
PROBLEMAS DE LA SEGURIDAD

DESAFÍOS DE LA CIBERSEGURIDAD PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS*

Diana Pamela Chávarry Gálvez

Ph.D. (Economía) (chavarri_galves_d@pfur.ru)

Profesora docente

Departamento de Modelado Económico y Matemático

Universidad Rusa de la Amistad de los Pueblos P. LUMUMBA
(RUDN Universidad)

Miklukho-Maklaya, 6, Moscú, 117198, Federación de Rusia

SPIN-código: 3015-9115; ORCID: 0000-0002-9201-9256;

Researcher ID: HOA-5632-2023; Scopus Author ID: 57230104500

Svetlana Y. Révinova

Ph.D. (Economía) (revinova_syu@pfur.ru)

Profesora asociada

Departamento de Modelado Económico y Matemático

Universidad Rusa de la Amistad de los Pueblos P. LUMUMBA
(RUDN Universidad)

Miklukho-Maklaya, 6, Moscú, 117198, Federación de Rusia

SPIN-código: 8036-1220; ORCID: 0000-0002-2442-2393;

Researcher ID: Q-7857-2018; Scopus Author ID: 56596756800

Recibido el 14 de febrero de 2025

Aceptado el 25 de abril de 2025

DOI: 10.37656/s20768400-2025-02-03

Resumen. Este artículo busca examinar principales amenazas para las pequeñas y medianas empresas en América Latina en materia de ciberseguridad, identificar los países y sectores económicos más vulnerables a las ciberamenazas y determinar los factores que dificultan la implementación efectiva de medidas de ciberseguridad para este tipo de empresas. Se hace énfasis en las principales amenazas en materia de ciberseguridad para las pequeñas y medianas empresas y se analizan los factores que dificultan la implementación más activa de programas de ciberseguridad a nivel regional y nacional. Se analiza la situación en los

Desafíos de la ciberseguridad para las pequeñas y medianas empresas

países más afectados por la ciberdelincuencia (Brasil, México y Chile) y en aquellos donde se están implementando medidas más efectivas para mejorar la situación.

Palabras clave: *América Latina, ciberseguridad, seguridad informática, economía digital, cibercrimen, pequeñas y medianas empresas*

* Estudio financiado por la Fundación Científica de Rusia (RNF). Proyecto 24-78-00165 “Mecanismos para ampliar la cooperación en el campo de las tecnologías digitales entre Rusia y los países de América Latina”.

CYBERSECURITY CHALLENGES FOR SMALL AND MEDIUM ENTERPRISES*

Diana Pamela Chavarri Galvez

*Ph.D. (Economics) (chavarri_galves_d@pfur.ru)
Senior lecturer*

Department of Economic and Mathematical Modeling

*P. LUMUMBA Peoples' Friendship University of Russia (RUDN University)
6, Miklukho Maklaya, Moscow, 117198, Russian Federation*

SPIN-code: 3015-9115; ORCID: 0000-0002-9201-9256;

Researcher ID: HOA-5632-2023 Scopus Author ID: 57230104500

Svetlana Y. Revinova

*Ph.D. (Economics) (revinova_syu@pfur.ru)
Associate Professor*

Department of Economic and Mathematical Modeling

*P. LUMUMBA Peoples' Friendship University of Russia (RUDN University)
6, Miklukho Maklaya, Moscow, 117198, Russian Federation*

SPIN-code: 8036-1220; ORCID: 0000-0002-2442-2393;

Researcher ID: Q-7857-2018; Scopus Author ID: 56596756800

Received on February 14, 2025

Accepted on April 25, 2025

DOI: 10.37656/s20768400-2025-02-03

Abstract. *This article aims to examine the main threats to small and medium enterprises in Latin America in the field of cybersecurity, identify the countries and sectors of the economy most vulnerable to cyber threats, and determine the factors that hinder the effective implementation of*

Diana Pamela Chávarry Gálvez, Svetlana Y. Révinova

cybersecurity measures for this type of enterprise. The key threats in the field of cybersecurity for small and medium businesses are identified and the factors that hinder the most active implementation of cybersecurity programs at both the regional and national levels are analyzed. The situation in countries that suffer the most from cybercrime (Brazil, Mexico, and Chile) and in those that are taking more effective measures to improve the situation are considered.

Keywords: Latin America, cybersecurity, cyber threats, information security, digital economy, computer security, cybercrime, small and medium businesses

* The research was funded by Russian Scientific Foundation (RNF). Project 24-78-00165 “Mechanisms for Expanding Cooperation in the Field of Digital Technologies between Russia and Latin American Countries”.

