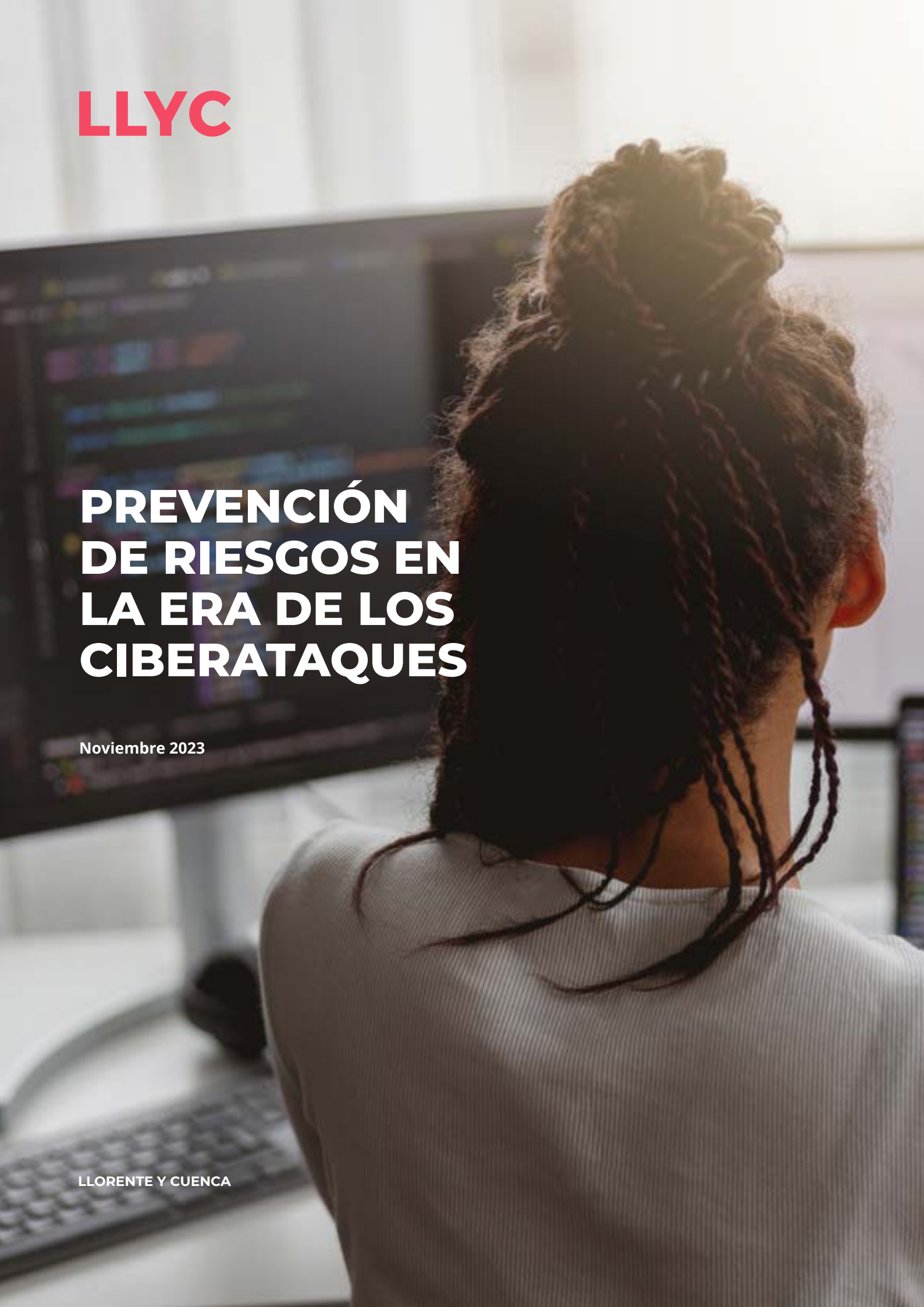
LLYC

PREVENCIÓN DE RIESGOS EN LA ERA DE LOS CIBERATAQUES

Noviembre 2023



LLORENTE Y CUENCA

ÍNDICE

LLYC

INTRODUCCIÓN

INTRODUCCIÓN

En esta era de innovación y digitalización, la tecnología se ha convertido en la columna vertebral de los gobiernos, las organizaciones y las empresas público-privadas que diseñan estrategias de gestión, marketing y servicio al cliente con nuevas y mejores experiencias para la población, los usuarios, los clientes, los colaboradores y los proveedores.

Las organizaciones empresariales se han comprometido en esta carrera contra el tiempo, y en los últimos años han convertido sus avances tecnológicos en un diferenciador clave en el mercado. Sin embargo, al tiempo que las empresas aumentan su reconocimiento y su participación en el mercado, y generan mejores experiencias, aumentan también los riesgos de ciberseguridad asociados a su propiedad intelectual, los procesos y los datos confidenciales de sus propios clientes/usuarios, sus colaboradores y sus empleados.

Estos riesgos, además, seguirán creciendo ante el avance de los sistemas de inteligencia artificial (IA), que está amenazados, por ejemplo, por la inyección de *prompt,* o *prompt injection*, una técnica empleada por los ciberdelincuentes para manipular la entrada, o instrucciones, que se le proporcionan a la IA.

Según el último Informe de Riesgos Globales del Foro Económico Mundial 2023, **el ciberataque y la inseguridad cibernética están en el top 10 de los riesgos globales** más graves de la última década. La actividad maliciosa en el ciberespacio está creciendo con más ataques agresivos y sofisticados que se aprovechan de una exposición cada vez más amplia y generalizada.

De acuerdo al ESET Security Report (ESR) Latinoamérica de 2023, informe que aborda el estado de la ciberseguridad corporativa en la región durante el 2022, las tendencias en ciberseguridad y cibercrimen en el ámbito corporativo, lejos de atenuarse, se orientaron en gran medida a grandes ataques y caídas de bandas de *ransomware*. Y también al impacto de vulnerabilidades de gran criticidad y con importante presencia desde hace algún tiempo.

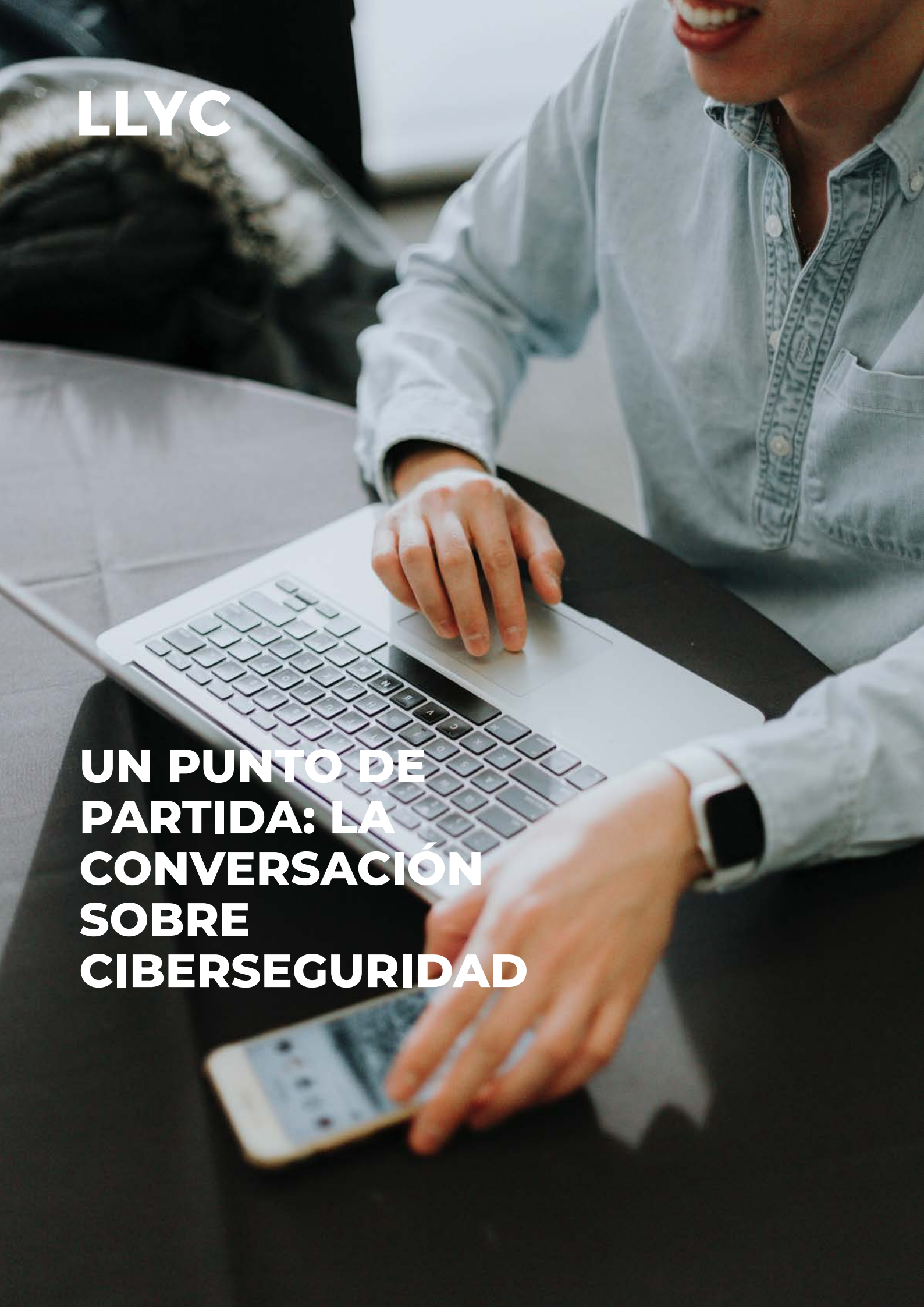
El informe encontró que **65%** de los encuestados asegura que el presupuesto asignado al área de **ciberseguridad no es suficiente** y que las **detecciones de vulnerabilidades** rompieron un récord en 2022, con más de **25 mil reportes,** lo que representa un **aumento del 26%** sobre el año anterior.

