



Ciberseguridad en Centroamérica y Caribe 2024

Amenazas y tendencias

BeDisruptive™

BeDisruptive es la boutique tecnológica especialista en ciberseguridad que acompaña a sus clientes en el diseño de soluciones y el mantenimiento de un entorno seguro.



Tabla de contenidos

| | |
|---------------------------------|-----------|
| 01. Resumen ejecutivo | Página 04 |
| 02. Panamá | Página 06 |
| 03. Belice | Página 09 |
| 04. Costa Rica | Página 11 |
| 05. Nicaragua | Página 13 |
| 06. Honduras | Página 15 |
| 07. El Salvador | Página 17 |
| 08. Guatemala | Página 20 |
| 09. República Dominicana | Página 22 |
| 10. Región del Caribe | Página 25 |
| 11. Recomendaciones | Página 27 |
| 12. Bibliografía | Página 28 |

01. RESUMEN EJECUTIVO

En el año de la quinta revolución industrial, el de la IA, Centroamérica será partícipe de las amenazas globales destacadas en el informe de [Cibercrimen 2024: análisis y tendencias](#).

Estas amenazas incluyen la propagación de *malware* avanzado impulsado por inteligencia artificial, la proliferación de *deep fakes* para la manipulación de la opinión pública, y los ataques dirigidos a infraestructuras críticas, entre otros desafíos destacados.

La adopción de la inteligencia artificial por parte de los cibercriminales junto con la inestabilidad que puede causar la agenda electoral en la región y la consolidación del hacktivismo, también serán amenazas a tener en cuenta en Centroamérica.




Además de las tendencias globales, a nivel regional, estos serán los factores clave para determinar el nivel de riesgos.

- La evolución de la penetración tecnológica.
- La madurez en ciberseguridad.
- Las tendencias de ataques globales.
- El crecimiento económico de la región que determinará el ROI de las actividades cibercriminales.
- Las tensiones geopolíticas que puedan provocar una campaña de actores de motivación política (como las APTs – Advanced Persistent Threats).

Los países centroamericanos deberán proteger con más afán las infraestructuras críticas, las redes gubernamentales, la cadena de suministro y las entidades financieras porque serán, previsiblemente, y como en años anteriores, los principales objetivos de ataque de los cibercriminales.

La actualidad de amenazas para América Central revela un aumento significativo en los ataques de *malware* contra ordenadores y dispositivos móviles, especialmente en intentos de ataques de *phishing*, *ransomware* y troyanos bancarios.

Los actores más esperados son los de motivación económica, representados principalmente por los grupos de ransomware y seguidos por campañas de fraude locales o regionales. Además, se pueden descubrir campañas puntuales por parte de APTs.



Según la empresa ESET el **69% de las organizaciones** de América Latina sufrió algún incidente de seguridad durante el último año. Los países de Centroamérica con el mayor porcentaje de detecciones de códigos maliciosos en campañas de *phishing* son:

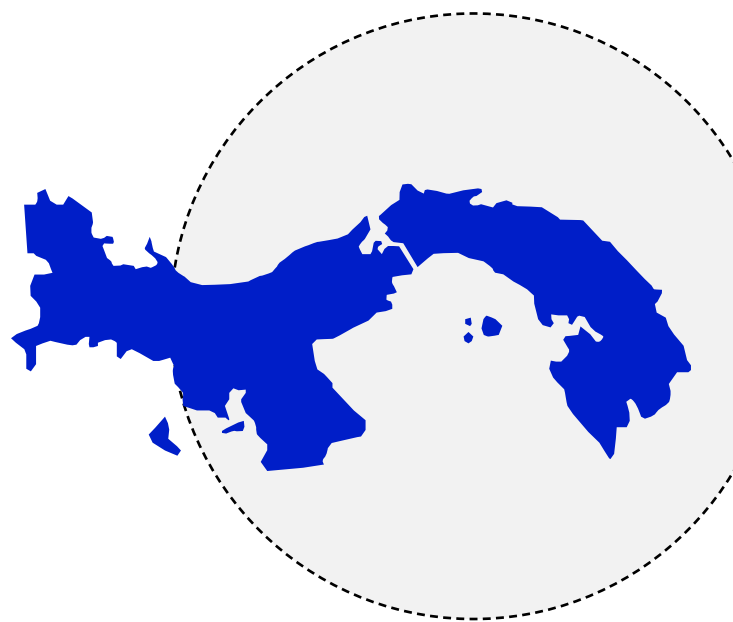
- 7,2% - COSTA RICA
- 5,2% - GUATEMALA
- 5,1% - EL SALVADOR



02. PANAMÁ

Panamá actualmente se posiciona en **el puesto 75** de la National Cybersecurity Index (2016–2023), un ranking que mide la preparación de los países para prevenir las ciberamenazas y gestionar los ciberincidentes. Actualmente Panamá ostenta el puesto 75 de los 176 registrados.

A pesar de que se ha reducido el número de ciberataques debido en parte al bajo impacto que han generado los mismos, hay que tener presente que Panamá, como uno de los principales países de Centro América, puede ser foco de posibles ciberataques derivados de posibles colaboraciones a nivel internacional en la región.



SECTORES MÁS AFECTADOS

● Sector financiero

Se ha posicionado y observado como uno de los más afectados en 2021 desde una perspectiva histórica, ya que aumentaron un 52% los ciberataques en dicho sector, tendencia al alza continuada durante 2022 y 2023.

● Sector salud y justicia

En verano de 2023, un ciberataque a gran escala a la compañía IFX Networks afectó a un total de 17 países en América, incluyendo Panamá. Dicho ciberataque fue un *ransomware* totalmente dirigido a la cadena de suministro, que dejó inhabilitados los servicios estatales de atención en línea al público en salud y justicia.

● Otros sectores

A lo largo del último año han tenido una afectación también el sector educativo, turístico, y sanitario.

● Entidades gubernamentales

En relación con las entidades gubernamentales, Panamá ha sido un objetivo frecuente en los últimos años.



Al analizar los anteriores datos, se puede observar y percibir la necesidad de mejorar en términos de formación en ciberseguridad, especialmente en Panamá, uno de los países líderes en Centroamérica, como se ha destacado al inicio de esta sección. Es esencial potenciar la concienciación para fortalecer la defensa ante posibles ataques dirigidos hacia la primera línea de defensa de las empresas: sus empleados.