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЙ*

Диана Памела Чаварри Гальвес

Канд. экон. наук (chavarri_galves_d@pfur.ru)

Старший преподаватель

Кафедра экономико-математического моделирования

Российский университет дружбы народов имени П. Лумумбы (РУДН)

РФ, Москва, 117198, ул. Миклухо-Маклая, 6

SPIN-код: 3015-9115; ORCID: 0000-0002-9201-9256;

Researcher ID: HOA-5632-2023; Scopus Author ID: 57230104500

Светлана Юрьевна Ревина

Канд. экон. наук (revinova_sy@pfur.ru)

Доцент

Кафедра экономико-математического моделирования

Российский университет дружбы народов имени П. Лумумбы (РУДН)

РФ, Москва, 117198, ул. Миклухо-Маклая, 6

SPIN-код: 8036-1220; ORCID: 0000-0002-2442-2393;

Researcher ID: Q-7857-2018; Scopus Author ID: 56596756800

Статья получена 14 февраля 2025 г.

Статья принята 25 апреля 2025 г.

DOI: 10.37656/s20768400-2025-02-03

Аннотация. В данной статье поставлена задача рассмотреть основные угрозы для малых и средних предприятий Латинской Америки в сфере кибербезопасности, выделить наиболее уязвимые к киберугрозам страны и отрасли экономики, определить факторы, препятствующие эффективному внедрению мер по кибербезопасности для этого типа предприятий. Выделены ключевые угрозы в области кибербезопасности для предприятий малого и среднего бизнеса и проанализированы факторы, препятствующие наиболее активному внедрению программ в сфере кибербезопасности как на региональном, так и на национальном уровне. Рассмотрена ситуация в странах, которые в наибольшей степени страдают от киберпреступлений (Бразилия, Мексика и Чили), и в тех, где предпринимаются более эффективные меры по улучшению ситуации.

Ключевые слова: Латинская Америка, кибербезопасность, информационная безопасность, цифровая экономика, киберпреступность, малый и средний бизнес

* Исследование выполнено при финансовой поддержке Российского научного фонда (РНФ). Проект № 24-78-00165 «Механизмы расширения сотрудничества в сфере цифровых технологий между Россией и странами Латинской Америки».

Introducción

Las ciberamenazas o amenazas a la seguridad informática son una de las tendencias más problemáticas en el contexto del rápido desarrollo de la economía digital. Esta tendencia se ha agudizado más que nada luego de la pandemia de COVID-19, que fue un factor de crecimiento del volumen de transacciones comerciales alrededor del mundo. Más del 60% de estas transacciones, según algunas estimaciones, se realizan a través de billeteras electrónicas e Internet [1]. Sin embargo, mientras que las grandes empresas tienen posibilidades de instalar sistemas de seguridad avanzados para sus computadores, servidores, dispositivos móviles, bases de datos, las pequeñas y medianas empresas son más vulnerables en este aspecto. Además, debido al desarrollo desigual de las tecnologías digitales en determinadas regiones del mundo, surge otra

situación de especial vulnerabilidad para los pequeños y medianos emprendimientos al adentrarse al mercado internacional. Esto fundamenta la relevancia de identificar los problemas de ciberseguridad, en parte, en América Latina, donde el sector de pequeña y mediana empresa abarca casi la totalidad de negocios. Aunque los procesos de digitalización en la región latinoamericana actualmente están avanzando rápidamente, la infraestructura informática y de telecomunicaciones se ve seriamente retrasada en comparación con los países líderes en esta área, que a su vez posibilita el aumento de amenazas en cuanto a ciberseguridad. Según el Índice Global de Ciberseguridad 2024, que calcula la Unión Internacional de Telecomunicaciones (UIT), América Latina tiene el mayor nivel de cibercrimen en comparación con otras regiones [2]. Hasta la fecha, se ha formado una amplia gama de trabajos dedicados a cuestiones de ciberseguridad en la literatura científica. Sin embargo, la investigación sobre este problema en los países latinoamericanos es insuficiente, a pesar de que ha cobrado especial relevancia para pequeñas y medianas empresas (PYMES) a partir de 2020. Entre los autores de trabajos que abordan aspectos de la ciberseguridad en el segmento de las PYMES, destacan Louise Marie Hurel [3], Ilona T. Stadnik y Natalia A. Tsvetkova [4], Alvaro José Chaves Guzmán [5], Anna Urbanovics, [6], Ecaterina Kosevich [7], Radomir Bolgov [8], entre otros. Sin embargo, los trabajos de estos autores no ofrecen un análisis exhaustivo de los problemas de ciberseguridad que enfrentan las PYMES en América Latina.

Materiales y métodos

En la investigación se utilizaron métodos científicos generales de análisis y síntesis, método estadístico, método de índice, método de agrupación y método de generalización. Los materiales para la elaboración del artículo fueron estudios de investigadores rusos y extranjeros sobre ciberseguridad en pequeñas y medianas empresas, incluyendo las de América Latina. Fueron utilizadas publicaciones de revistas científicas,

tales como *América Latina, Iberoamérica, Journal of Governance and Development, Strategic Paper, Per Concordiam*. También fue utilizada información de los sitios web de ministerios y organismos oficiales de los países latinoamericanos, datos del Índice global de ciberseguridad.