Un reciente artículo de EY asegura que "la cantidad de ataques cibernéticos dirigidos a OT (tecnologías de operación) ha aumentado drásticamente. De acuerdo con el Cyber heat map 2022 de Moody's, **la infraestructura crítica se encuentra bajo el mayor riesgo general,** y se consideran de muy alto riesgo los servicios públicos de electricidad, gas y agua y los hospitales. Los sectores de alto riesgo incluyen bancos, tecnología, telecomunicaciones, empresas de productos químicos y energía *midstream* (transporte de combustibles)".

Según este mismo artículo, **los costos globales de daños por delitos cibernéticos en el 2023 representarán US$ 8 billones,** una cifra que ascenderá a US$ 10,5 para el 2025. Esto, sin contemplar los daños reputacionales a los que se enfrentan las compañías que a causa de un ciberataque ponen en riesgo no solo información confidencial de propiedad intelectual y procesos, sino los datos confidenciales de sus *stakeholders*, con lo que rompen uno de los ejes fundamentales de la relación con ellos: la CONFIANZA.

Ante este escenario, las empresas deben avanzar hacia estrategias de antifragilidad, y ya no solo gestionar estos riesgos desde la anticipación. La hipertransparencia y la comunicación serán clave para conservar la confianza.

LLYC



UN PUNTO DE PARTIDA: LA CONVERSACIÓN SOBRE CIBERSEGURIDAD

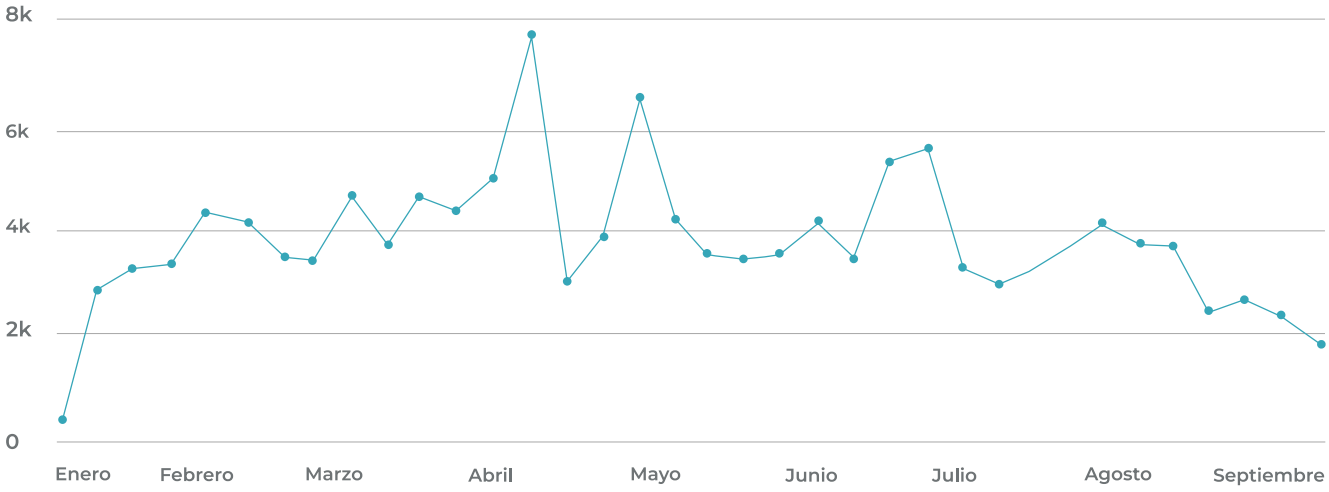
UN PUNTO DE PARTIDA: LA CONVERSACIÓN SOBRE CIBERSEGURIDAD

Comprendiendo que en esta nueva era de permacrisis, los ciberriesgos han aumentado exponencialmente su impacto y su probabilidad, realizamos un análisis de *big data* acerca de la conversación sobre ciberseguridad en Twitter, medios digitales, foros y blogs en México, República Dominicana y Panamá entre enero y agosto de 2023.

En estos ocho meses de conversación *online* se analizaron datos masivos con foco en la identificación de comunidades y sus influyentes. Se combinaron técnicas para la clasificación de temáticas con Procesamiento de Lenguaje Natural (NLP, por sus siglas en inglés), *kw matching y machine learning.* Además de técnicas de análisis de grafos, modularidad y centralidades para la identificación de comunidades.

De esta manera, se identificaron un total de 132.1k mensajes y 33.2k perfiles en torno a la conversación sobre ciberseguridad. De los cuales 91.3% son de México, 5.4% República Dominicana y 3.3% de Panamá.

VOLUMEN DE MENCIONES: "CIBERSEGURIDAD"
(AÑO 2023)



LLYC

¿QUÉ ES LO QUE MÁS PREOCUPA Y DE LO QUE MÁS HABLAN LOS USUARIOS EN EL TERRITORIO DE LA CIBERSEGURIDAD?

El análisis de la data destaca un Top 3 de temas prioritarios para los usuarios:

- Ciberataques
- Robo de bases de datos
- Espionaje

Sin embargo, la realidad de la conversación varía de acuerdo al país analizado. Los antecedentes, los incidentes ciber o la demanda de una mejor protección de los datos modifican las temáticas de las que hablan los usuarios y el tono de la conversación positiva, neutra y negativa.

En los tres mercados la conversación sobre los ciberataques en sus distintas modalidades —troyanos, virus, *phishing*, denegación de servicio, etc.— lideran la conversación con tono negativo. En los tres países, la conversación neutra es mayormente conducida por los medios de comunicación, con un foco en la divulgación de información sobre prevención y protección frente a la nueva amenaza ciber. Por último, la conversación positiva sí varía por país, pero en general exalta eventos y acciones del sector privado para contribuir en la educación de los usuarios para proteger su información digital.

Con la información extraída de la conversación digital hemos llevado a cabo un análisis de la realidad mercado por mercado, complementada con la opinión de expertos de México, República Dominicana y Panamá, para comprender cómo los sectores donde se desempeñan están gestionando los riesgo reputacionales que se derivan de los ataques cibernéticos y si la voz de los usuarios en redes se está tomando en cuenta.

LLYC

MÉXICO: ENTRE LA INCERTIDUMBRE DE LOS CIBERATAQUES Y LA OPORTUNIDAD DE ANTICIPAR Y COMUNICAR

MÉXICO:

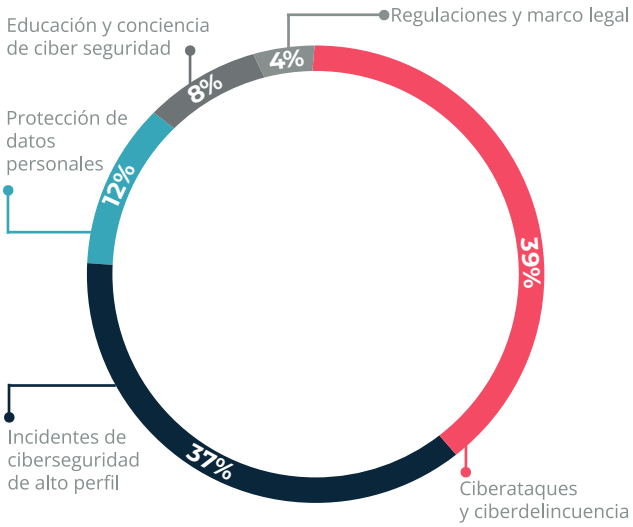
ENTRE LA INCERTIDUMBRE DE LOS CIBERATAQUES Y LA OPORTUNIDAD DE ANTICIPAR Y COMUNICAR

TÓPICOS PRIORITARIOS EN LA CONVERSACIÓN DE MÉXICO

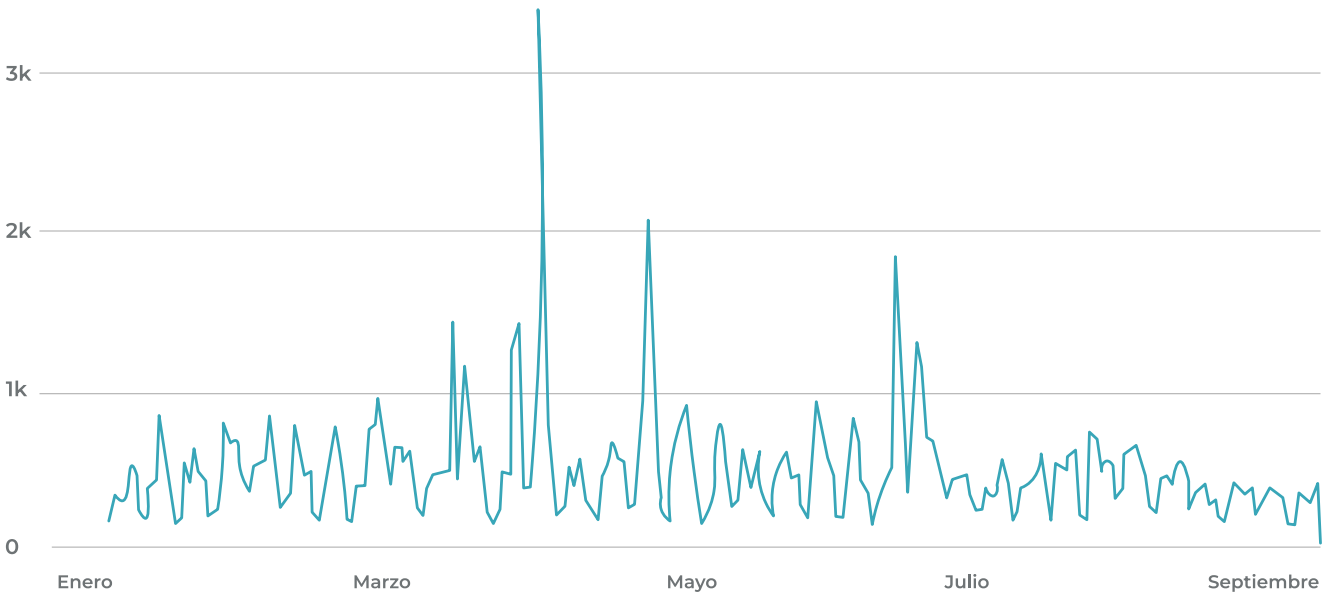
Según información de Fortinet, en la primera mitad de 2022 los intentos de ciberataque en Latinoamérica crecieron un 50% frente al mismo periodo del año anterior. **México fue el país más atacado de la región con 85 mil millones de intentos.** De esto da cuenta el análisis de la conversación digital en México entre enero y agosto del 2023, en la que más de 30 mil perfiles en redes sociales y páginas web generaron más de 120 mil menciones alrededor de temas de ciberseguridad y ciberdelincuencia.