TROYANO GRANDOREIRO



Como otros países de la zona, Panamá ha sufrido un gran impacto por el troyano bancario "Grandoreiro", recientemente desarticulado mediante colaboración internacional. Dicha amenaza se trata de un malware que ha estado activo desde al menos 2020 y no sólo ha afectado a toda Latinoamérica, sino también a España.

Este *malware* se ha dirigido principalmente a usuarios de bancos panameños, con el objetivo de robar sus credenciales bancarias y realizar transacciones fraudulentas. Poniéndonos en situación en relación a esta amenaza y fijándonos en un pasado reciente, en 2021, se detectó una campaña de *phishing* que utilizaba correos electrónicos falsos del Banco Nacional de Panamá (BNP) para distribuir Grandoreiro. Los correos electrónicos invitaban a los usuarios a actualizar sus datos bancarios a través de un enlace falso que, al ser pulsado, descargaba el *malware* en el dispositivo del usuario.



ENERO 2024

La empresa ESET colaboró con la Policía Federal de Brasil en un intento de desmantelar los sistemas del grupo cibercriminal detrás de Grandoreiro, lo que condujo a la identificación y detenciones de los individuos que controlaban la trama.

El troyano ha experimentado un desarrollo rápido y constante, con la presencia de nuevas variantes del código malicioso con frecuencia.

Grandoreiro es un ejemplo de las ciberamenazas que afectan a América Latina y resalta la importancia de contar con soluciones antimalware robustas y estar al tanto de las actualizaciones de seguridad.

RIESGOS Y DEBILIDADES



Aumento de ataques contra infraestructuras críticas todavía no reconocidas.



Falta de legislación regulatoria en términos de ciberseguridad en parte por la falta de concienciación al respecto.



Desinformación durante las elecciones de mayo.

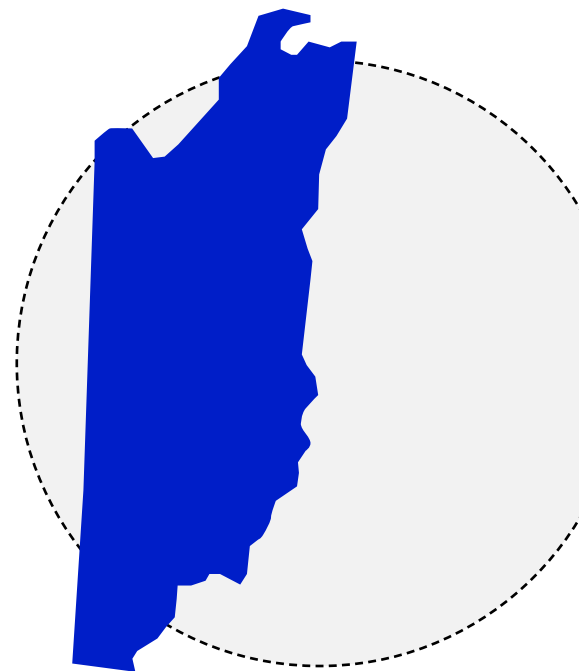


03. BELICE

Este país se encuentra en el **puesto 136** del National Cyber Security Index.

Si bien a nivel de ciberseguridad, la región no presenta ni el nivel de madurez, ni de amenazas que otros países vecinos, esto no le exime de ser víctima de ciberataques.

En julio de 2023, la empresa de electricidad Belize Electricity Limited fue víctima de un *ransomware* de RagnarLocker.



Al ser un país pequeño, es más que probable que, tecnológicamente, dependa de proveedores tecnológicos extranjeros como ocurre con muchos otros países. Esta dependencia hace que, los ataques de cadena de suministro supongan el principal riesgo para este país.

Por otro lado, Belice destaca por ser un foco turístico y por alojar las islas privadas de algunas celebridades. Junto con los turistas, llegan a la isla sus datos personales, por lo que la privacidad de estos puede suponer un riesgo para el país.

EXPOSICIÓN A CIBERATAQUES

La penetración de Internet es menor al 50%, es decir, menos de la mitad de la población usa Internet o dispositivos móviles.

De la misma manera, las infraestructuras tecnológicas se implantan a una velocidad menor que en el resto del mundo.

Estos factores suponen una menor exposición a ciberataques.

NIVEL GEOPOLÍTICO

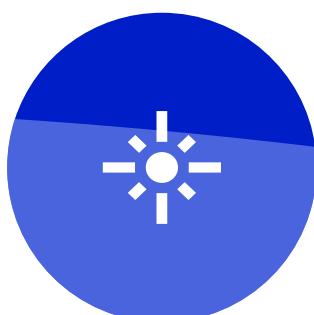
A nivel geopolítico, el país actualmente no cuenta con tensiones internacionales recientes que supongan un riesgo crítico de ataque con motivación política.

A pesar de que el gobierno condenó las acciones de Rusia en Ucrania y la visita de Andrij Melnyk en marzo de 2023, no se registraron ataques por parte de actores hacktivistas rusos. Por otro lado, el apoyo del gobierno beliceño a Taiwán contra las intenciones del gigante chino podría suponer un riesgo de ciberataque por parte de APTs (*Advanced Persistent Threats*), si bien este riesgo se considera bajo.

RIESGOS Y DEBILIDADES



Ataques contra infraestructuras críticas que puedan una disrupción del servicio.



Ataques de cadena de suministro por dependencia tecnológica de terceros.



Robo de información sobre turistas, visitantes del país y VIPs.



04. COSTA RICA

Costa Rica se encuentra en el **puesto 77** de la National Cyber Security Index.

Esta apuesta por mejorar la ciberseguridad en el país en parte se debe a que, en 2022, Costa Rica fue atacada repetidamente por varios grupos de ransomware, especialmente Conti.

Estos ataques pusieron encima de la mesa la necesidad de crear la reciente Estrategia Nacional de Ciberseguridad 2023-2027. Este cambio le ha permitido ser el primer exportador de servicios TI per cápita de Latinoamérica.