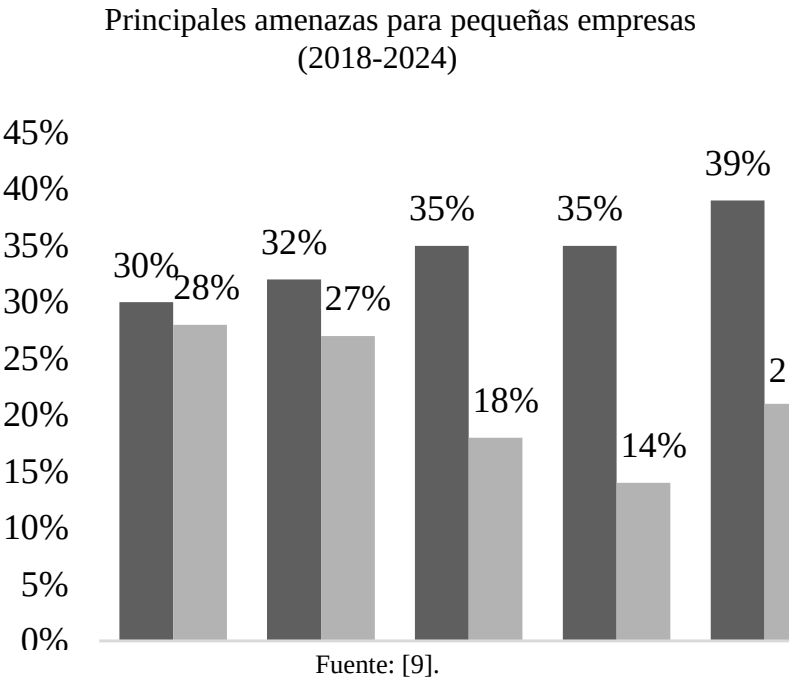
Ciberseguridad en las pequeñas y medianas empresas

La ciberseguridad (o seguridad informática, digital) se refiere a un conjunto de métodos e instrumentos para la protección de computadores, servidores, dispositivos móviles y bases de datos ante acciones malintencionadas. El objetivo principal de la ciberseguridad es mantener a salvo la información y prevenir daños a los sistemas informáticos o a los usuarios. Se pueden resaltar varios enfoques en cuanto a la seguridad en esta categoría: seguridad de las redes (protección de las redes informáticas frente a amenazas externas, como pueden ser virus o ataques directos para robar los datos); seguridad de las aplicaciones (protección de teléfonos móviles, que pueden verse amenazados al instalar aplicaciones); seguridad informática (garantizar la integridad y confidencialidad de los datos tanto durante su almacenamiento, como durante su transmisión), etc.

En las últimas dos décadas, a medida que la cuestión de garantizar la seguridad, la integridad y la confidencialidad de la información se presenta como algo crítico, crece la importancia de implementar instrumentos, capaces de manera efectiva salvaguardar la información en las empresas, que a su vez permitirían una minimización real de las amenazas a sus actividades comerciales. De acuerdo con datos del portal *Statista*, los riesgos clave para las pequeñas empresas, en el período de 2018 al 2024, fueron los crímenes cometidos a través de Internet, fallas en la infraestructura informática y fugas de datos (fue encuestado el 32% de los representantes del sector de pequeñas empresas). Desastres naturales también fueron

mencionados por el 24% de los encuestados, aunque las amenazas de este tipo se consideraron menos significantes (Diagrama 1).

Diagrama 1



El garantizar la seguridad informática para pequeñas y medianas empresas teniendo en cuenta su mayor vulnerabilidad en el mercado en comparación con grandes compañías permite minimizar diferentes riesgos, entre ellos, relacionados a pérdidas económicas, tecnológicas, de reputación o de personal, de producción, etc. Una importancia especial es la que adquiere la seguridad informática de las pequeñas y medianas empresas en los países en desarrollo.

Resultados

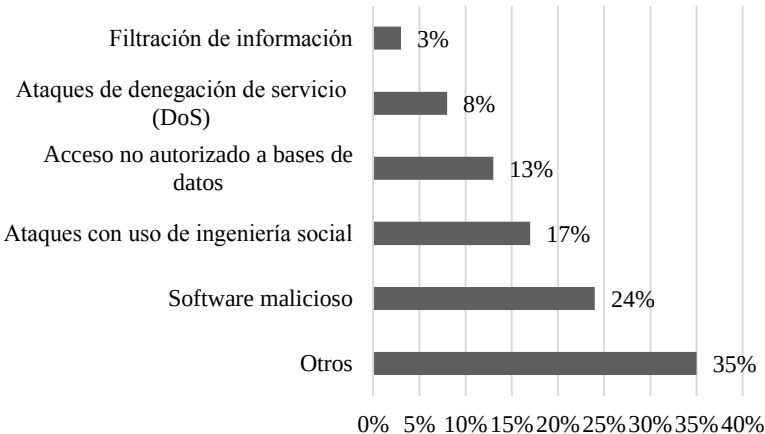
El nivel de digitalización en la región latinoamericana es muy desigual. El elevado coste de tráfico de Internet, el bajo desarrollo del comercio electrónico en varios países retrasados en cuanto al nivel de digitalización, la inaccesibilidad a Internet en algunas zonas remotas de ciertos países, etc., pueden verse más complicados por el alto riesgo de delitos informáticos que se tiene debido a la ausencia de una distribución masiva entre las PYMES de sistemas de seguridad ante ataques cibernéticos.