Los temas más relevantes entre los cibernautas mexicanos se concentraron entre el pánico y la desinformación alrededor de incidentes detectados y amenazas de ciberataques, Y, en un menor porcentaje, pero con foco de poder crecer, en conversaciones alrededor de la protección de datos, la eduación/ conciencia y ,las regulaciones, con un tono más neutral y en muchos casos positivo.

TERRITORIOS DE CONVERSACIÓN: "CIBERSEGURIDAD MÉXICO" (AÑO 2023)



VOLUMEN DE MENCIONES: "CIBERSEGURIDAD MÉXICO" (AÑO 2023)



TRANSPARENCIA ANTE ATAQUES

Según información de FortiGuard Labs, en 2021 México recibió 14 billones de amenazas cibernéticas de un total de 41 billones en toda América Latina. Con alrededor del 34% del total, es el segundo país del área que sufre más ataques de *ransomware.*

Esta realidad analizada en la conversación digital en México indica que en lo corrido del 2023, el 21% de la conversación ha sido en gran medida negativa. Y se basa principalmente en la comunicación del impacto que han generado los ciberataques a figuras de alto perfil y a la preocupación general de los mexicanos por ser víctimas de estos hechos.

"Tanto el volumen como la complejidad de las amenazas cibernéticas han aumentado y evolucionado de manera significativa en los últimos años. Un área que se ha convertido en un generador de amenazas importantes para las organizaciones es la cadena de suministro y el manejo de relaciones con terceros", asegura Carlos A.P. Chalico, Socio Líder de Ciberseguridad y Privacidad de datos, EY Canadá.

Dentro de los principales temas identificados en la conversación negativa de los cibernautas mexicanos están:

- **Ciberataques y *ransomware*:** Un informe revela que el 85% de las organizaciones han experimentado al menos un ciberataque y el 80% de ellos ha pagado un rescate. Sin embargo, esto no garantiza la recuperación de los datos.

- **Preocupaciones sobre ciberseguridad en relación a Starlink:** Funcionarios de inteligencia y ciberseguridad están preocupados por las conversaciones sobre Starlink. Los países temen alienar a Elon Musk y sus prioridades nacionales y geopolíticas.

- **Riesgos de ChatGPT para la ciberseguridad:** El uso de ChatGPT y sus variantes maliciosas plantea riesgos para la seguridad cibernética, ya que los usuarios expresan preocupaciones sobre la posibilidad de que pueda codificar *software* malicioso capaz de espiar.

Estos tópicos generadores de conversaciones negativas y de incertidumbre evidencian la ausencia de una labor proactiva y de liderazgo por parte de las compañías en el plano de la comunicación, los planes proactivos de identificación y la gestión de riesgos reputacionales.

Así lo afirma *Stefan Moller, CEO* de Klar cuando dice que "la transparencia y una comunicación efectiva después de un incidente de ciberseguridad no solo son esenciales para mantener y restaurar la confianza, sino que también desempeñan un papel crucial en la resolución ágil del problema y la prevención de futuros desafíos. Al comunicarnos de manera clara y oportuna con nuestros clientes y partes interesadas, facilitamos una comprensión más rápida del incidente, permitiendo a todos tomar las medidas adecuadas".

Agrega Klar que "además, el *feedback* y la colaboración que surge de una comunicación transparente pueden iluminar áreas de mejora y ayudarnos a fortalecer nuestras defensas. Siendo la claridad uno de nuestros valores fundamentales, creemos que una comunicación abierta no solo es una responsabilidad, sino una herramienta vital para construir un ecosistema financiero más seguro y resiliente".

UNA RESPUESTA FAVORABLE A LA PREVENCIÓN Y EDUCACIÓN, QUE NO SIEMPRE ESTÁ PRESENTE

Pese a los altos niveles de riesgo de un ciberataque en varios sectores público-privados, en las conversaciones digitales en México predomina un tono neutral, con un 77% de conversaciones centradas en informar de incidentes de ciberseguridad al Gobierno y en especial en las acciones y recomendaciones para la prevención.

Durante el período comprendido entre enero y agosto de 2023, los mexicanos también mantuvieron un 2% de conversaciones positivas alrededor de acciones e iniciativas que buscan concientizar y prevenir situaciones de riesgo en materia de ciberseguridad para empresas y particulares. Así bien, los principales tópicos concentrados en tonos neutrales y positivos dan cuenta de la oportunidad que tienen las compañías de aprender a vivir entre la incertidumbre de los ciberataques anticipando acciones para salvaguardar su seguridad y reputación.

PRINCIPALES TÓPICOS EN TONO NEUTRO Y POSITIVO:

- **Ciberseguridad y ciberataques:** Muchos titulares hacen referencia a la ciberseguridad y los ciberataques. Se habla de hackeo, espionaje, delitos cibernéticos y protección contra estos ataques.

- **Eventos y ferias:** Hay titulares sobre próximos eventos, conferencias y ferias relacionadas con la ciberseguridad y otros campos especializados como la seguridad pública, las comunicaciones electrónicas y la seguridad industrial.

- **IA y tecnologías emergentes:** Algunos titulares mencionan el impacto de la inteligencia artificial y otras tecnologías emergentes, como el uso de IA para detectar noticias falsas y desinformación, así como su aplicación en diferentes aspectos de la vida y la economía.

- **Polémica sobre herramientas de espionaje y contratos de gobierno:** Se mencionan disputas relacionadas con el uso de herramientas de espionaje, contratos del gobierno y la implicación de contratistas en la obtención de información sensible.

"Históricamente hemos visto muchos casos en los que, al enfrentar un incidente de ciberseguridad, las compañías se enfrentan a mayores consecuencias por un pobre manejo de comunicaciones y relaciones públicas al comunicar el incidente, que por el incidente mismo. Es importante definir una estrategia para comunicar debidamente a todas las partes interesadas cuando haya un ataque o amenaza de ciberseguridad, y establecer mecanismos para un protocolo de comunicación tanto reactivo como proactivo", asegura Carlos A.P. Chalico, Socio Líder de Ciberseguridad y Privacidad de datos, EY Canadá.

Después de analizar las conversaciones *online* en México en tono neutro y positivo, se podría concluir que los mismos cibernautas están dándole a las compañías las pautas de cómo anticiparse ante este tipo de riesgos y amenazas cada vez más latentes y cercanos. Las compañías necesitan entender que su reputación depende de gestionar este tipo de situaciones y riesgos a través de una comunicación proactiva, llenando vacíos de información que han ido llenando las conversaciones alrededor del miedo y la desinformación, transmitiendo que los ciberataques y la ciberdelincuencia son una realidad y que solo al anticiparse se pueden generar relaciones de confianza con sus grupos de interés.

"Primero, la base de la industria financiera es la **confianza:** o sea, el **principal activo** que tiene un banco es la confianza que tienen los clientes en nosotros. Entonces nosotros, para poder seguir gozando de esta confianza, pues hacemos unas metodologías de trabajo tanto internas como externas. Entonces se hacen de manera continua **ejercicios de simulación,** de penetración. Tienen diferentes tipos de denominación, son pruebas de intrusión en nuestro sistema de diferente naturaleza, y eso es un ejercicio que se realiza de manera continua. Y eso pues nos permite determinar puntos de mejora dentro de todos los sistemas de toda la infraestructura de seguridad y política de seguridad que tenemos", afirma un alto ejecutivo de la banca en México.

Guardar silencio o manejar un bajo perfil frente a este tipo de situaciones o actuar de manera reactiva ya no es una opción. Para Paul Lara, periodista de Excélsior, "en el caso de México hace falta mucho el tema de comunicación exterior, muchas empresas que lamentablemente son vulneradas, cibernéticamente o inclusive que han sido atacadas y a lo mejor han logrado sobrevivir a este ciberataque, muchas veces no comunican. Cuando normalmente son afectadas, es cuando menos comunican por el tema de reputación. No quieren dar a conocer que fueron vulneradas"

Sin ninguna duda, la responsabilidad frente a los ciberataques y la ciberdelincuencia es responsabilidad de todos, tanto de las compañías como de sus grupos de interés. Pero son las empresas las llamadas a levantar la voz, a prepararse, anticiparse y abrir los canales necesarios para construir confianza y un cerco de protección para todos los involucrados. "La comunicación es esencial para enfrentar ciberriesgos. No solo es vital mantener informados a nuestros clientes, sino que también es crucial asegurarnos de que nuestro equipo interno, los reguladores y nuestros proveedores estén al tanto. Ya sea para garantizar una respuesta rápida, mantener la confianza, asegurar la transparencia con las autoridades o para trabajar en conjunto con nuestros socios, consideramos la comunicación en múltiples niveles como un pilar fundamental en la prevención y gestión de riesgos cibernéticos" asegura *Stefan Moller, CEO* de Klar.