A raíz de estos ataques, España, EE. UU. y los principales fabricantes del país han prestado apoyo y guía a Costa Rica. La cooperación internacional ha sido una de las estrategias clave para su rápida adaptación a las medidas de ciberseguridad necesarias.

Actualmente, Costa Rica ha reducido su nivel de riesgo frente a ciberataques. Desde 2023 se ha observado una reducción clara del número de ciberataques de *ransomware* públicos contra el país y se ha aumentado la madurez en ciberseguridad en las instituciones y empresas.

A pesar de ello, la apertura de negocio y las perspectivas de crecimiento económico en el próximo año serán un reclamo para el cibercrimen con motivación económica, lo que conlleva un aumento claro en el riesgo de ciberataque. Un ejemplo de la importancia tecnológica del país en la región es la Planta de Ensamble y Prueba de INTEL en Costa Rica.



ESFERA POLÍTICO NACIONAL

En la esfera política nacional, no hay nuevas elecciones a la vista, dado que en febrero de 2024 han tenido lugar las elecciones municipales sin incidentes y hasta 2026 no se celebrarán comicios generales.



TENSIONES INTERNACIONALES

Las principales tensiones internacionales en la esfera tecnológica se centran en la adopción del 5G por parte de Costa Rica. El pasado mes de agosto, el gobierno decretó que las tecnologías a adoptar deberían ser de países suscritos al Convenio de Budapest sobre ciberseguridad.

Esta medida excluye a las tecnologías de China, Corea, Brasil o Singapur. El decreto provocó que China emitiese un comunicado criticando la exclusión de su tecnología.

RIESGOS Y DEBILIDADES



Espionaje APT contra el gobierno con motivo de las negociaciones por el 5G y la Plana de Ensamble y Prueba de INTEL.



Tendencias de cibercriminalidad acordes al panorama de amenazas global: ataques de cadena de suministro, deep fakes y desinformación, etc.



Posible aumento del número de ciberataques acorde al crecimiento económico del país.

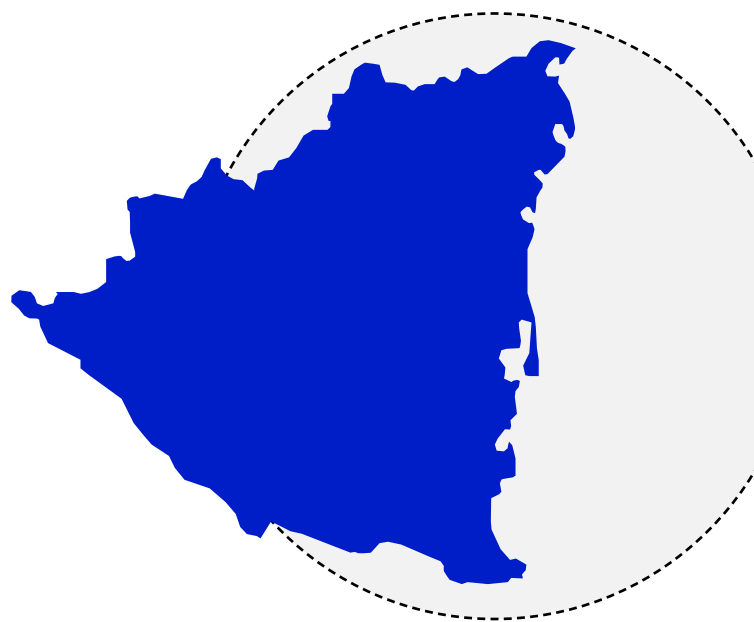


05. NICARAGUA

Nicaragua se encuentra en el **puesto 107** de la National Cyber Security Index.

Desde finales de 2020, Nicaragua ha incrementado las denuncias por agresiones mediante medios digitales e intentos de sabotaje y desaparición de cuentas en redes sociales y plataformas web de corte independiente.

Estos ciberataques, que se han producido en consecuencia del avance digital obligado en época de pandemia.



Posteriormente, tras conocerse la cooperación entre Rusia y Nicaragua de 2022 a 2026, el objetivo final preestablecido es la defensa de la soberanía nacional de cada uno de los participantes de dicha cooperación.

Tal y como se observa la situación actual a nivel mundial se reconoce que podría categorizarse como una táctica militar de espionaje en vez de una estrategia de cooperación en ciberseguridad, según Víctor Ruiz, fundador del centro de ciberseguridad SILIKN en México.



TRIGONA RANSOMWARE

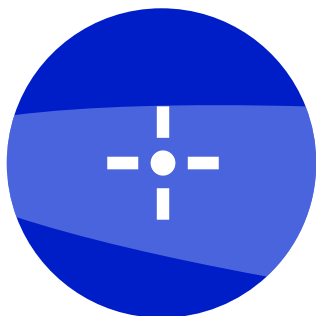
En el comienzo de este 2024, el sector de las telecomunicaciones ha sufrido el impacto del *ransomware* Trigona, lo que posiblemente lo sitúa nuevamente como uno de los más críticos.



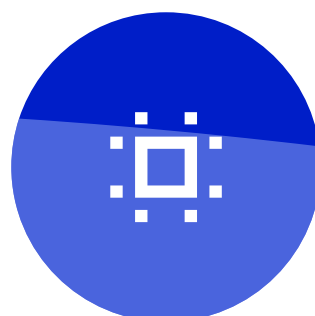
ATAQUES DE PHISHING

A medida que los ataques de *phishing* están en aumento en la región y el uso de *ransomware* sigue una tendencia ascendente, en Nicaragua persiste una población poco formada en conceptos de ciberseguridad. Este hecho vuelve a la población vulnerable ante los ciberdelincuentes, quienes aprovechan el *phishing* y la ingeniería social para sus ataques. Por este motivo, el riesgo derivado de la ejecución de amenazas sofisticadas hacia las infraestructuras críticas se incrementa significativamente.

RIESGOS Y DEBILIDADES



Posible espionaje por parte de entidades afiliadas al gobierno ruso.



Infraestructuras críticas de fácil acceso por fallo humano y baja resiliencia.



Robo de datos y suplantación de identidad.



Campañas de phishing y uso de técnicas de Ingeniería Social en redes sociales.