Durante una investigación, resultados de la cual están disponibles en el portal *Statista*, fueron identificadas áreas clave de los delitos informáticos con los que las PYMES se encuentran más frecuentemente. El 24% de los encuestados resalta el software malicioso, el 17%, ataques con uso de manipulación o ingeniería social, mientras que el 13% de los encuestados resalta el acceso no autorizado a bases de datos o a aplicaciones (Diagrama 2).

Según una encuesta de dirigentes de seguridad informática de todo el mundo, realizada en 2024 y disponible en el portal *Statista* (entre los países latinoamericanos, participó Brasil), los principales temores de los directivos de empresas brasileñas son los siguientes factores, relacionados a ciberseguridad: un paro de los procesos comerciales (el 45% de los encuestados), pérdida de clientes actuales (el 42%), impacto en la valuación de la empresa (el 38%), pérdida de beneficios (el 38%), pérdidas en cuanto a reputación (el 33%) [11].

Diagrama 2

Principales ciberdelitos en las empresas de América Latina



Fuente: elaboración de las autoras a base de [10].

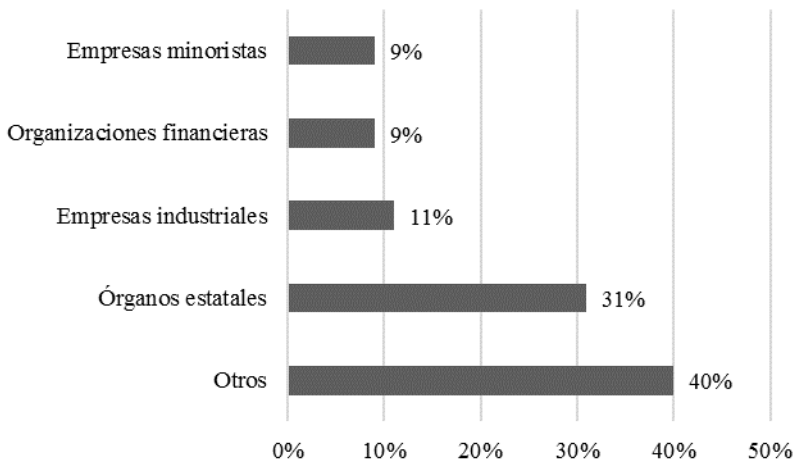
Según los datos de *Positive Technologies*, ataques de extorsionadores, que hoy día son un problema actual en todos los países del mundo, en Latinoamérica poseen indicadores más altos. Tales ataques afectan las actividades del 52% de las pequeñas y medianas empresas y resultan en consecuencias negativas tales como: interrupción de procesos de producción debido a la pérdida de acceso a la infraestructura informática o a la de datos en general. En la región latinoamericana, los ataques de extorsión en gran parte están dirigidos a conseguir información de compañías para luego explotarla en el mercado negro. Este problema más que nada afecta a Brasil, México y Argentina. Por ejemplo, a las PYMES de Brasil fue dirigido el 22% de todos los ciberataques en la región en el año 2022, a las PYMES en México, el 12%, en Argentina, el 10%, luego le siguen Costa Rica con el 9%, Colombia, con el 9% y Chile, con el 8% del total de ciberataques en la región [12].

Desafíos de la ciberseguridad para las pequeñas y medianas empresas

Según *Positive Technologies*, la mayor parte de los ataques fue dirigida a órganos estatales y complejos industriales. También son afectados por estos ataques empresas del sector financiero y empresas minoristas (Diagrama 3).

Diagrama 3

Estructura de ciberataques en Latinoamérica por sectores del Estado y economía



Fuente: [12].

También se puede mencionar el porcentaje de empresas que han sido víctimas de ciberataques por países en América Latina. Más que nada estas empresas se han encontrado en Ecuador (el 70%) y Paraguay (el 70%). La menor cantidad se encuentra en Panamá, aunque las cifras siguen siendo altas (el 54%) (Cuadro 1).

Cuadro 1

Porcentaje de empresas, víctimas de delitos informáticos por países de Latinoamérica

Nº	País	Porcentaje del total de empresas, %	Nº	País	Porcentaje del total de empresas, %
1	Ecuador	70	7	Argentina	59
2	Paraguay	70	8	Colombia	58
3	Brasil	60	9	Perú	58
4	Costa Rica	60	10	El Salvador	58
5	Honduras	60	11	Chile	55
6	México	59	12	Panamá	54

Fuente: elaboración de las autoras sobre los datos de [13].