LLYC

REPÚBLICA DOMINICANA: LA DENUNCIA COMO HERRAMIENTA DE CONCIENCIA Y LA PREVENCIÓN CON TECNOLOGÍA Y EDUCACIÓN

REPÚBLICA DOMINICANA:

LA DENUNCIA COMO HERRAMIENTA DE CONCIENCIA Y LA PREVENCIÓN CON TECNOLOGÍA Y EDUCACIÓN

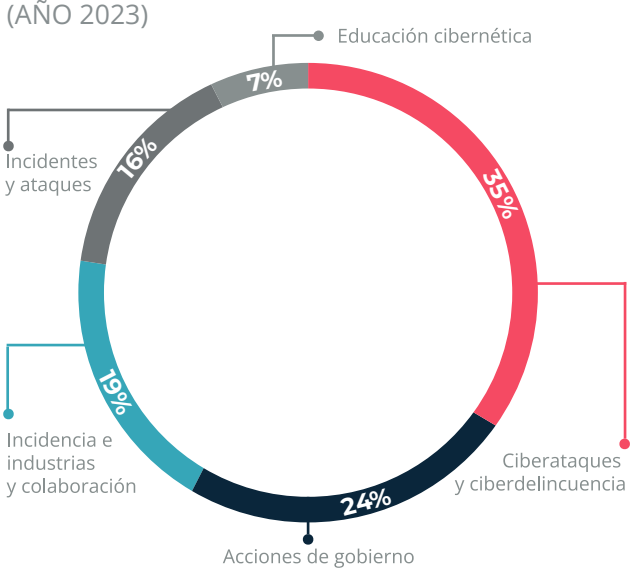
TÓPICOS PRIORITARIOS EN LA CONVERSACIÓN DE REPÚBLICA DOMINICANA

En el primer semestre de 2023, **República Dominicana fue víctima de 470 millones de intentos de ciberataques,** de acuerdo con el informe Panorama Global de Amenazas, realizado por FortiGuard Labs, el área de inteligencia contra amenazas de Fortinet. El mayor pico de conversación se registró en agosto, mes en el que coincidieron el caso del exjugador de Grandes Ligas David Ortiz, *Big Papi,* quien denunció ser víctima de extorsión tras sufrir un hackeo a su información personal, y el ataque que se concretó contra el Instituto Agrario Dominicano (IAD).

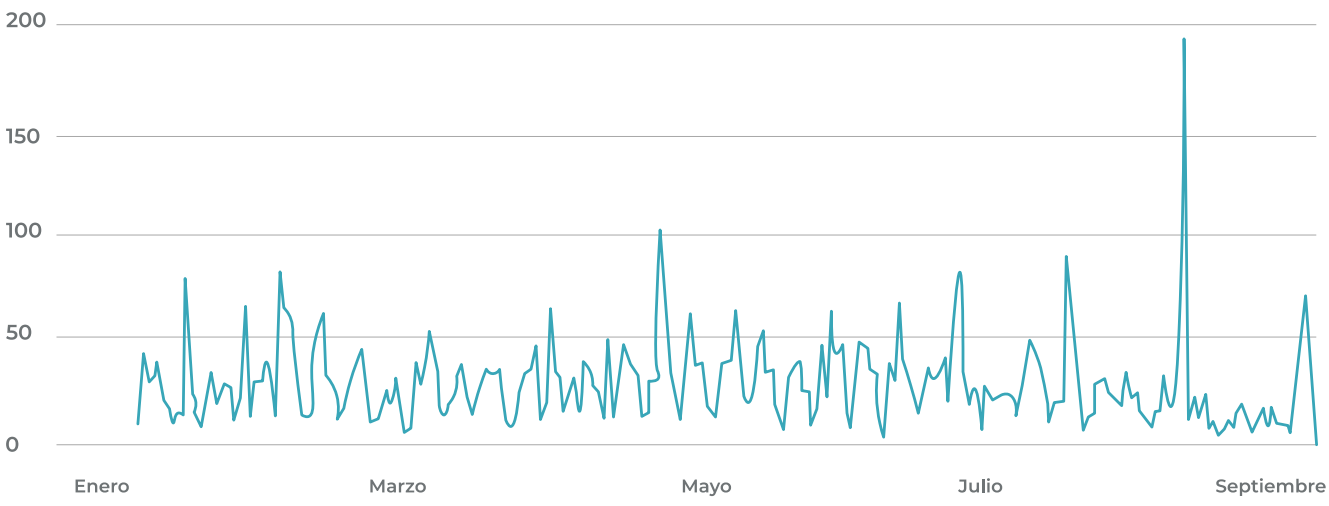
El segundo momento de mayor conversación sobre ciberseguridad en el periodo analizado fue en mayo, con la atención que atrajo la denuncia de la periodista y presentadora Nuria Piera de ser espiada luego de detectar el *spyware* o *software* espía Pegasus en su teléfono móvil.

El análisis de la conversación sobre ciberseguridad en las redes en República Dominicana arroja más de 7 mil 100 menciones generadas por más de mil 700 perfiles que se pueden resumir en cinco temáticas principales para los cibernautas dominicanos:

TERRITORIOS DE CONVERSACIÓN: "CIBERSEGURIDAD REPÚBLICA DOMINICANA"
(AÑO 2023)



VOLUMEN DE MENCIONES: "CIBERSEGURIDAD REPÚBLICA DOMINICANA"
(AÑO 2023)



Precisamente, los primeros dos tópicos con mayor volumen de conversación se ligan tanto al incidente contra el Instituto Agrario Dominicano y el rol que el Centro Nacional de Ciberseguridad (CNCS) jugó para atender el caso con el despliegue del Equipo Nacional de Respuesta a Incidentes Cibernéticos (Csirt-RD), junto a la Oficina Gubernamental de Tecnología de la Información y Comunicaciones (Ogtic), así como al manejo de la comunicación del evento.

El tipo de ataque fue *ransomware,* o secuestro de información, en el que el objetivo de los delincuentes cibernéticos es solicitar un pago de rescate. La CNCS comunicó que el Estado Dominicano no contempla el pago de recompensas.

El *ransomware* es cada vez más dirigido. Arturo Torres, estratega de FortiGuard Labs de Fortinet para América Latina y el Caribe, explica que "FortiGuard Labs ha documentado picos sustanciales en el crecimiento de variantes de *ransomware* en los últimos años, impulsados en gran medida por la adopción de *ransomware* como servicio (RaaS). Otra tendencia en este tipo de ataque es que son cada vez más específicos y dirigidos, gracias a la creciente sofisticación de los atacantes y el deseo de aumentar el monto monetario por ataque".

Por su parte, José David Montilla, Viceministro de Agenda Digital en el Ministerio de la Presidencia de República Dominicana, complementa que "otro tipo de ataque y riesgo cibernético que puede afectar tanto a gobiernos como a compañías es la denegación de servicio, en el que se inhabilitan los servicios digitalizados y disponibles, los dirigidos a infraestructuras críticas que afecten tecnologías operativas y/o los sistemas de control industrial, mermando la disponibilidad de servicios indispensables como energía eléctrica, agua y/o telecomunicaciones, con lo que se puede detener cualquier operación de negocio".

Dentro del análisis de la conversación en torno a los ataques cibernéticos la calificada como negativa sumó mil 200 menciones, representando el 17% del total de lo publicado en República Dominicana, cuyo foco fueron los incidentes de seguridad y las implicaciones para el país.

IDENTIFICAR LOS RIESGOS Y PREVENIRLOS CON TECNOLOGÍA Y CAMPAÑAS DE COMUNICACIÓN INTERNAS

La conversación neutral acapara el mayor volumen de publicaciones, con más de 5 mil 500 menciones, que representan el 79%. Y se centra en comunicar acciones y avances del gobierno en materia de ciberseguridad y experiencias y acciones en materia de formación y educación. En contraste, la positiva representa el 4% con sólo 271 menciones referentes a eventos de difusión en torno a la ciberseguridad y labor preventiva.

Queda claro que la anticipación y la gestión de los riesgos ciber es clave para la continuidad del negocio y su blindaje reputacional. Para Arturo Torres, "las empresas deben considerar la ciberseguridad como parte de su estrategia de negocios adoptando una arquitectura resiliente, que cubra cada capa de la superficie de red: *hardware, software,* puntos de acceso, nube, IoT, etc.; y que sea capaz de extenderse conforme los activos digitales lo hagan. Esto incluye revisiones e inventarios periódicos para asegurar que cada capa está protegida".

"Los cibercriminales son cada vez más sofisticados en sus ataques, utilizan tecnología de punta impulsada por IA y *Machine Learning,* y están constantemente buscando las formas de infiltrar las redes, estos procesos son usualmente muy silenciosos y difíciles de detectar si no se cuenta con las herramientas adecuadas, y la realidad es que una vez que han perpetrado la red es muy difícil recuperar los datos, y operación de las empresas. Y aun cuando se logre si los datos no están inventariados es muy complicado saber si todos han sido devueltos o si no fueron además vendidos en la *dark web*, sin mencionar las pérdidas económicas no solo de pagar un rescate, si no del cese de operaciones o el daño a la reputación que producen los ciberataques", precisó Torres.

La reputación y la confianza de la compañía con sus usuarios, clientes o proveedores se impacta con una vulneración a los sistemas informáticos, y ni decir con un secuestro de información confidencial o la paralización de operaciones.

"La cuantificación de todos los riesgos debidamente identificados y asociados a cada uno de los activos de la organización, en adición a las acciones de mitigación asociadas a cada riesgo, con el objetivo de garantizar la recuperación efectiva, ante la eventual materialización de un evento de riesgo, es primordial", señala José David Montilla, Viceministro de Agenda Digital en el Ministerio de la Presidencia de República Dominicana.

Sin embargo, aunque las compañías estén preparadas con la protección tecnológica y los mecanismos de gobernanza corporativos adecuados, igualmente no saldrán bien libradas de la crisis reputacional ante un ataque si sus colaboradores no son parte de esta estrategia. Es necesario implementar campañas de concientización y educación dentro de las empresas para asegurar una postura de prevención como una buena práctica dentro de la organización.