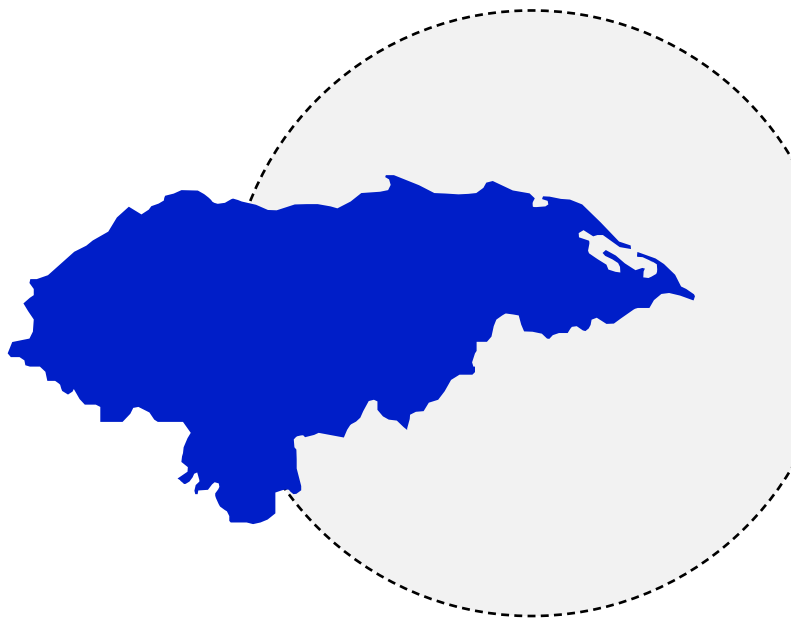


06. HONDURAS

Honduras se encuentra en el **puesto 122** de la National Cyber Security Index.

Actualmente en Honduras se ha observado un alto esfuerzo en la digitalización a nivel regional. Si bien es cierto, que ciertos sectores se han visto más afectados a raíz de la pandemia, podemos focalizar el de la educación principalmente.

Tal como se ha podido observar con el tiempo, los altos esfuerzos en la digitalización del sector educativo están teniendo un gran éxito, pero Honduras se enfrenta a un gran reto: la alfabetización digital está atrasada y este hecho genera una necesidad de estrategia concertada.



MARCO LEGISLATIVO

Honduras presenta un gran sesgo a nivel legislativo. Esta región cuenta con un marco débil en la protección de datos y en la recopilación de información personal, tanto a nivel privado como público.

Ya que ningún organismo de control hace cumplir con dicha protección de datos, el país se ve frágil y accesible en la recopilación de datos por ciberdelincuentes.

Estos problemas fueron reconocidos por portavoces de organizaciones internacionales, organizaciones de derechos digitales, el sector privado y el gobierno hondureño.

Continuando con el marco legislativo, el Gobierno de Honduras actualmente carece de capacidad para judicializar los delitos digitales, forma en la que los ciberdelincuentes evaden la legislación.



BRECHAS DIGITALES

En Honduras se establece una brecha digital y, además, de género.

Según la United States Agency International Development en su informe de evaluación país del ecosistema digital de mayo de 2023, las mujeres tienen menos de un 15% de probabilidad de poseer telefonía móvil de forma personal en vez de forma laboral, en consecuencia de las condiciones sociales, por lo que es más probable que se refleje un costo socioeconómico en el país.

Esto hace más fácil a los ciberdelincuentes el acceso a perfiles que no tienen esa facilidad en entornos digitales por la falta de experiencia, aumentando así el porcentaje de víctimas en el país.

RIESGOS Y DEBILIDADES



Ataques de ingeniería social como consecuencia de la baja experiencia en entornos digitales.



Pocos perfiles adaptados a la evolución digital.



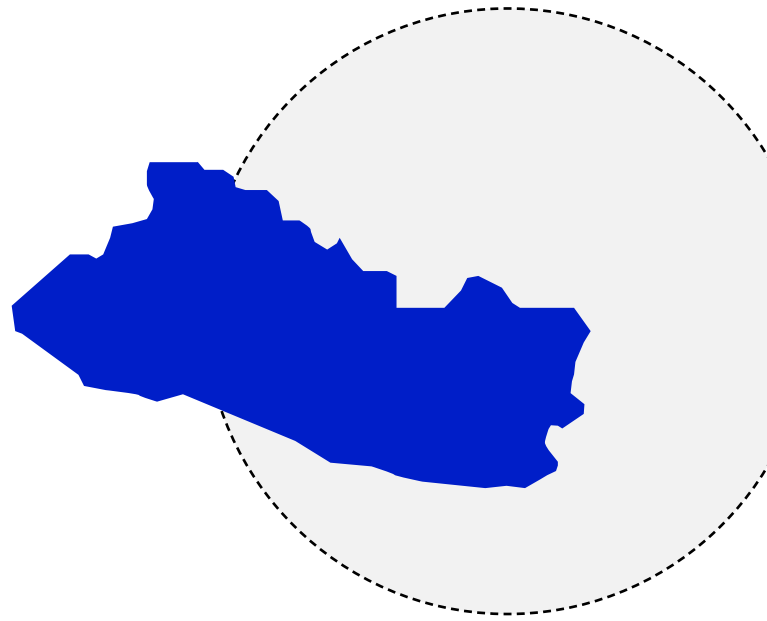
Sencillez para los delincuentes a la hora de evadir la legislación actual.



07. EL SALVADOR

El Salvador se encuentra en el **puesto 119** de la National Cyber Security Index.

El Salvador enfrenta riesgos digitales en los ámbitos político, económico y social. Se prevé que en los próximos años se incremente la estabilidad del país, especialmente tras la reelección de Nayib Bukele como presidente del Gobierno central el pasado 4 de febrero.



Además, El Salvador se ha enfrentado a desafíos económicos, cambio climático y ciberataques, que han afectado a empresas y al país en general. Estos cambios y desafíos han marcado un período de transformación significativa en la nación centroamericana.

+200.000 ciberataques al año

En los últimos 3 años en El Salvador se reportaron +200.000 ciberataques al año, siendo el sector bancario uno de los principales objetivos de los ciberdelincuentes en el país.