La mayor parte de los ciberataques, dirigidos a usuarios o infraestructuras en concreto, se observan en Brasil (el 56% de todos los casos en la región), también en México (el 28%) y Colombia (el 10%). Desde el año 2020 en América Latina se registra un aumento crítico de ciberataques. Además, en comparación con los indicadores promedios a nivel mundial, en la región latinoamericana fueron identificados los niveles más altos de cibercrimen en el mundo [14].

Las pequeñas y medianas empresas, que llevan a cabo su actividad en Latinoamérica, se enfrentan a ciberataques por los siguientes motivos: falta de recursos financieros para obtener sistemas de protección de mayor calidad ante ciberataques; un débil nivel de conocimientos sobre los algoritmos para la detección de riesgos informáticos, falta de ofertas que sigan el criterio “calidad – precio” en el mercado de ciberseguridad, etc.

En relación a esto es que crece la necesidad de realizar medidas concretas para resolver el problema de ciberamenazas en las PYMES. Para reducir el nivel de su vulnerabilidad ante ellas, se deben considerar dos aspectos clave: en primer lugar, medidas tomadas por parte del Estado, y planes a realizarse por las propias PYMES. Sin embargo, hay que entender, que

medidas más amplias y, por consiguiente, más eficaces, pueden ser tomadas sólo a nivel estatal con políticas de ciberseguridad.

Resaltamos que a nivel internacional a la lucha contra el cibercrimen se unieron sólo algunos países de Latinoamérica. El Convenio de Budapest sobre la ciberdelincuencia fue firmado por Brasil, Argentina, Colombia, Chile y Costa Rica [12]. En cuanto al nivel regional, la armonización de las cuestiones de ciberseguridad también avanza muy lentamente. Más que nada, estas cuestiones se incluyen en el orden del día en las reuniones de diversas organizaciones regionales, tales como la Organización de los Estados Americanos (OEA), Comunidad de Estados Latinoamericanos y Caribeños (CELAC), entre otras. Con la firma de la Estrategia Interamericana Integral de Seguridad Cibernética en el 2004 en el marco de la OEA se hizo un intento de reglamentar y unificar la resolución de problemas relacionados al cibercrimen en la región latinoamericana. Sin embargo, este documento, que ya tiene 20 años de vigencia, no está actualizado y no tiene en cuenta nuevas tendencias en el área de cibercrimen. En el año 2012 los países de la OEA adoptaron la Declaración del Fortalecimiento de la Seguridad Cibernética en las Américas [15], la cual contiene puntos concretos sobre la lucha contra las amenazas cibernéticas, entre ellas se destaca la urgencia de formar grupos especializados, dirigidos al desarrollo de medidas contra los delitos informáticos y a la mejora de la infraestructura informática para hacerles frente. También se puede mencionar la Declaración sobre el fortalecimiento de la ciberseguridad, adoptada en 2012 por el Comité Interamericano contra el Terrorismo. La aprobación de estos documentos por una parte de los países de América Latina permitió alcanzar cierto entendimiento mutuo, principalmente, en cuanto a intercambio de informaciones en la lucha contra los ciberdelitos [4], aunque varias cuestiones siguen sin contemplarse.

Por otro lado, la actividad en las organizaciones regionales dedicadas a cuestiones de ciberseguridad en Latinoamérica no es tan alta [6]. Por ejemplo, en el programa de ciberseguridad de la OEA los más activos participantes son apenas algunos países – Colombia, Paraguay, Chile y México.

Cabe mencionar que en ciertos países de Latinoamérica han sido adoptadas estrategias propias de ciberseguridad, pero éstas no permiten desarrollar un sistema común regional de ciberseguridad ante amenazas [16] y llevar a cabo una política más efectiva en esta área.

Por lo tanto, hoy día Latinoamérica está en una situación, en la cual planes estratégicos nacionales en el área de ciberseguridad dificultan el desarrollo de un sistema único de ciberseguridad regional. Además, está claro que sin un sistema como tal se vuelve muy difícil la coordinación de las acciones entre los Estados contra tales crímenes, que no solo afectan a la región, sino que son problemas actuales para todos los países del mundo.