"El factor humano sigue siendo uno de los más grandes riesgos; por ende, cualquiera que tenga acceso a nuestra red debe estar informado sobre el panorama de amenazas y cómo evitar caer presa de algún actor malicioso. Nuestros colaboradores son la primera línea de defensa cuando hablamos de protegernos contra ciberriesgos", destaca Arturo Torres.

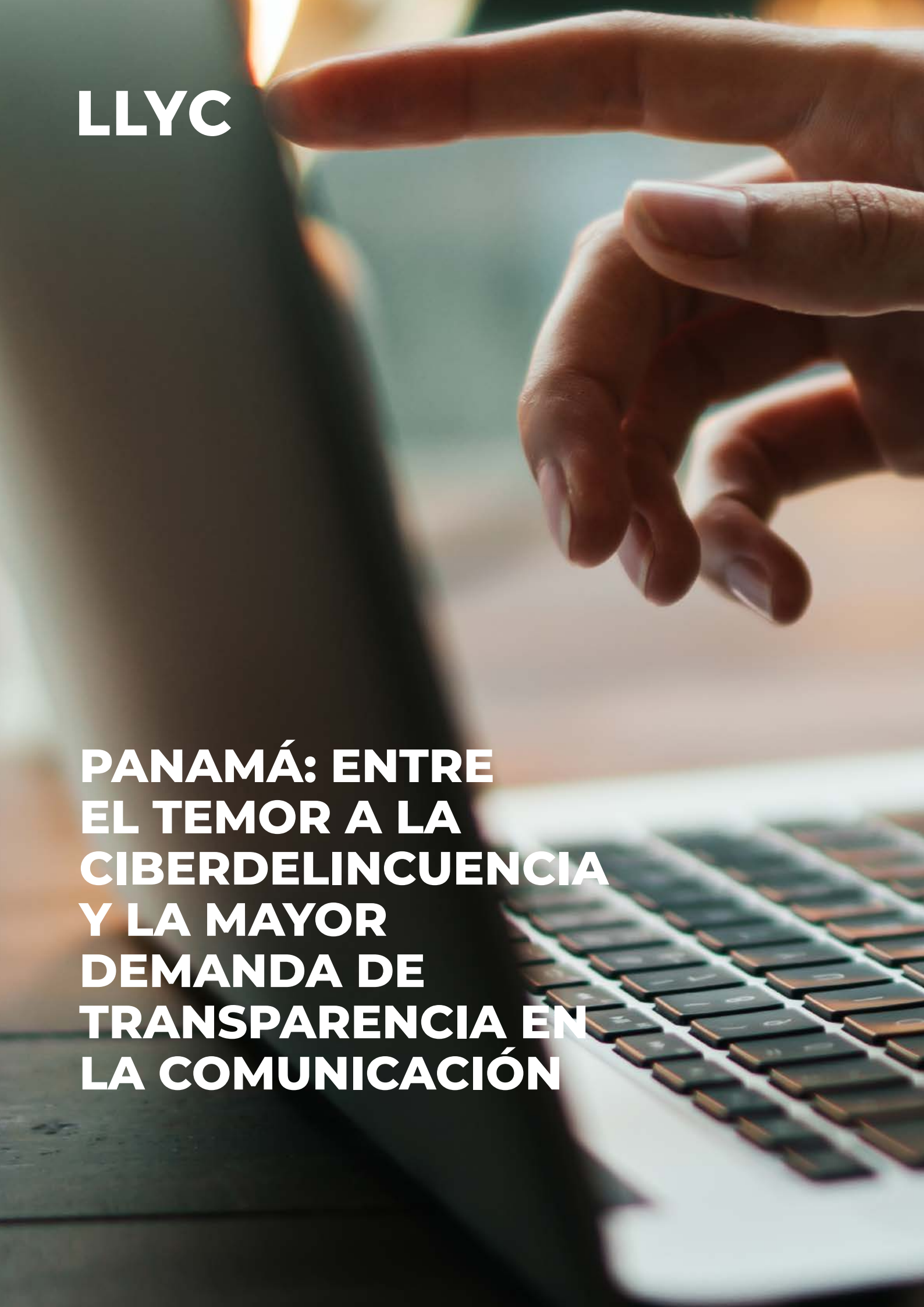
LA COMUNICACIÓN ES CLAVE ANTE EL ATAQUE

Todo sistema puede ser vulnerado y un agente malicioso puede secuestrar información confidencial o inhabilitar sistemas a través de programas que aprovechan vulnerabilidades tanto del *software* como de la concientización en colaboradores. Además de las tecnologías y la educación del talento, se debe considerar una preparación y gestión de los mensajes que se darán a los distintos *stakeholders* de una organización para minimizar el impacto reputacional a partir del control de la narrativa.

Responder con hechos frente a los rumores ayuda a frenar la desinformación. Se debe hacer hincapié en las acciones de mitigación que se están implementando y asumir la responsabilidad del incidente.

"Contar con un plan de comunicaciones ayuda a fortalecer a las organizaciones a responder de manera oportuna y así minimizar el eventual impacto a la reputación de la entidad, y evitar el mermado de la confianza de la población. Evitar la propagación de desinformación, la cual repercute y fortalece una de las motivaciones posibles de los atacantes, que es la afectación de la reputación de la organización y pérdida de la confianza pública", señala José David Montilla.

LLYC



PANAMÁ: ENTRE EL TEMOR A LA CIBERDELINCUENCIA Y LA MAYOR DEMANDA DE TRANSPARENCIA EN LA COMUNICACIÓN

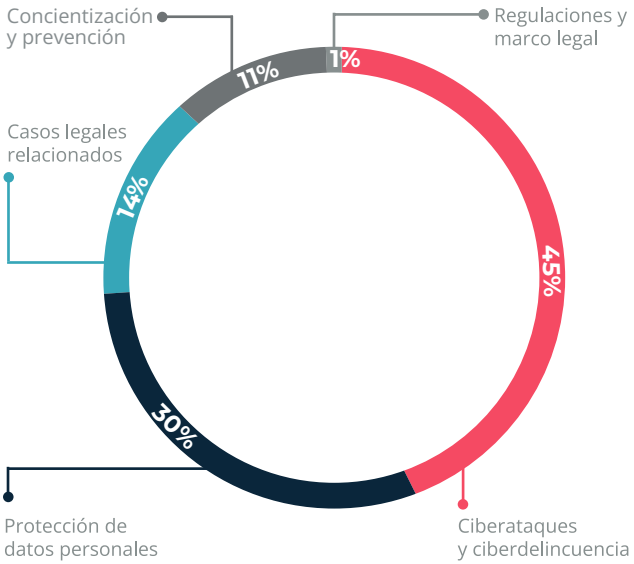
PANAMÁ:

ENTRE EL TEMOR A LA CIBERDELINCUENCIA Y LA MAYOR DEMANDA DE TRANSPARENCIA EN LA COMUNICACIÓN

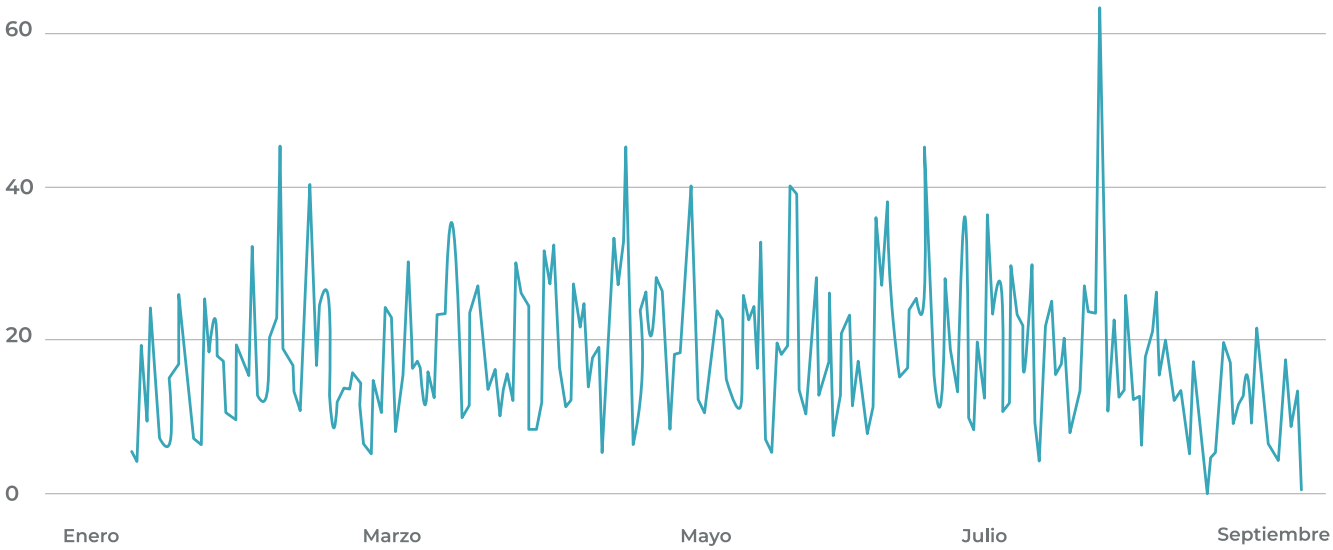
TÓPICOS PRIORITARIOS EN LA CONVERSACIÓN DE PANAMÁ

El análisis de la conversación digital en Panamá muestra que en los tres últimos meses ha decrecido la conversación sobre ciberseguridad en las redes, sin embargo, los más de 4.3 mil menciones generadas por más de 900 perfiles se puede resumir en cinco temáticas principales para los cibernautas panameños:

TERRITORIOS DE CONVERSACIÓN: "CIBERSEGURIDAD PANAMÁ"
(AÑO 2023)



VOLUMEN DE MENCIONES: "CIBERSEGURIDAD PANAMÁ"
(AÑO 2023)



Al hacer un zoom de estos resultados, vemos que el 16% de la conversación es de tono negativo. Está enfocado en su mayoría a reclamos por víctimas de ciberdelincuentes y conversaciones sobre experiencias internacionales de ciberataques. Se agrupan en tres grandes temáticas:

- ***Hacking* y violación de la privacidad:** relacionada a incidentes de piratería informática, violaciones de la privacidad y la importancia de respetar la privacidad. Cuestionamiento por la poca comunicación que hacen las empresas cuando son víctimas de ataques.