58% de las empresas han sufrido un ciberataque en 2020

Según un oficial de seguridad de la información de Equifax, en 2020, el 58% de las empresas en El Salvador registró algún tipo de incidente cibernético.

~24M de intentos de ciberataques

Estos números han ido creciendo desde entonces y durante el primer trimestre de 2023, se registraron 24 millones de intentos de ciberataque en el país.

Estas estadísticas reflejan la creciente exposición de las empresas salvadoreñas a los ciberataques, lo que subraya la importancia de fortalecer las medidas de ciberseguridad en todo el país y en entidades y empresas de cualquier tamaño.

Las principales amenazas de ciberseguridad en El Salvador incluyen un alto número de intentos de ciberataques, riesgos por casos de phishing, extorsión y robo de datos personales, y la vulnerabilidad de las entidades bancarias a la fuga de información y ataques internos intencionados (llamados también "insiders").

Según datos que se pueden observar en el gráfico de más abajo de la Cámara Salvadoreña de Comercio e Industria, en El Salvador, destaca la importancia de considerar las necesidades y desafíos específicos de las MIPYMES al abordar la ciberseguridad y la protección contra ciberataques.



CRIPATOMONEDAS



Un dato interesante son los ciberataques relacionados con criptomonedas, ya que en El Salvador han sido una preocupación creciente, debido a su adopción oficial como moneda. Según el informe de incidentes de ciberseguridad de la empresa SISAP, casi el 20% de los ciberdelitos en El Salvador y Guatemala se relacionan con criptomonedas, con la mayoría de ellos vinculados al secuestro de datos o suplantación de identidad.

PROPAGANDA



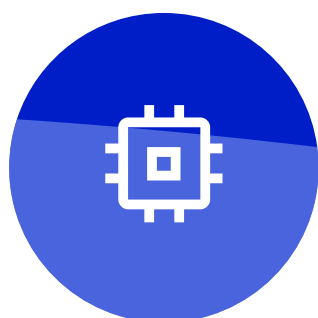
Un aspecto más a tener en cuenta es el uso de herramientas tecnológicas para hacer propaganda por parte de sectores de muy diversa índole contra el actual presidente Bukele, desde opositores políticos y poderes económicos o facciones sociales descontentos con su gestión, hasta poderosos actores criminales de la zona castigados con sus políticas, que podrían desinformar para provocar su pérdida de popularidad.



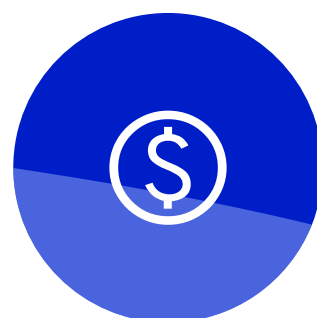
RIESGOS Y DEBILIDADES



Falta de concienciación en ciberseguridad por las MIPYMES.



Desarrollo de *software* de baja calidad y sin seguridad por diseño.



Industria bancaria más vulnerable respecto a otras zonas.



Riesgos asociados a vulnerabilidades y robos de carteras de criptomonedas debido a la adopción oficial del país.



Riesgos de desinformación asociada a la actividad sociopolítica.

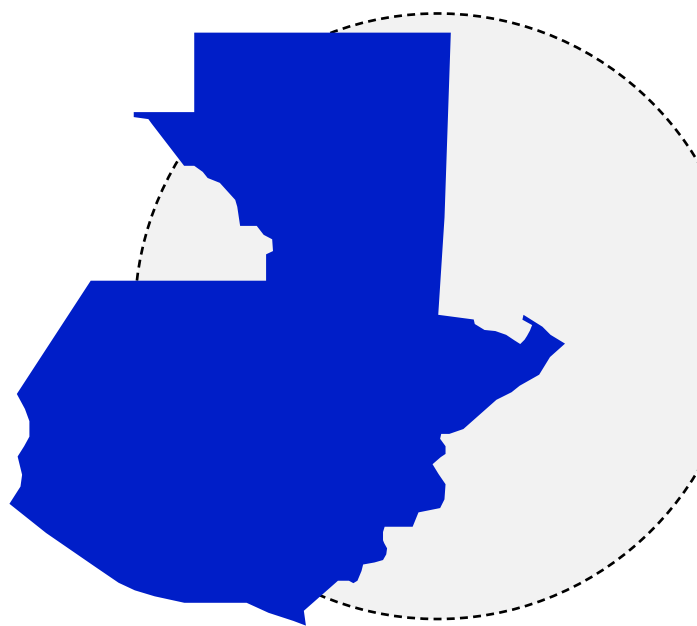


08. GUATEMALA

Guatemala se encuentra en el **puesto 118** de la National Cyber Security Index.

La región de Guatemala mantiene la tónica respecto a ciberamenazas y estado de ciberseguridad de la región.

Según el informe de incidentes de ciberseguridad de la empresa SISAP, durante el 2023 se registraron más de 34 mil millones de eventos de ciberseguridad en el país.



Entre los principales ataques figuran el phishing, que ha sido utilizado por ciberdelincuentes para personalizar ataques y engañar a los destinatarios, lo que ha llevado a la descarga de archivos con software malicioso, la divulgación de credenciales o "leaks" (usuarios y contraseñas), e incluso fraudes en transferencias de dinero que los usuarios realizan pensando que son transacciones legítimas, mediante ataques de ingeniería social o phishing dirigidos.

Según el informe "El Estado del Ransomware" de Sophos, el 74% de las empresas en Centroamérica fueron víctimas de ciberataques, con los más altos porcentajes en Guatemala, seguida de Panamá. Los sectores más afectados por estos ataques han sido el de manufactura, retail, tecnología, construcción, servicios financieros, servicios profesionales, área legal y salud.



CONCIENCIACIÓN

Los errores humanos han sido la causa del 90% de los ciberataques en el país, lo que subraya la importancia de la concienciación y la formación en ciberseguridad, tanto para los empleados de las empresas como para los ciudadanos en general.

En particular, acciones formativas que eviten los ataques conocidos como *breach replay* y *password spray*, o también concienciar sobre datos personales intencionalmente expuestos que faciliten a los ciberdelincuentes los ataques de ingeniería social en base a la información obtenida fácilmente en internet.