Las ciberamenazas son muy actuales para todos, pero hay países en los cuales se llevan a cabo intentos más sólidos para hacerles frente. Colombia siempre se ha destacado por el alto nivel de crimen (que hoy día está abarcando el sector digital), se unió a la lucha contra los crímenes cibernéticos ya hace dos décadas. Desde el año 2007 el gobierno colombiano realiza intentos para disminuir el número de crímenes a través de Internet. En 2011, Colombia fue el primer país latinoamericano que aprobó una Estrategia Nacional de Ciberseguridad que en 2016 fue seriamente reformada y recibió un nuevo nombre – Política Nacional de Seguridad Digital [17]. Como sus objetivos clave se tomaron tres direcciones: mejorar la base normativa y legal, la cual coordinaría medidas a tomarse para la lucha contra el cibercrimen; fortalecer la cooperación internacional en el área de ciberseguridad; ampliar programas científicos y educativos en el área de lucha contra el cibercrimen. Resulta interesante,

cómo para la realización de los mencionados objetivos en Colombia se crearon varios órganos: Comisión Intersectorial en Materia de Ciberseguridad y Ciberdefensa, Equipo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT), Comando Conjunto Cibernético de las Fuerzas Militares de Colombia, Centro Cibernético Policial [5]. Sin embargo, hay que constatar que, a pesar de ciertos éxitos con las medidas tomadas, no han llevado a los resultados esperados: Colombia sigue siendo uno de los países con los más altos indicadores de ciberdelito en Latinoamérica junto con México y Brasil. En conjunto, en estos tres países tienen lugar 9 nueve de cada 10 casos registrados de ciberataques en la región [18].

Hasta el año 2020 sólo algunos países poseían estrategias de ciberseguridad: Colombia (2011), Panamá (2017), Paraguay (2017), Chile (2017), Costa Rica (2017), México (2017) y Argentina (2019) [3]. Desde nuestro punto de vista, la presente situación la justifican varias razones, concretamente: infravaloración de la importancia de estrategias de ciberseguridad; infravaloración de la seriedad de las amenazas cibernéticas no sólo para las PYMES, sino también para el desarrollo económico, social y político de los países; ausencia de experiencia formando estrategias en sectores similares; falta de comprensión de las formas específicas de abordar los problemas relacionados con el delito cibernético y otros factores.

En 2020, debido a las consecuencias sin precedentes de la pandemia de COVID-19 y a la necesidad de resolver una serie de retos en el área de ciberseguridad, 18 países de Latinoamérica hicieron intentos para desarrollar estrategias nacionales en esta área. Sin embargo, sólo 12 países consiguieron lo propuesto. El más activo en tales procesos es Brasil. En 2020, el gobierno brasileño adoptó urgentemente la Estrategia Nacional de Ciberseguridad (E-Ciber). Su adopción fue motivada por serios problemas, caracterizados por un aumento drástico de

ciberataques, debido a los cuales sufrieron más que nada las PYMES. En la estrategia E-Ciber se priorizan las siguientes directrices: cooperación nacional e internacional; integración de conocimientos, sostenibilidad de los esfuerzos; educación relacionada con la ciberseguridad [3]. El gobierno brasileño pretende aplicar una serie de medidas alineadas con las tareas de la estrategia E-Ciber, incluida la protección de las PYMES, que a su vez impulsan el desarrollo económico del país.

En 2024 en otro gran país latinoamericano –Argentina– fue adoptada Resolución sobre la Utilización de Inteligencia Artificial (IA) a nivel estatal y fue creado un Departamento Especial de Inteligencia Artificial para la lucha contra el delito cibernético. Hoy día oficialmente tiene lugar un monitoreo de las redes sociales con inteligencia artificial, se realizan patrullas de territorios extensos mediante drones, se procesan grandes cantidades de datos provenientes de varias fuentes, se identifican transacciones sospechosas, etc. Todas estas medidas permiten a su vez una garantía adicional de protección para las PYMES.

Como se ha mencionado anteriormente, el país más activo en la lucha contra el cibercrimen es Colombia. Entre tanto, las medidas colombianas están dirigidas tanto a la protección de sectores bajo el control del Estado, como a la protección de empresas independientes. Hasta el año 2020, cuando la introducción de sistemas de ciberseguridad en Latinoamérica no era tan activa, el 72% de las empresas ya poseían ciertos programas y productos para la minimización de riesgos informáticos y amenazas. Entre ellos, programas antivirus, sistemas cortafuegos o *firewall*, programas para la segura duplicación de datos [11].

Con el objetivo de hacer frente al problema de las amenazas cibernéticas para las PYMES en América Latina es importante el adquirir productos de seguridad de calidad, pero asequibles. Sin embargo, su mercado en Latinoamérica aún está poco

desarrollado, lo que dificulta la búsqueda de variantes óptimas para las PYMES con recursos limitados.

Según opiniones de expertos, para el año 2028 el mercado de ciberseguridad en Latinoamérica alcanzará US\$ 11 mil millones [18]. Hoy los mercados más significativos de estos productos se encuentran en Brasil, México y Argentina. En general, podemos decir que este mercado posee un gran potencial debido a dos factores: el aumento de la importancia de las cuestiones de ciberseguridad para las empresas de la región, insuficiencia de ofertas en el mercado de ciberseguridad, que cumplan con el criterio “calidad-precio”.

