four-cyberattacks-in-latin-america.html>
- [18] [En línea]. Disponible: <https://blog.checkpoint.com/research/the-growing-danger-of-blind-eagle-one-of-latin-americas-most-dangerous-cyber-criminal-groups-targets-colombia>
- [19] [En línea]. Disponible: <https://thehackernews.com/2025/08/blind-eagles-five-clusters-target.html>
- [20] [En línea]. Disponible: <https://www.kiteworks.com/cybersecurity-risk-management/latin-america-cyber-threat-landscape-2026-intel-471-report>
- [21] [En línea]. Disponible: <https://www.ibm.com/think/insights/unveiling-latest-banking-trojan-threats-latam>
- [22] [En línea]. Disponible: <https://accesspartnership.com/opinion/access-alert-colombia-releases-national-digital-strategy-2023-2026>
- [23] [En línea]. Disponible: <https://www.trade.gov/country-commercial-guides/colombia-digital-economy>
- [24] [En línea]. Disponible: <https://www.trade.gov/country-commercial-guides/chile-information-technologies>
- [25] [En línea]. Disponible: <https://thehackernews.com/2025/05/horabot-malware-targets-6-latin.html>
- [26] [En línea]. Disponible: <https://www.trade.gov/market-intelligence/chile-information-technology-new-cybersecurity-framework-law>
- [27] [En línea]. Disponible: <https://alcor.com/overview-of-the-technology-industry-in-mexico/>

-
- [28] [En línea]. Disponible: <https://alcor.com/outsourcing-to-latin-america/>
- [29] [En línea]. Disponible: <https://mexicobusiness.news/cybersecurity/news/many-mexican-firms-hit-supply-chain-cyberattacks-kaspersky>
- [30] [En línea]. Disponible: <https://mexicobusiness.news/cybersecurity/news/mexico-unveils-national-cybersecurity-plan-2025-2030>
- [31] [En línea]. Disponible: <https://mexicobusiness.news/cybersecurity/news/mexico-mandates-zero-trust-across-federal-agencies>
- [32] [En línea]. Disponible: <https://investmentpolicy.unctad.org/investment-policy-monitor/measures/4930/launches-the-brazilian-artificial-intelligence-plan-2024-2028>
- [33] [En línea]. Disponible: <https://www.itic.org/news-events/techwonk-blog/realizing-brazils-ai-ambition-through-futureproof-regulation>
- [34] [En línea]. Disponible: <https://blog.equinix.com/blog/2025/05/07/the-digital-pulse-of-latin-america-brazils-rise-as-a-global-tech-innovator>
- [35] [En línea]. Disponible: <https://blog.lacnic.net/en/the-perfect-storm-the-largest-cyberattack-on-brazils-financial-system>
- [36] [En línea]. Disponible: <https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-is-the-worlds-second-most-vulnerable-country-to-cyberattacks>
- [37] [En línea]. Disponible: <https://socradar.io/wp-content/uploads/2024/10/SOCRadar-Brazil-Threat-Landscape-Report-2024.pdf>
- [38] [En línea]. Disponible: <https://medium.com/aardvark-infinity/comprehensive-list-of-brazilian-apt-groups-4cfbec72a1d6>
- [39] [En línea]. Disponible: <https://www.mattosfilho.com.br/en/unico/cybersecurity-strategy-decree>
- [40] [En línea]. Disponible: <https://digi-tracker.com/regulations/national-cybersecurity-policy-pnciber/?format=pdf&content-Lang=eng-GB&v=1>
- [41] [En línea]. Disponible: <https://iclg.com/practice-areas/data-protection-laws-and-regulations/brazil>
- [42] [En línea]. Disponible: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/brazil>
- [43] [En línea]. Disponible: <https://www.trade.gov/country-commercial-guides/ecuador-digital-economy>
- [44] [En línea]. Disponible: <https://www.bnamerica.com/en/features/spotlight-ecuadors-new-digital-transformation-policy>
- [45] [En línea]. Disponible: <https://freedomhouse.org/country/ecuador/freedom-net/2024>
- [46] [En línea]. Disponible: <https://www.dexpose.io/tengu-ransomware-targets-anfibius-in-ecuador>
- [47] [En línea]. Disponible: <https://appcheck-ng.com/ecuador-citizens-data-leak>
- [48] [En línea]. Disponible: https://link.springer.com/chapter/10.1007/978-981-96-8563-9_44
- [49] [En línea]. Disponible: <https://eandt.theiet.org/2019/04/17/ecuador-faced-40-million-ddos-attacks-after-assange-arrest>
- [50] [En línea]. Disponible: <https://database.cyberpolicyportal.org/entity/v939ugxukzg?file=1658911956789x9ant1tq6k.pdf&page=1>
- [51] [En línea]. Disponible: <https://www.telecomunicaciones.gob.ec/el-gobierno-nacional-presento-la-estrategia-nacional-de-ciberseguridad>
- [52] [En línea]. Disponible: <https://www.dlapiperdataprotection.com/index.html?t=law&c=EC>
- [53] [En línea]. Disponible: <https://www.centerforcybersecuritypolicy.org/insights-and-research/bridging-the-cybersecurity-gap-in-latam-how-isacs-enhance-regional-cooperation>
- [54] [En línea]. Disponible: <https://www.weforum.org/stories/2024/05/latin-america-cybersecurity-report-ransomware-attacks>
- [55] S. Smart, Business, Human Rights, Technology, and Transitional Justice in Latin America: Tracing Connections, Palgrave Macmillan, 2025.
- [56] [En línea]. Disponible: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026_Regional_Analysis_Latin-America_and_the_Caribbean.pdf
- [57] [En línea]. Disponible: https://api.gcforum.org/api/files/public/upload/39c147e6-27f2-418c-99ea-c5a1890a0c8b_Bridging-the-Gender-Gap-in-Cybersecurity.pdf
- [58] [En línea]. Disponible: <https://iapp.org/news/a/brazils-lgpd-now-in-effect-what-does-this-mean-for-enforcement>
- [59] [En línea]. Disponible: <https://blog.checkpoint.com/research/latin-america-sees-sharpest-rise-in-cyber-attacks-in-december-2025-as-ransomware-activity-accelerates/>
- [60] [En línea]. Disponible: <https://fpf.org/blog/chiles-new-data-protection-law-context-overview-and-key-takeaways>

■ **Sobre Darktrace**

Darktrace es líder mundial en IA para la ciberseguridad y ayuda a las organizaciones a anticiparse cada día a un panorama de amenazas en constante evolución. Fundada en 2013 en Cambridge, Reino Unido, Darktrace proporciona la plataforma de ciberseguridad esencial para proteger a las organizaciones frente a amenazas desconocidas mediante una IA que aprende de cada empresa en tiempo real. La plataforma y los servicios de Darktrace cuentan con el respaldo de 2.300 empleados que protegen a cerca de 10.000 clientes en todo el mundo. Para obtener más información, visite darktrace.com.