SOFTWARE MALICIOSO

En otras ocasiones el *software* malicioso instalado en los ordenadores o móviles se instala a raíz de buscar programas o servicios gratis que incluyen este *malware*. Esto se evita de igual forma con educación tecnológica.

RIESGOS Y DEBILIDADES



Falta de concienciación en el uso y gestión de las cuentas y contraseñas.



Falta de Concienciación sobre el cuidado de los datos personales.



Descargas de *software* de sitios no oficiales.



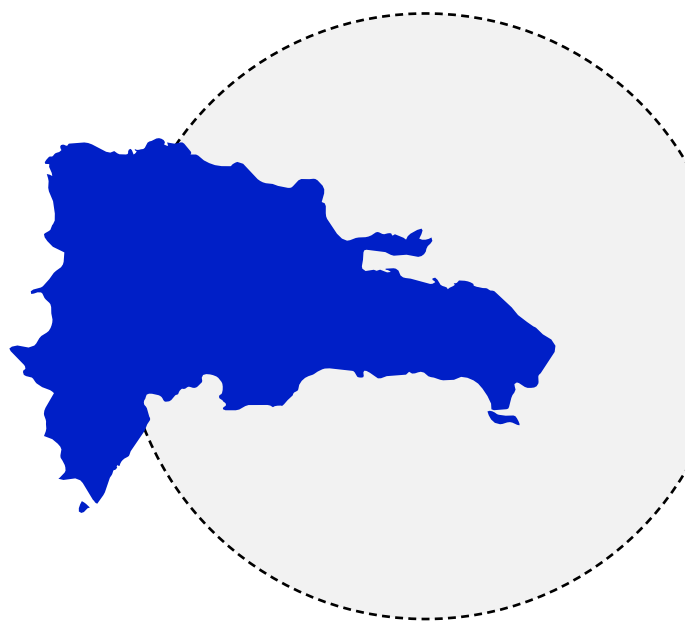
09. REPÚBLICA DOMINICANA

El país se encuentra en el **puesto 29** de la National Cyber Security Index, es el primer país de América en el ranking por delante de Estados Unidos y Canadá.

Dado el buen desempeño de las medidas orquestadas desde las agencias gubernamentales, el país ha ido avanzando desde el puesto 58 con medidas específicas como la Agenda Digital 2030 y la Estrategia Nacional de Seguridad 2030.

Además, República Dominicana ha establecido su red de colaboración a través de asociaciones como el Centro de Cibercapacidades para Latinoamérica y el Caribe (LAC4).

Sin embargo, dado el desarrollo económico de la zona, sigue siendo un objetivo para grupos especializados de ciberdelincuentes.



APT BUDWORM



En junio de 2023 se identificó una campaña de una APT llamada "Budworm" dirigida principalmente contra Taiwán, pero que contenía dominios y direcciones IP de República Dominicana. Con respecto a dicho *ransomware*, se han detectado ataques de grupos reconocidos en la escena cibercriminal como Rhysida, Medusa y Alphv contra empresas del sector público, energético y sanitario.

La información obtenida nos muestra que República Dominicana no está exenta de sufrir todo tipo de ciberataques. Tanto el *ransomware*, como los grupos APTs, están presentes en la región en sectores estratégicos y se espera que esta situación continúe en los próximos meses con una perspectiva similar.

Un tipo de ataque que no se ha observado es la denegación de servicio por parte de actores hacktivistas. Si bien en este mes de marzo la viceministra de Asuntos Exteriores de Ucrania se reunió con el Embajador de República Dominicana en Alemania, los hacktivistas no han atacado de momento el país caribeño.



Correo Electrónico Empresarial (BEC)

Por otro lado, uno de los ciberataques más destacados en los últimos años es el Compromiso de Correo Electrónico Empresarial (BEC por sus siglas en inglés), el cual, es un ciberataque en el que los atacantes se hacen pasar por trabajadores o socios de confianza de una empresa (lo que se denomina ataque de ingeniería social) para engañar a los empleados y obtener información confidencial o realizar transferencias de dinero hacia cuentas de los ciberdelincuentes.

El caso más conocido de BEC es el llamado "Fraude del CEO" donde los atacantes envían correos electrónicos a los empleados del departamento financiero, instándoles a realizar transferencias de fondos a una cuenta bajo su control, haciéndose pasar por el CEO o el director general de la empresa.



ATAQUES DE PHISHING

Forbes califica los ataques de *phishing* en la zona actualmente como "epidemia", donde 4 de cada 10 intentos de *phishing* se dirigen a datos financieros, entre los que estarían este tipo de ciberataques BEC.

Para combatir estos tipos de ataque basados en ingeniería social, es fundamental el uso responsable de la tecnología.

En febrero de este año, el Centro Nacional de Ciberseguridad (CNCS), adscrito al Ministerio de la Presidencia, ha formalizado un informe sobre la evaluación del nivel de madurez de ciberseguridad de la zona coordinándose con la Policía Nacional del país.



FRAUDE ONLINE

En los últimos años se están desmantelando redes locales dedicadas al fraude *online*, muchas veces contra ciudadanos estadounidenses.

Un ejemplo de lo anterior se dio en la operación Discovery en agosto de 2023, cuando se arrestaron a 24 personas que en un call center que llamaban a personas de avanzada edad en Estados Unidos para que enviaran dinero bajo coacción.



RIESGOS Y DEBILIDADES



Mayor riesgo de ciberataque sobre infraestructuras críticas e instituciones gubernamentales.



Presencia de varios grupos de *ransomware* atraídos por la prosperidad económica del país con respecto al resto de la región.