Como regla general, la gran mayoría de los actores en el mercado de ciberseguridad de Latinoamérica son compañías estadounidenses y corporaciones de Europa Occidental. Además, podemos destacar la presencia de compañías rusas de informática. Existe un interés creciente en la región hacia los productos y servicios rusos, especialmente por sus precios accesibles y alta calidad. Podemos mencionar dos compañías rusas bastante populares en el área de ciberseguridad – *Kaspersky Lab* y *SearchInform* [19]. La primera tiene presencia en Brasil, Argentina, México y Cuba. *SearchInform* sólo está presente en Brasil. Se está ampliando la actividad de compañías nacionales y regionales en este sector. Por ejemplo, la mayor compañía brasileña de inversiones *Patria Investments* compró dos grandes importantes proveedores de servicios de ciberseguridad: *Neosecure* y *Proteus*. El objetivo de la compra es crear la mayor plataforma nacional de seguridad informática en América Latina [19].

Podemos concluir que el potencial del mercado de ciberseguridad en Latinoamérica aún no está del todo descubierto y tiene grandes perspectivas. Su crecimiento se ve impulsado por la creciente demanda de productos de ciberseguridad ante el aumento de amenazas y delitos cibernéticos, parcialmente, de parte de las PYMES. Es

importante ampliar cada vez más la gama de productos de este tipo, pero que sean asequibles para la mayoría de pequeñas y medianas empresas.

El Cuadro 2 presenta algunos criterios, con los cuales se busca definir, en qué países los problemas de ciberseguridad son más actuales; qué países se han involucrado activamente en la lucha contra el crimen cibernético a nivel nacional y regional; en qué países los mercados de ciberseguridad están más desarrollados.

Cuadro 2

Países de Latinoamérica y la cuestión de ciberseguridad

	Mayor número de ciberataques a PYMES	Países de AL, primeros en adoptar una estrategia nacional de ciberseguridad	Participación activa en iniciativas a nivel internacional
Países	Brasil, México, Argentina, Costa Rica, Colombia, Chile	Colombia (2011), Panamá (2017), Paraguay (2017), Chile (2017), Costa Rica (2017), México (2017), Argentina (2019)	Brasil, Argentina, Colombia, Chile, Costa Rica
	Participación activa en las iniciativas a nivel regional	Mayores mercados de productos de ciberseguridad	Presencia de compañías rusas de ciberseguridad
Países	Colombia, Paraguay, Chile, México	Brasil, México, Argentina	Brasil, Argentina, México, Cuba

Fuente: elaboración de las autoras.

El país con más problemas en cuanto a crimen cibernético es Brasil, donde se registra el mayor número de ciberataques y donde las pequeñas y medianas empresas sufren la mayor cantidad de pérdidas. El país más activo a la hora de abordar los problemas de ciberseguridad, incluidos los que enfrentan las PYMES, es Colombia, donde se ha creado un marco

institucional fuerte y se apoya activamente a las empresas privadas, entre ellas, las PYMES. Brasil puede considerarse como el mayor mercado de productos de ciberseguridad en Latinoamérica, donde tienen más presencia compañías rusas, en comparación con otros países de la región.

Conclusiones

El creciente problema del crimen cibernético en el mundo, que es particularmente grave en los países de América Latina, tiene un serio impacto que se ve reflejado en el funcionamiento de las pequeñas y medianas empresas, que representan un sector muy vulnerable y que hoy día en la región constituyen la mayoría e negocios existentes. En mayor parte el problema se presenta ante los complejos industriales, las organizaciones financieras, también las empresas de servicios y minoristas. Entre las amenazas más actuales, con las que se encuentran hoy las PYMES en Latinoamérica, se destacan caídas de sistema y fallas en la infraestructura informática, fuga de datos confidenciales, extorsión a través de Internet. Todos estos problemas han provocado importantes pérdidas económicas y de reputación para las PYMES.

Entre las razones por las cuales han aumentado las amenazas cibernéticas para las PYMES latinoamericanas se destacan: falta de recursos económicos para adquirir productos de calidad, tanto a nivel regional como nacional; insuficiente desarrollo del mercado de productos de ciberseguridad y falta de los que cumplan con el criterio “calidad-precio”; insuficiencia de conocimientos en las PYMES sobre los algoritmos para detectar riesgos y delitos cibernéticos, sobre cómo reaccionar ante ellos.

Brasil se encuentra entre los países más afectados por las ciberamenazas. El problema también es grave para las empresas de México y Chile. La mayor actividad en la lucha contra la ciberdelincuencia, tanto a nivel empresarial como estatal, se concentra en Colombia. Brasil es el mayor mercado de

productos de ciberseguridad de Latinoamérica. También hay mayor actividad en este país por parte de empresas rusas que ofrecen productos económicos y de alta calidad para la protección contra ciberamenazas, lo que amplía las posibilidades de mejorar la ciberseguridad para las PYMES brasileñas.

Bibliografía References Библиография

1. Cyber Security in Small and Medium Enterprises (SMEs): What's Good or Bad? *Journal of Governance and Development (JGD)*. Sintok, 2022, vol. 18, no. 1, pp. 75-87. DOI: 10.32890/jgd2022.18.1.5.