- **Ciberataques y *ransomware:*** que han experimentado empresas, hospitales y organismos gubernamentales en el exterior, así como al desmantelamiento de redes internacionales de *ransomware.*

- **Robo de identidad y pirateo de redes sociales:** casos de usurpación de identidad y piratería informática en plataformas de redes sociales, como Facebook y Twitter.

Víctor Betancourt, Gerente General de Sonda Panamá, coincide en que la mayor preocupación para los usuarios, como para las compañías, es el avance de la ciberdelincuencia. Señala que "hay dos tipos de empresas: las que ya les pasó y las que les va a pasar. Las empresas pueden estar invirtiendo en políticas, capacitaciones. Sin embargo, estos defraudadores están buscando constantemente vulnerabilidades nuevas", destaca.

Aunque Panamá puede ser un mercado pequeño en comparación a otro país, sufre estas mismas amenazadas. Así lo destaca el informe Panorama Global de Amenazas de FortiGuard Labs de Fortinet, que indica que Panamá fue objeto de más de 1.500 millones de intentos de ciberataques en el primer semestre de 2023.

Jorge Freiburghaus, de la Comisión de Seguridad Informática de la Asociación Bancaria de Panamá, considera que el grado de preparación de las empresas panameñas en general es intermedio.

"Hay empresas trasnacionales con una madurez mayor, pero que deben practicar localmente sus planes de contingencia y comunicación ante amenazas ciber. Los simulacros constantes permiten que las compañías sean más robustas y ágiles para atender un incidente de ciberseguridad. El mayor reto es que sea un trabajo en equipo entre el personal técnico y las áreas de negocio y de comunicación de las organizaciones, ya que estamos frente a un riesgo que tiene impacto en la confianza de los clientes".

MAYOR TRANSPARENCIA EN LA COMUNICACIÓN

Sumado al temor de perder su información o que quede expuesta, los usuarios panameños cuestionan la poca transparencia del sector público o privado al momento de haber sufrido un incidente de ciberseguridad. Se revive el dilema entre comunicar proactivamente y con transparencia o no comunicar para evitar el pánico.

Para Marie Claire González, representante de GetXplor, que a través de la autogestión y biométrica implementa soluciones digitales con canales omnicanal para múltiples usuarios/clientes, la respuesta siempre será la transparencia y la comunicación oportuna. "En nuestro caso manejamos data muy sensitiva, con lo cual un ciberataque hay que comunicarlo inmediatamente a todos los *stakeholders.* Nuestra primera estrategia es la comunicación interna, limitando el pánico lo mayor posible y asegurando a los clientes todas las medidas"

En esta línea coincide Víctor Betancourt: "a veces los clientes que ni siquiera tuvieron afectaciones quieren estar seguros que no están involucrados en este ataque. Por eso es imprescindible que la comunicación esté prediseñada y se haga de forma periódica".

Para Jorge Freiburghaus, la estrategia de comunicación debe estar orientada a la transparencia, "que la gente entienda lo que está ocurriendo, pero sobre todo que la empresa lo está atendiendo con diligencia. Riesgo cero no existe, pero la gestión adecuada de la comunicación ante cada audiencia impactada hará la diferencia".

DEMANDA POR MÁS EDUCACIÓN AL USUARIO

El 81% de la conversación local es neutra, impulsada por los medios de comunicación con contenidos en materia de prevención, entendimiento de los ciberriesgos y destacando inversiones e innovaciones. Mientras que el 3% es de tono positivo, también promovido por medios y algunas empresas y organizaciones sobre eventos educativos y concientización.

- **Consejos y recomendaciones sobre ciberseguridad:** titulares ofrecen consejos y recomendaciones sobre cómo protegerse frente a las ciberamenazas, como la necesidad de tener precaución al navegar por Internet, orientaciones para los padres sobre la protección de los menores en la red y consejos para instalar servicios de vigilancia seguros.

- **Eventos y conferencias sobre ciberseguridad:** múltiples titulares mencionan conferencias y eventos centrados en la ciberseguridad, destacando su importancia y la participación de expertos en la materia.

- **Inversión e innovación en ciberseguridad:** varios titulares hablan de inversiones en infraestructuras e iniciativas de ciberseguridad, incluyendo el lanzamiento del futuro Hub Digital de Innovación y Tecnología Gubernamental de Panamá, que incluirá el Centro de Gobernanza de la Transformación Digital; Centro de Datos y Observatorio de Gobierno Digital; Laboratorio de Innovación Digital y el Centro Nacional de Ciberseguridad.

- **Contenidos de concientización:** notas por parte de medios especializados con titulares que buscan generar tranquilidad visibilizando lo sencillo que es proteger tus datos frente a riesgos.

Está clara la demanda y necesidad de mayor información, que permita a los clientes y usuarios detectar los ciberriesgos y evitar ser víctimas de los ciberdelincuentes cada vez más sofisticados. A mayor digitalización de procesos, ventas e interacciones en redes sociales, app y plataformas, aumenta el riesgo para los usuarios y las organizaciones.

En este sentido, Jorge Freiburghaus, resalta la importancia del papel de los usuarios/colaboradores como el elemento más importante en materia de prevención. “El factor humano es el elemento al que más atención hay que prestarle. El error humano es la falla mayor, porque aunque hay amenazas muy complejas, la mayoría entran por un descuido de las personas”.

LLYC

CLAVES PARA LA GESTIÓN DE LOS CIBERRIESGOS MÁS ALLÁ DE LA INVERSIÓN EN SISTEMAS INFORMÁTICOS

CLAVES PARA LA GESTIÓN DE LOS CIBERRIESGOS MÁS ALLÁ DE LA INVERSIÓN EN SISTEMAS INFORMÁTICOS

AVANZAR HACIA LA ANTIFRAGILIDAD: la digitalización que se institucionalizó con fuerza a partir de la Covid-19 exponenció los ciberriesgos. Eso provocó que muchas empresas trabajaran estrategias de resiliencia ante estos nuevos riesgos.

Sin embargo, en una era de permacrisis, el sector privado debe moverse hacia estrategias de antifragilidad, porque ya no se trata de sobrevivir, sino de permanecer y fortalecerse ante las adversidades. Cuando todos estamos expuestos a un ciberataque, la diferencia está en cómo se gestiona y cómo se comunica para que impacte lo menos posible la reputación corporativa.

En este sentido, las empresas deben sumar a sus directivos de comunicación y relaciones institucionales a la estrategia de respuesta ante un incidente de ciberseguridad, que debe estar diseñada y practicada con antelación, a través de simulacros integrales (equipo técnico + equipo de comunicación corporativa).

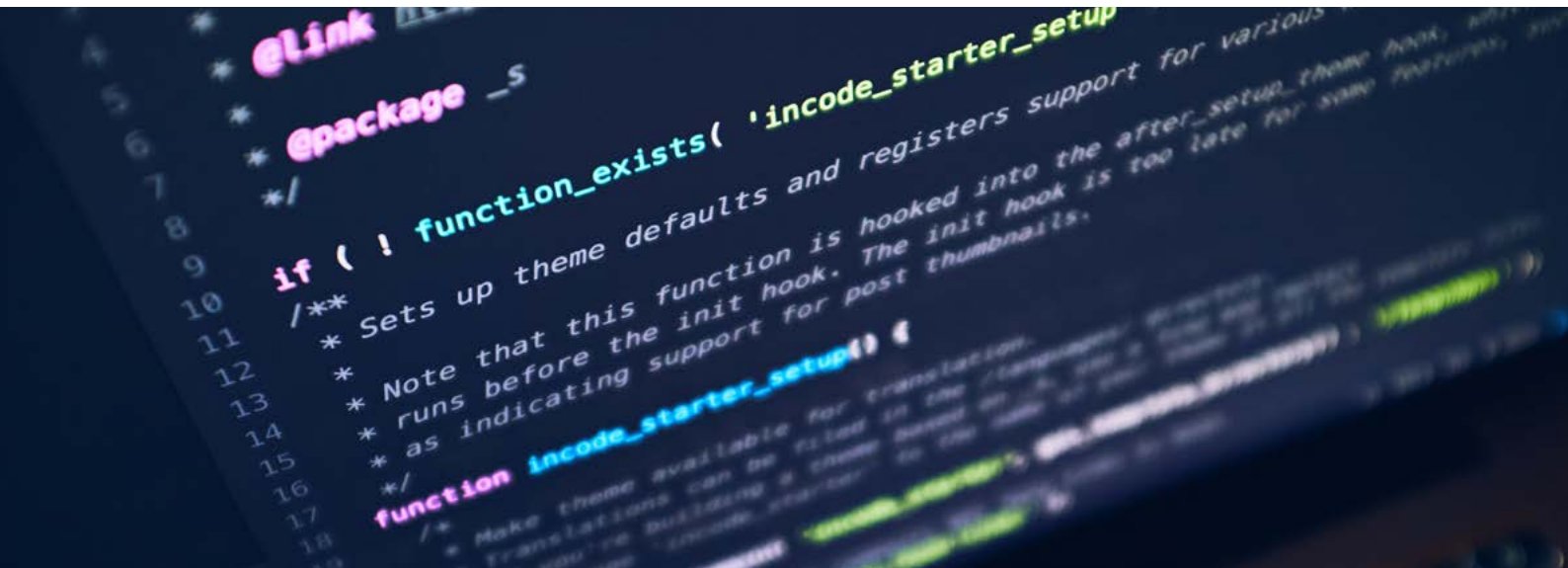
Además, intercalando la *big data* y el conocimiento de los expertos se pueden construir modelos prospectivos que orienten el abordaje más holístico ante las ciberamenazas.