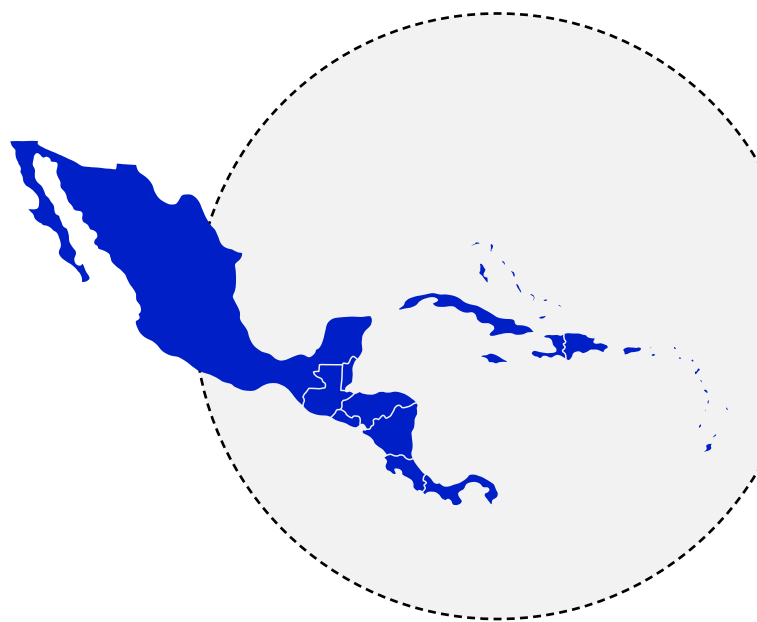
Creciente número de ciberataques vía email por ingeniería social (BEC).



10. RESTO DEL CARIBE

La región del Caribe tiene unas pautas parecidas a otras zonas de Centroamérica a nivel de ciberseguridad, aunque un desarrollo inferior a nivel gubernamental en cuanto a planes y estrategias de ciberseguridad.

En 2022, se registraron un promedio de 1.200 ataques de *ransomware* por semana en América Latina y el Caribe, y todo indica que las cifras han ido a peor durante 2023. Según un informe de la OEA, el 60% de los países del Caribe no tiene una estrategia nacional de ciberseguridad.



Cabe destacar que, para fomentar la colaboración interestatal en materia de ciberseguridad en septiembre de 2023, Costa Rica, Honduras, Panamá y República Dominicana han creado una Alianza de Ciberseguridad, de modo que Los centros de respuesta a incidentes de seguridad informática (CSIRT) de estos países firmaron un memorando de entendimiento para promover la cooperación y mejorar el intercambio de información a nivel de ciberseguridad en Centroamérica y el Caribe.



ATAQUES DE RANSOMWARE

Todos los países del Caribe han sufrido un aumento de ataques de *ransomware*, con un enfoque en las infraestructuras críticas como los gobiernos y los servicios públicos. Se calcula que el costo promedio de un ataque de *ransomware* para las empresas del Caribe es de \$100.000.

Se ha observado un aumento en la actividad de grupos de ciberdelincuencia conocidos, como FIN7 y REvil, que operan en la región.



VECTORES DE ENTRADA

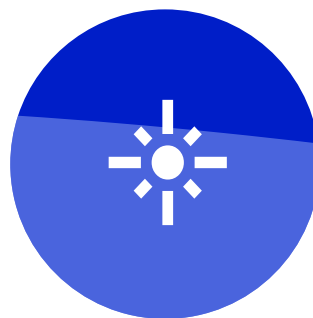
Los vectores de entrada para estos ciberataques son principalmente explotando las vulnerabilidades de software desactualizadas, como las de Microsoft Exchange y SolarWinds, para obtener acceso a sistemas informáticos, o también aquellos relacionados con la cadena de suministro, ya que se están utilizando estas vías de entrada para vulnerar empresas del Caribe a través de sus proveedores.



RIESGOS Y DEBILIDADES



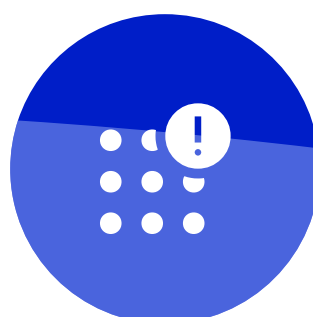
Aumento de los ataques de *ransomware*.



Mayor actividad de grupos ciberdelincuentes de relevancia.



Explotación de las vulnerabilidades de *software*.



Aumento de los ataques a la cadena de suministro.

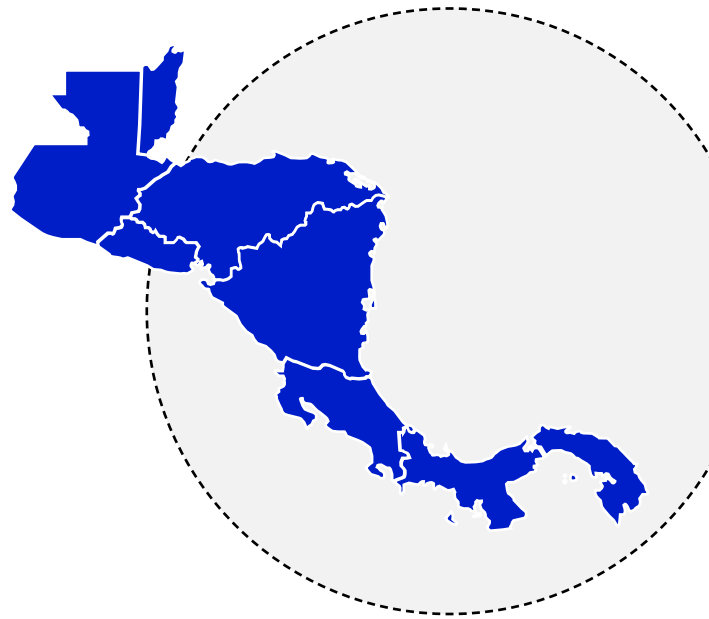


11. RECOMENDACIONES

Las medidas de ciberseguridad más eficientes son aquellas que están orientadas a mejorar la madurez de sus sistemas y la educación de sus ciudadanos y trabajadores.

Para que la madurez se materialice es necesario que, desde el poder legislativo, se establezcan unos buenos estándares de seguridad y se invierta en educación y desarrollo tecnológico seguro.

A continuación, se facilitan una serie de medidas imprescindibles para aumentar la madurez en ciberseguridad.



DESARROLLAR PLANES DE CIBERSEGURIDAD NACIONALES

Implementar una estrategia nacional de ciberseguridad y desarrollar foros de comunicación entre las distintas organizaciones privadas y públicas de la zona que permitan compartir información de amenazas y promover un enfoque integral de ciberseguridad para fortalecer tanto los sistemas gubernamentales como las infraestructuras críticas.