2. Global Cybersecurity Index. URL: <https://www.itu.int/hub/publication/d-hdb-gci-01-2024/> (accessed 19.01.2025).

3. Hurel L.M. Cybersecurity in Brazil: An Analysis of the National Strategy. *Strategic Paper 54*. Rio de Janeiro, Igarapé Institute, 2021, pp. 10-12.

4. Стадник И.Т., Цветкова Н.А. Место и роль стран Латинской Америки в системе международной и региональной кибербезопасности. *Латинская Америка*. М., 2021, № 4, с. 69-84 [Stadnik I.T., Tsvetkova N.A. Mesto i rol' stran Latinskoy Ameriki v sisteme mezhdunarodnoy i regional'noy kiberbezopasnosti [Place and Role of Latin American Countries in the System of International and Regional Cybersecurity]. *Latinskaya Amerika*. Moscow, 2021, no. 4, pp. 69-84 (In Russ.)].

5. Chaves Guzmán A.J. Colombia Develops a Comprehensive New Cyber Security Policy. *Per Concordiam*, Garmisch-Partenkirchen, 14.07.2016.

6. Urbanovics A. Cybersecurity Policy-Related Developments in Latin America. *AARMS—Academic and Applied Research in Military and Public Management Science*. Budapest, 2022, vol. 21, no. 1, pp. 79-94.

7. Kosevich E.Y. Estrategias de seguridad cibernética en los países de América Latina. *Iberoamérica*. Moscow, 2020, núm. 1, pp. 137-159.

8. Bolgov R. The UN and Cybersecurity Policy of Latin American Countries. *2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG)*. Buenos Aires, 2020, pp. 259-263. DOI: 10.1109/icedeg48599.2020.9096798.

9. Leading Risks for Small Enterprise Companies Worldwide from 2018 to 2024. URL: <https://www.statista.com/statistics/1018196/leading-small-business-risks-globally/> (accessed 11.01.2025).

10. Leading IT Security Incidents among Companies in Latin America in 2021. URL: <https://www.statista.com/statistics/1180445/leading-it-security-incidents-companies-latin-america/> (accessed 11.01.2025).

Desafíos de la ciberseguridad para las pequeñas y medianas empresas

11. Biggest Concerns of Board of Directors (BOD) of Organizations Worldwide Regarding Cybersecurity in 2024, by Country. URL: <https://www.statista.com/statistics/1350834/biggest-cybersecurity-concerns-of-global-bod-by-country/> (accessed 11.01.2025).

12. Актуальные киберугрозы для стран Латинской Америки и Карибского бассейна: 2022-2023 [Aktual'nyye kiberugrozy dlya stran Latinskoy Ameriki i Karibskogo basseyna: 2022-2023 [Current Cyber Threats to Latin America and the Caribbean: 2022–2023]. URL: <https://ptsecurity.com/ru-ru/research/analytics/latam-cybersecurity-threatscape-2022-2023/> (accessed 23.01.2025) (In Russ.)].

13. Share of Companies that Suffered Cybersecurity Incidents in Selected Latin American Countries in 2019. URL: <https://www.statista.com/statistics/1180166/share-companies-cybersecurity-incidents-latin-america/> (accessed 11.01.2025).

14. Countries in Latin America Most Targeted by Cyberattacks in 2020. URL: <https://www.statista.com/statistics/818412/latin-american-countries-highest-share-cyber-attacks/> (accessed 01.12.2024).

15. Declaration: Strengthening Cyber-Security in the Americas. URL: <https://2009-2017.state.gov/p/wha/rls/221498.htm> (accessed 01.12.2024).

16. Горелик И.Б. Роль международных организаций в процессе противодействия киберпреступности. *Международное право*. М., 2022, № 3, с. 28-41 [Gorelik I.B. Rol' mezhdunarodnykh organizatsiy v protsesse protivodeystviya kiberprestupnosti [The Role of International Organizations in the Process of Counteracting Cybercrime]. *Mezhdunarodnoye pravo*. Moscow, 2022, no. 3, pp. 28-41 (In Russ.)].

17. Política Nacional de Seguridad Digital. Bogotá, D.C., 11 de abril de 2016.

18. Bianci T. Cybercrime in Latin America – Statistics & Facts. URL: <https://www.statista.com/topics/7126/cybersecurity-in-latin-america/> (accessed 11.01.2025).

19. Мягков В.Ю., Орлова Г.А., Савинов Ю.А. Деятельность российских компаний на рынке цифровых технологий Латинской Америки. *Российский внешнеэкономический вестник*. М., 2020, № 4, с. 87-95 [Myagkov V.Y., Orlova G.A., Savinov Y.A. Deyatel'nost' rossiyskikh kompaniy na rynke tsifrovyykh tekhnologiy Latinskoy Ameriki [Activities of Russian Companies in the Digital Technology Market of Latin America]. *Rossiyskiy vneshneekonomicheskiy vestnik*. Moscow, 2020, no. 4, pp. 87-95 (In Russ.)].