HIPERTRANSPARENCIA: los resultados del análisis de la conversación digital comprueban que los clientes/usuarios no quieren que las empresas "oculten sus ciberamenazas bajo la alfombra". Por el contrario, demandan una comunicación transparente y oportuna. Una demanda que en algunos países, además, va acompañada de nuevas leyes sobre protección de datos que obligan a las empresas a comunicar sus incidentes en materia de ciberseguridad.

La transparencia en lo que ha ocurrido y cómo se protege a los usuarios cobra más valor ante la ciberdelincuencia, porque se pone en riesgo el mayor valor que tienen las personas: sus datos. Y, al no gestionar bien esa expectativa de confianza entre usuarios y compañía, la reputación de las organizaciones queda impactada, ya no por el ataque, sino por la mala gestión de la comunicación del hecho.

Proteger los activos de la empresa frente al ataque, incluye proteger la reputación. El trabajo de los equipos técnicos, líderes de la organización y comunicación debe ser el resultado de una estrategia anticipada donde están claramente definidos los roles, responsabilidad, mensajes y vías de comunicación.

El objetivo principal es que cada audiencia impactada sea atendida de manera cercana, en su tono, con foco hacia la información del qué sucedió y qué estamos haciendo, para que el pánico, inevitable en estas situaciones, no sea el protagonista de la comunicación.



LLYC

COMPLIANCE CONECTADO: el riesgo reputacional y el riesgo cibernético son en sí riesgos de cumplimiento. En ambos casos las decisiones que tomen las personas en cuanto a medidas de prevención, priorización del riesgo y definición de presupuestos serán clave en el abordaje que haga la compañía cuando enfrente una ciberataque, de cualquier tipo o tamaño.

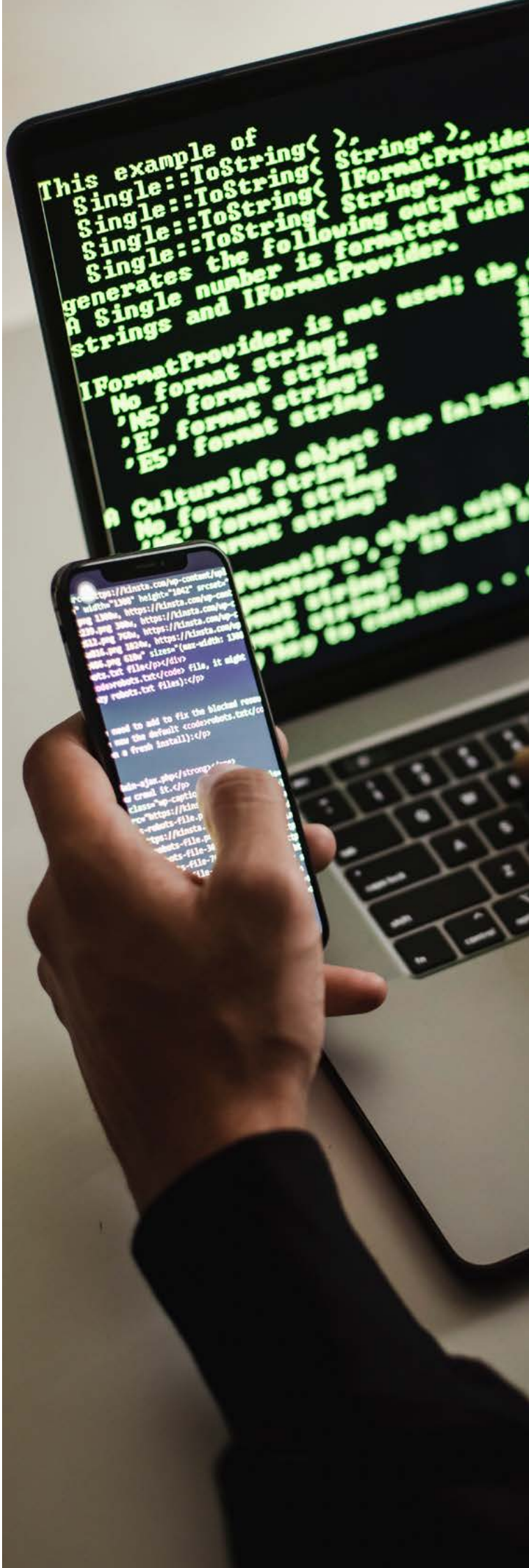
Mitigar el riesgo ciber y su impacto en la reputación empresarial no es solo una tarea hacia fuera, sino también hacia adentro. Recordemos que los colaboradores son el *endpoint* que supone como riesgo su puesto de trabajo y todas sus extensiones móviles.

Como decía el padre del management moderno, Peter Drucker, "la cultura se come la estrategia en el desayuno". Por eso hay que tener un programa que conecte esta política de cumplimiento a la cultura de la organización, que es la mejor vía para garantizar su verdadera implementación. En este punto, la gamificación y la creatividad en la comunicación con los colaboradores es el factor diferencial entre seguir mandando memorandos de "reglas y deberes" vs un cumplimiento conectado a la cultura de la organización.

RESPONSABILIDAD DE TODOS: en materia de ciberseguridad hay dos hechos irrefutables: las personas son la primera barrera de protección y no hay riesgo cero.

Desde el sector público y privado, la comunicación creativa y diferencial para generar mayor sensibilidad y educación sobre el papel de cada uno frente a las ciberamenazas debe ser una prioridad. Porque todo indica que los riesgos seguirán creciendo y las vías de ataque serán más sofisticadas, e incluirán el robo de datos biométricos a través de los populares filtros.

Solo en una estrategia de anticipación a este tipo de riesgos y situaciones tiene la capacidad de convocar a todos los involucrados y a crear un cerco de protección en el que todos entiendan sus derechos y deberes.



AUTORES

Margorieth Tejeira Directora Senior de Riesgos y Corporativo

Con más de 20 años de experiencia como periodista y asesora de comunicación, especializada en el área de riesgos, litigios y comunicación corporativa. Ha gestionado cuentas del sector público, privado y ONGs. Laboró en medios, entidades y banca. Presidenta de Dircom Panamá.

Encargada del diseño de estrategias, mapas de riesgos, simulacro de crisis, gestión de medios y relacionamiento.

mtejeira@llyc.global

Catalina Barragán Directora Comunicación Corporativa

Es profesional en mercadeo y publicidad con 20 años de experiencia en el área de comunicaciones estratégicas y reputación corporativa, relaciones públicas, asuntos institucionales y comunicaciones de marketing. Ha liderado proyectos para diversos sectores, entre ellos de consumo masivo, hospitalidad (restaurantes), educación, salud, industrial, como Natura Cósmeticos, Avon, Coca-Cola, Mercedes Benz, Alpina, Grupo Takami, Tetra Pak, entre otros, generando valor estratégico y liderando los planes de ejecución.

Catalina tiene un amplio conocimiento en manejo de crisis para el sector público/privado y cuenta con experiencia en la capacitación de voceros para contacto con medios y presentaciones efectivas.

catalina.barragan@llyc.global

Renata Sánchez Directora de Asuntos Corporativos

Con más de 15 años de experiencia como periodista y consultora de comunicación, Renata ha trabajado con industrias altamente reguladas como la energética, alimentos y bebidas, plásticos, automotriz de lujo, del juguete, así como con ONG de protección al medio ambiente donde ha planeado y ejecutado estrategias de comunicación, anticipación y gestión de riesgos, así como manejo de crisis.

vsanchez@llyc.global

AUTORES

Ernesto González Director de *Deep Digital Business* Región Norte

Es especialista en el mundo digital. Fue Director General Operativo y Director de Inteligencia en la agencia de publicidad BESO, ahora BESO by LLYC. Ha enfocado sus esfuerzos en diseñar soluciones únicas y efectivas para ayudar a las grandes empresas a trabajar de manera más inteligente y efectiva a través del uso de data y nuevas tecnologías. Ernesto ocupó también el rol de Director Senior de *Deep Learning* Región Norte y Estados Unidos de LLYC.

egonzalezs@llyc.global

César Vázquez Mánica Director *Deep Learning* Región Norte

Es un apasionado de la tecnología y la innovación, especialista en transformación digital con más de 12 años de experiencia desarrollando estrategias de negocio y comunicación, diseñando procesos de trabajo y brindando consultoría en *big data* a diversos tipos de clientes desde **startups** hasta marcas trasnacionales. Hasta diciembre de 2021, Cesar se desempeñaba como Director Regional *Business Intelligence* en BESO by LLYC.

cesar.manica@llyc.global

LLYC

Dirección Corporativa

José Antonio Llorente
Socio Fundador y Presidente
jallorente@llyc.global

Luis Miguel Peña
Socio y Chief Talent Officer
lmpena@llyc.global

Marta Guisasola
Socia y Chief Financial Officer
mguisasola@llyc.global

Albert Medrán
Director Corporativo
amedran@llyc.global

Juan Pablo Ocaña
Director Senior de Legal & Compliance
jpocana@llyc.global

José Manuel Casillas
Director Senior de IT Global
jmcasillas@ llyc.global

Europa

Luisa García
Socia y CEO Europa
lgarcia@llyc.global

Arturo Pinedo
Socio y Chief Client Officer Europa
apinedo@llyc.global

Rafa Antón
Chief Creative Officer Europa
Cofundador y Director General
Creativo de China parte de LLYC
rafa.anton@llyc.global
CHINA parte de LLYC

Madrid

Jorge López Zafra
Socio y Director General
jlopez@llyc.global

Joan Navarro
Socio y Vicepresidente
Asuntos Públicos
jnavarro@llyc.global

Amalio Moratalla
Socio y Director Senior Deporte
y Estrategia de Negocio
amoratalla@llyc.global