INVERTIR EN SOLUCIONES TECNOLÓGICAS DE CIBERSEGURIDAD

Adquirir e implementar soluciones de ciberseguridad avanzadas, como *firewalls*, sistemas de detección de intrusiones, antivirus, prevención de fuga de datos, etc.

CAPACITAR A LOS USUARIOS SOBRE LA CIBERSEGURIDAD

Promover la concienciación sobre los riesgos de ciberseguridad y la importancia de las mejores prácticas en este ámbito.

La educación es fundamental para que las organizaciones y los individuos comprendan y aborden las ciberamenazas.

DESARROLLAR UNA FUERZA LABORAL DE CIBERSEGURIDAD CUALIFICADA

Se hace necesario Invertir en la formación y certificación de profesionales en ciberseguridad para fortalecer las capacidades internas de las organizaciones y entidades públicas.

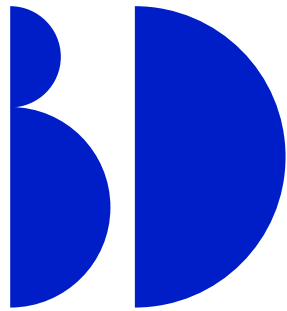
DESARROLLO NORMATIVO

Invertir en el cumplimiento de regulaciones y estándares de ciberseguridad aplicables a nivel nacional e internacional, que fuerce a todos los componentes sociales a mantener una política de ciberseguridad aceptable.

12. BIBLIOGRAFÍA

- [Forbes | Phishing la nueva epidemia](#)
- [Policianacional.gob.do | policia nacional de la republica dominicana recibe informe sobre evaluacion de ciberseguridad](#)
- [Insightcrime.org | Dominican Republic Cybercrime Ring Shows Extent of Caribbean's Financial Fraud Crisis](#)
- [Occrp.org | Cyber scam network dismantled in Dominican Republic](#)
- [segurilatam.com | Alianza de ciberseguridad en centroamerica y el caribe](#)
- [advicegroup-latam.com | Estadísticas de ciberseguridad en Centroamérica y Colombia](#)
- [icex.es | El mercado de la ciberseguridad en Panama](#)
- [Revisa Martes Financiero | Más de mil ataques de ciberseguridad por semana reciben empresas en Panamá](#)
- [ega.ee | NCSI: Panama](#)
- [panama24horas.com.pa | Panorama de Amenazas 2023 de Kaspersky destaca el crecimiento de los ciberataques en Centroamérica – Noticias de panamá Periódico diario de Panamá Novedades](#)
- [soymireyarodriguez.com | 1164 veces por semana es atacada en promedio una organización en Panamá](#)
- [panama24horas.com.pa | Predicciones de ciberseguridad de Check Point y Soluciones Seguras para el 2024](#)
- [welivesecurity.com | Grandoreiro: análisis de un troyano bancario dirigido a Brasil, España, México y Perú](#)
- [welivesecurity.com | ESET participa en una operación internacional para desarticular el troyano bancario Grandoreiro](#)
- [ega.ee | NCSI: Belize](#)
- [breakingbelizenews.com | Ransomware hackers released compromised data after Belize Electricity Limited \(BEL\) missed 'deadline'](#)
- [lovefm.com | Online Shopping Scams Surge in Belize: Buyers Left in Financial Woes](#)
- [augustman.com | 7 Private Islands Owned By Celebrities Including Shakira & Johnny Depp](#)
- [oas.org | Belice](#)
- [lovefm.com | Ukraine's Deputy Foreign Ministers Visits Belize](#)
- [ega.ee | NCSI: Costa Rica](#)
- [elespanol.com | Costa Rica, de paraíso natural a un país a la vanguardia de la ciberseguridad en Latinoamérica](#)
- [usaid.gov | Evaluación país del ecosistema digital – Honduras](#)
- [Kaspersky | El panorama de amenazas para 2023 de Kaspersky también revela un aumento del 50% en los ataques de troyanos bancarios en la región, lo que equivale a 5 ataques por minuto](#)
- [welivesecurity.com | ESET Security Report 2023: el panorama de la seguridad en las empresas de América Latina](#)
- [criptonoticias.com | Casi 20% de los ciberdelitos en El Salvador y Guatemala se relacionan con criptomonedas](#)
- [Diario El Mundo | Stefanini: los ciberataques pueden ser 'millones' en El Salvador cada mes](#)
- [revistaeyn.com | Empresas en Costa Rica, Guatemala y El Salvador entre las más vulnerables a ciberataques](#)
- [ujmd.edu.sv | La pequeña y mediana empresa en El Salvador](#)
- [DPL News | El Salvador – Aumenta la exposición de empresas a los ciberataques](#)
- [sophos.com | Informe sobre el ransomware 2023: El estado del ransomware](#)
- [criptonoticias.com | Casi 20% de los ciberdelitos en El Salvador y Guatemala se relacionan con criptomonedas](#)
- [mascontainercentroamerica.com | Panamá ha sufrido 1500 millones de ciberataques en 2023](#)
- [numu.group | Evento Ciberseguridad RD](#)
- [global-strategy.org | Estrategias Nacionales de Ciberseguridad en América Latina](#)





BeDisruptive™
It's an attitude

Limiting threats for an unlimited future.



**BICSA Financial Center, Piso 46, Avenida
Balboa y Calle Aquilino de la Guardia.
Panamá, República de Panamá.**



**Contáctanos en
info@bedisruptive.com**



www.bedisruptive.com

© 2024 | BeDisruptive

El presente documento ha sido desarrollado y es de titularidad de DISRUPTIVE CONSULTING, SL (en adelante, "BeDisruptive"). La información contenida en el mismo es de carácter general y orientativo y no pretende constituir un asesoramiento técnico, profesional o jurídico que pueda conllevar responsabilidad del autor del texto. Del mismo modo, el presente documento tiene finalidades meramente informativas y no puede ser usado con fines académicos e históricos. La información contenida en el texto no es necesariamente exhaustiva, completa, exacta ni actualizada; contiene en algunas ocasiones enlaces a páginas externas sobre las que BeDisruptive no tiene control alguno y respecto de cuyo contenido BeDisruptive declina toda responsabilidad.