Región de Murcia

info REGIÓN DE MURCIA

Oportunidades de negocio de ciberseguridad en Colombia para 2022/2023

Este estudio ha sido realizado por
José Pedro Martínez Caballero

Becario del Instituto de Fomento de la Región de Murcia en la Oficina económica y comercial de la Embajada de España en Colombia

13 de diciembre de 2022
Bogotá

Índice

1. Información general

Colombia es uno de los países de Latinoamérica con más potencial en la región, tras la llegada del COVID experimentó un crecimiento en transformación digital y el uso de las herramientas digitales, lo que conllevó un crecimiento de ciberataques a usuarios de este país. Según la Asociación Nacional de Industriales (ANDI), tras el inicio de la pandemia, el 60% de las empresas han establecido estrategias de transformación digital.

Ante este panorama, durante el año 2021, Colombia recibió siete billones de ataques cibernéticos, esta tendencia irá en aumento debido a que los cibercrímenes generan cada vez más rentabilidad para los criminales y para frenarlo, el país necesita de unas infraestructuras solidas que permitan repeler las amenazas que surjan.

Para ponernos en contexto de la situación actual del país, según el informe presentado por la Fiscalía General de la Nación, en Colombia aumentó un 30% los ataques el año pasado si lo comparamos con el anterior. Debemos mencionar que las compañías y entidades oficiales se han encargado de desarrollar estrategias que les permitieran protegerse de los ciberataques, pero no han sido suficientes para evitarlos. Por ejemplo, casos como ataques a entidades mediante Ransomware para el robo de datos continúan dándose y esto ha generado grandes pérdidas en términos económicos para las entidades afectadas.[1]

Según una encuesta realizada por Kaspersky, indica que Colombia recibió durante el año 2021 87 ciberataques por minuto ocupando el quinto lugar en la región (11,09). Los ataques más comunes que reciben las empresas son los accesos no autorizados con el objetivo de dañar sistemas, secuestrar información (ransomware) y ciber espionaje con fines de beneficio económico. Otra de las amenazas presentes es la de un cracker que intenta obtener datos de los activos de la compañía a través de los empleados de la empresa. Es importante destacar, que según el informe Cyber Threat Report 2021, Colombia se situó entre los 10 países con mayores ataques de ramsomware y el segundo en la región de Latinoamérica. También se situó en el cuarto lugar, a nivel mundial, en detecciones maliciosas.

[1] https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/

Ante esta línea, las empresas se han ido reforzando en temas de seguridad, junto con un alto conocimiento de redes y protocolos de comunicación, para evitar los ciberataques que están en constante evolución. [2]

Según el Centro de Seguridad Industrial en Colombia, para proteger los sistemas de automatización industrial, las Organizaciones colombianas aplican: Consultoría/Asesoría en Ciberseguridad Industrial, Implantación de Sistemas de Gestión de la Seguridad, Hacking ético, Auditorias de Seguridad Internas/Externas, Diseño de Arquitecturas y Redes, Desarrollo de Planes de Continuidad/Contingencia, Firewalls Industriales y Control de Aplicaciones Industriales. [3]

[2] https://acis.org.co/portal/content/ciberseguridad-en-colombia-%C2%BFc%C3%B3mo-enfrentarse-las-amenazas-inform%C3%A1ticas-en-la-industria-40

[3] https://www.cci-es.org/maps/colombia/

2. Características del Mercado

2.1. Definición precisa de las actividades / productos del sector estudiado

Según el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC), la ciberseguridad se define como "el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio." [4]

El sector de la ciberseguridad se distingue en dos categorías principales: Desarrollo de software y hardware, y, servicios.