Iván Pino
Socio y Director Senior Crisis y Riesgos
ipino@llyc.global

Marta Aguirrezabal
Socia y Directora Ejecutiva
CHINA parte de LLYC
marta.aguirrezabal@llyc.global

Pedro Calderón
Socio Fundador y Director Ejecutivo
CHINA parte de LLYC
pedro.calderon@llyc.global

Barcelona

María Cura
Socia y Directora General
mcura@llyc.global

Oscar Iniesta
Socio y Director Senior
oiniesta@llyc.global

Gina Rosell
Socia y Directora Senior Health
grosell@ llyc.global

Lisboa

Tiago Vidal
Socio y Director General
tvidal@llyc.global

Américas

Alejandro Romero
Socio y CEO Américas
aromero@llyc.global

Juan Carlos Gozzer
Socio y Chief Operating Officer
América Latina
jcgozzer@llyc.global

Javier Rosado
Socio y Chief Client Officer Américas
jrosado@llyc.global

Javier Marín
Director Senior Healthcare Américas
jmarin@llyc.global

José Beker
Chief Creative Officer Américas
Cofundador y CEO de Beso by LLYC
BESO by LLYC
jose.beker@llyc.global

Antonieta Mendoza de López
Vicepresidenta de Advocacy para
América Latina
amendoza@llyc.global

Estados Unidos

Juan Felipe Muñoz
CEO Estados Unidos
fmunoz@llyc.global

Darío Álvarez
Director Ejecutivo LLYC Miami
dalvarez@llyc.global

Región Norte

David González Natal
Socio y Director General Regional
dgonzalezn@llyc.global

Mauricio Carrandi
Director General LLYC México
mcarrandi@llyc.global

Manuel Domínguez
Director General LLYC Panamá
mdominguez@llyc.global

Iban Campo
Director General LLYC República
Dominicana
icampo@llyc.global

Región Andina

María Esteve
Socia y Directora General Regional
mesteve@llyc.global

Marcela Arango
Directora General LLYC Colombia
marango@llyc.global

Gonzalo Carranza
Socio y Director General LLYC Perú
gcarranza@llyc.global

Carlos Llanos
Socio y Director General LLYC Ecuador
cllanos@llyc.global

Región Sur

Juan Carlos Gozzer
Socio y Director General Regional
jcgozzer@llyc.global

Maria Eugenia Vargas
Directora General LLYC Argentina
mevargas@llyc.global

Thyago Mathias
Director General LLYC Brasil
tmathias@llyc.global

Deep Digital Business

Adolfo Corujo
Socio y CEO de Deep Digital Business
acorujo@llyc.global

Jesús Moradillo
Director General Deep Digital
Business Europa
CEO y fundador de Apache Digital
APACHE parte de LLYC
jesus.moradillo@llyc.global

Federico Isuani
Director General de Deep Digital
Business Región Norte y USA
Cofundador y CEO de Beso by LLYC
BESO by LLYC
federico.isuani@llyc.global

Daniel Fernández Trejo
Director Senior de Deep Digital
Business y CTO global
dfernandez@llyc.global

Anahí Raimondi
Directora de Operaciones Deep
Digital Business
araimondi@llyc.global

David Martín
Director General de Deep Digital
Business Región Andina
david.martin@llyc.global

Diego Olavarría
Director Senior Deep Digital
Business Región Sur
dolavarria@llyc.global

Luis Manuel Núñez
Director Sénior Global de Tecnología
y Estrategia Digital
luisma.nunez@llyc.global

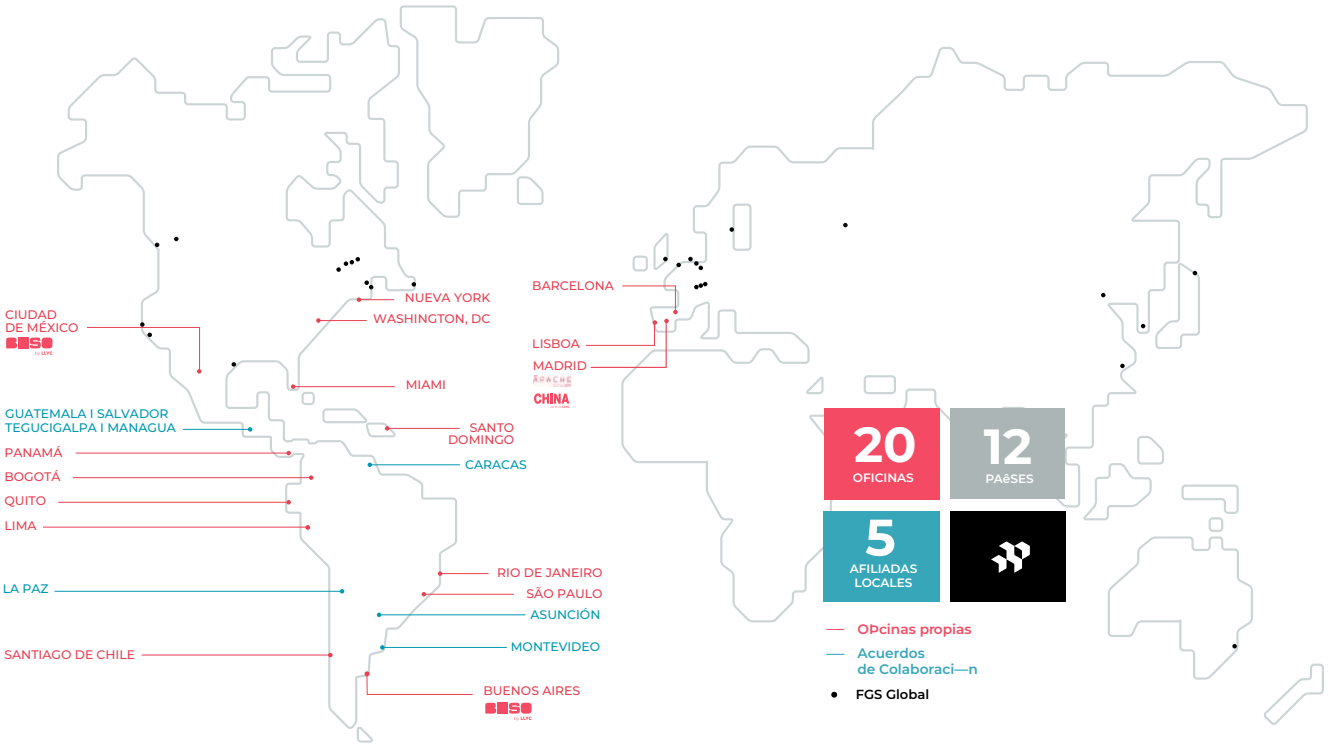
Carmen Gardier
Directora Senior Influencia Digital
Américas
cgardier@llyc.global

Alejandro Dominguez
Director Influencia Digital Europa
adominguez@llyc.global

Fernanda Hill
Directora General Beso by LLYC
BESO by LLYC
fernanda.hill@llyc.global

LLYC

Oficinas



LLYC

Madrid
Lagasca, 88 - planta 3
28001 Madrid, España
Tel. +34 91 563 77 22

Barcelona
Muntaner, 240-242, 1º-1ª
08021 Barcelona, España
Tel. +34 93 217 22 17

Lisboa
Avenida da Liberdade nº225, 5º Esq.
1250-142 Lisboa, Portugal
Tel. + 351 21 923 97 00

Miami
600 Brickell Avenue, Suite 2125
Miami, FL 33131
United States
Tel. +1 786 590 1000

Nueva York
3 Columbus Circle, 9th Floor
New York, NY 10019
United States
Tel. +1 646 805 2000

Washington
1025 F st NW 9th Floor
Washington DC 20004
United States
Tel. +1 202 295 0178

Ciudad de México
Av. Paseo de la Reforma 412
Piso 14. Colonia Juárez
Alcaldía Cuauhtémoc
CP 06600, Ciudad de México
Tel. +52 55 5257 1084

Panamá
Sortis Business Tower
Piso 9, Calle 57
Obarrio - Panamá
Tel. +507 206 5200

Santo Domingo
Av. Abraham Lincoln 1069
Torre Ejecutiva Sonora, planta 7
Suite 702, República Dominicana
Tel. +1 809 6161975

San José
Del Banco General 350 metros oeste
Trejos Montealegre, Escazú
San José, Costa Rica
Tel. +506 228 93240

Bogotá
Av. Calle 82 # 9-65 Piso 4
Bogotá D.C. – Colombia
Tel. +57 1 7438000

Lima
Av. Andrés Reyes 420, piso 7
San Isidro, Perú
Tel. +51 1 2229491

Quito
Avda. 12 de Octubre N24-528 y
Cordero - Edificio World Trade
Center – Torre B - piso 11
Ecuador
Tel. +593 2 2565820

Sao Paulo
Rua Oscar Freire, 379, Cj 111
Cerqueira César SP - 01426-001
Brasil
Tel. +55 11 3060 3390

Rio de Janeiro
Rua Almirante Barroso, 81
34º andar, CEP 20031-916
Rio de Janeiro, Brasil
Tel. +55 21 3797 6400

Buenos Aires
Av. Corrientes 222, piso 8
C1043AAP, Argentina
Tel. +54 11 5556 0700

Santiago de Chile
Avda. Pdte. Kennedy 4.700,
Piso 5, Vitacura
Santiago
Tel. +56 22 207 32 00
Tel. +562 2 245 0924

ÁPACHE parte de LLYC

Arturo Soria 97A, Planta 1
28027, Madrid, España
Tel. +34 911 37 57 92

CHINA parte de LLYC

Velázquez, 94
28006, Madrid, España
Tel. +34 913 506 508

BESO by LLYC

El Salvador 5635, Buenos Aires
CP. 1414 BQE, Argentina

Av. Santa Fe 505, Piso 15,
Lomas de Santa Fe,
CDMX 01219, México
Tel. +52 55 4000 8100

LLORENTE Y CUENCA