Desarrollo de software y hardware

- Anti Fraude y Anti Malware
- Firewalls Industriales
- Diseño de Redes y Arquitecturas
- SIEM (Gestión de Eventos e Información de Ciberseguridad)
- Control de Autenticación y acceso
- Cumplimiento legal
- Inteligencia de seguridad
- Protección de las comunicaciones
- Prevención de fuga de información
- Seguridad de dispositivos móviles

Servicios

- Certificación normativa
- Auditoria Seguridad, planificación y asesoramiento
- Planes de Continuidad y Contingencia
- Formación y concienciación
- Gestión de Incidentes

[4] https://mintic.gov.co/portal/inicio/18723:Ciberseguridad

- Implantación de Soluciones y Sistemas
- Seguridad en la nube
- Consultoría y asesoría
- Soporte y mantenimiento

2.2. Tamaño del mercado

Colombia es uno de los países que más ataques recibe de la zona, concretamente, con fecha hasta octubre, en lo que llevamos de 2022, el Centro Cibernético de la Policía Nacional ha recibido 52.886 denuncias de ataques cibernéticos, esto representa un 20% más que el año anterior si lo situamos en el mismo periodo.

Respecto a los tipos de ataques recibidos, el acceso abusivo a sistemas informáticos se situó en un 65%, interceptación de datos informáticos (43%), acceso ilegítimo a sistemas informáticos o redes de telecomunicaciones (40%), hurto de datos por medios informáticos (33%) y, por último, daños informáticos (28%). En menor medida, destacan otros delitos como la transferencia no consentida de activos (8%), violación de datos personales (3%), uso de software malicioso (3%) y suplantación de sitios web (2%).

En cuanto a las zonas más afectadas por este tipo de ataques, en primer lugar, se sitúa Bogotá (15.080), Medellín (4.600), Cundinamarca (3.554), Cali (3.336) y Barranquilla (1.889)

Por otro lado, la modalidad más común de ataque es el phishing en el que las víctimas piensan que están introduciendo los datos en una página web aparentemente oficial, por ejemplo, sitios web bancarios, y, los criminales, mediante este método, se hacen con datos personales y financieros para transferencias de dinero ilegales y suplantaciones. [5]

Por último, según datos de Statista, en el primer semestre de 2022, Colombia se situaba entre los mercados más valiosos en temas de ciberseguridad con un valor en mercado de 390 millones de dólares, únicamente superado por Brasil (1,817 mil millones de dólares) y México (1,091 mil millones de dólares). En términos generales, el valor de mercado de ciberseguridad en Latinoamérica se valoraba en 5.730 millones de dólares en 2021, se estimó que hasta 2027 crecería a una tasa anual compuesta de un 11,8% hasta situarse en 10,01 mil millones de dólares en 2027. [6]

[5] https://caracol.com.co/2022/10/26/se-dispara-el-crimen-cibernetico-cuales-son-los-delitos-mas-comunes/
[6] https://www.statista.com/statistics/1180184/value-cybersecurity-market-latin-america/

3. España como actor clave

3.1. Oferta Española

España tiene una importante base de empresas dedicadas a la ciberseguridad afincadas en el país, a diciembre de 2022, según el Catálogo de Empresas y soluciones de Ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), hasta el momento se identifican 1.852 empresas españolas con un total de 8.326 soluciones en ciberseguridad.

La presencia de las empresas españolas en Colombia es importante, a continuación destacamos algunas de interés que operan a nivel nacional y ofrecen servicios de ciberseguridad: Indra, S2Grupo, Seidor, Proactivanet, GMV, Oesia, Ikusi, Telefónica etc.

La percepción por parte de los colombianos, de las empresas españolas que ofrecen este tipo de servicios, es buena. Generalmente, los productos, tecnologías y conocimientos de España, son bien recibidos por los ciudadanos colombianos. Estas empresas de ciberseguridad suelen trabajar para el sector privado, pero también para el sector público como, por ejemplo, defensa y gobierno.

3.2. Oportunidades de negocio

En el año 2022, un 69% de las empresas colombianas van a incrementar las inversiones en el sector de la ciberseguridad si atendemos a diversos estudios. Durante el 2021, las empresas invirtieron 329 millones de dólares en este sector, en el que un 87% del total, situaba a la ciberseguridad como prioridad a abordar en las empresas. El gobierno colombiano ha hecho hincapié en este sector tomando medidas adecuadas para reforzar la seguridad de las compañías colombianas.

Ante este escenario, Colombia se presenta como un mercado que ofrece grandes oportunidades para reforzar este sector. Además del peligro que corren las grandes empresas y las instituciones públicas de sufrir estos ciberataques, las pequeñas y medianas empresas también corren el peligro, por lo que esto es un nicho importante para cubrir.

A raíz del aumento de ataques a redes corporativas, aumentó un 50% durante el año anterior, y de una sofisticación de estos, las empresas demandan soluciones de ciberseguridad consolidadas para afrontar estos nuevos retos. Otros de los desafíos que enfrentan las compañías, de los más importantes, es la seguridad en redes; durante el año anterior, las empresas colombianas sufrían 5.000 ataques por día. Lo que hace vulnerable las redes básicamente son dos aspectos: no tener

una trazabilidad de los equipos y su gestión, y el segundo, su simplicidad; por lo tanto, es primordial disponer de herramientas que refuercen el control de acceso para minimizar los riesgos.[7]

En cuanto a las predicciones de ciberseguridad que se han realizado para este 2022, la Cámara Colombiana de Informática y Telecomunicaciones destacan las siguientes:

- **Evolución del Ransomware.** Estos ataques se enfocarán en secuestros exprés, las opciones de extorsión se ampliarán y las empresas tendrán el desafío de evitar o recuperar el control y acceso a información
- **Aumento enfoque identidad.** Técnicas de reconocimiento facial, huellas biométricas etc son algunos de los consejos para proteger y prevenir le robo de identidad y datos personales,
- **Sofisticación phishing.** Mayor enfoque en un phishing personalizado teniendo como objetivo cargos que estén relacionados con puestos estratégicos empresarial.
- **Cadena de suministros.** Este sector será objetivo para los criminales ya que serán objetivo de ataques las empresas que provean de servicios de TI a este sector. Las empresas deberán contar con una política sólida y definida de ciberseguridad que proteja la información.
- **Ataques smartphones.** Los smartphones son también un objetivo de los delincuentes, estos deben de incluirse dentro del diseño de la política de ciberseguridad de la empresa.
- **Visibilidad riesgos.** Debido al aumento del teletrabajo, se tiene que implementar políticas de ciberseguridad que protejan las organizaciones y controlen el riesgo de ataques.
- **Necesidad de tener un seguro de cibernético.** El aumento de ataques cibernéticos ha generado una necesidad de contratación de pólizas de seguro.
- **Necesidad de talento.** Se hace necesario contar con talento en las compañías que sean expertos en esta materia, por lo que cada vez, son más valorados dentro de las compañías.

[7] https://www.larepublica.co/empresas/condiciones-del-mercado-de-ciberseguridad-colombiano-atraen-a-nuevos-jugadores-3324669

4. Organismos

Colombia cuenta con diversos organismos públicos nacionales que velan por generar un marco legal adecuado, que garantice la progresiva incorporación de la ciberseguridad industrial en las estructuras de las empresas con presencia nacional (principalmente infraestructuras críticas), entre las principales cabe destacar:

- Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT
- Comando Conjunto Cibernético - CCOC
- Centro Cibernético Policial - CCP
- Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia - MinTIC
- Ministerio de Defensa Nacional - MinDefensa

5. Eventos y ferias

Feria Internacional de Seguridad ESS+
16-18 agosto 2023
Corferias – Centro de Convenciones, Carrera 37 nº 24 67 Bogotá (CO)
https://securityfaircolombia.com/

CyberSecurity Bank & Government
14 septiembre 2023
Lugar de celebración por confirmar
https://www.mticsproducciones.com/cybersecurity-bank-and-government-2023/#/

Expodefensa 2023
Fecha por confirmar
Corferias – Centro de Convenciones, Carrera 37 nº 24 67 Bogotá (CO)
https://www.expodefensa.com.co

ANDICOM, Congreso Internacional TIC 2023
6-8 septiembre 2023
Cartagena de Indias
https://andicom.co/es/