



2020 es el año que aceleró la economía digital en América Latina y también el período en el que las amenazas digitales se han vuelto aún más enfocadas y efectivas. El Informe de amenazas de SonicWall de los primeros seis meses de este año muestra, por ejemplo, que Brasil ha sufrido más de 69 millones de ataques, ocupando el sexto lugar en el ranking mundial de países más afectados por ransomware.

Una situación similar ocurrió con México, blanco de 10 millones de ataques en el mismo período. Los expertos de Capture Labs de SonicWall también informan que el volumen de ataques de malware diseñados especialmente para dispositivos IoT ha aumentado en un 50%. El daño causado por este tipo de malware puede ser alto: solo en nuestra región, según Frost & Sullivan, deberíamos tener 50 mil millones de sensores IoT conectados para 2023.

Sin embargo, las ganancias aportadas por la expansión de la infraestructura digital latinoamericana tienen un lado oscuro: puede haber un desajuste entre la implementación de las nuevas redes y la solución a los desafíos de seguridad en estos entornos. Los múltiples ataques que hemos visto en nuestro mercado muestran el resultado de esta desconexión. Es fundamental entrar al 2021 con una nueva perspectiva: diseñar e implementar entornos digitales que ya nacen seguros, y que se sigan actualizando a lo largo de su ciclo de vida. La sostenibilidad de la economía digital en nuestra región depende de esto.

## **Vea a continuación los grandes ejes de la transformación digital en América Latina en 2021:**

La madurez digital será más importante que nunca - Vivir la transformación digital ya no será suficiente en 2021, será fundamental que las empresas busquen evolucionar en su madurez digital. Según el MIT Sloan Management Review, la madurez digital es el proceso mediante el cual la organización en su conjunto aprende a responder adecuadamente a las demandas de la economía digital.

Toda empresa que busca la madurez digital está, de hecho, luchando por diferenciarse en sus verticales a través de la innovación digital. Una encuesta realizada por el MIT en 2016 a



3700 CEOs de 131 países muestra que el 80% de las empresas más maduras destacan por ver y gestionar el riesgo, por su agilidad en los procesos y por la colaboración entre equipos heterogéneos.

Nada de esto será posible sin sumar, al paraguas de la madurez digital, acciones que aumenten la madurez de la ciberseguridad de esta organización. Esto implica rediseñar procesos.

Las leyes de privacidad de datos llegaron para quedarse - En todo el mundo, incluso en América Latina, las leyes de privacidad de datos han demostrado ser una respuesta poderosa y efectiva a la monetización de datos. La información sobre las personas es un tesoro codiciado por los delincuentes digitales, que venden bases de datos llenas de detalles sobre clientes, empleados y colaboradores en la Dark Web.

Leyes como la LGPD (Ley General de Protección de Datos) brasileña y otras legislaciones en diferentes etapas en países como Chile, Argentina, Colombia y México con la Ley Federal de Protección de Datos en Posesión de Particulares (LDPPP) castigan a las empresas que no protegen esta información y sufren ataques y filtraciones. Esta realidad está transformando el rostro del mercado.

La pandemia y las nuevas leyes cambiarán la lógica interna de las empresas - La suma de la pandemia con la implementación de las leyes de privacidad de datos está revolucionando los procesos internos de las empresas.

La adhesión a las mejores prácticas de seguridad de la información avanzará, en 2021, a las áreas de negocio de las empresas usuarias. CISO dedicará parte de su tiempo a comunicar conceptos críticos de seguridad a su organización.

La base de este posicionamiento es un Análisis de Riesgos muy bien hecho, capaz de señalar las vulnerabilidades de la empresa en todos los entornos digitales (on-premises, cloud, edge computing, teletrabajo, IoT, IIoT, etc.) y construir casos de negocio que muestren el impacto de este riesgo en el negocio.



Cómputo en la nube seguirá creciendo: La adhesión de las empresas latinoamericanas a la nube es algo tangible: solo en México se trata de un mercado que dejará una derrama económica de 1,430 millones de dólares en México en 2020, 31% por arriba de 2019, y de 1,877 millones en 2021, lo que supone un crecimiento también de 31%, según datos de Statista.

En toda la región, millones de empresas han migrado sus negocios a la nube, con una fuerte presencia en la red. Esto significa una mayor demanda de soluciones como la plataforma CAS, que protege aplicaciones web como Office365 o el entorno Salesforce.

La criticidad de la aplicación que se ejecuta en la nube es alta, y es fundamental que, en 2021, esta plataforma tenga su integridad y disponibilidad garantizadas. Paralelamente, seguirá siendo un desafío para las empresas de usuarios más grandes, con entornos de múltiples nubes, resolver los detalles técnicos, incluida la seguridad, y la facturación de cada una de las grandes nubes (Azure, AWS, Google).

El Edge de la red estará en el centro de atención: El Edge de la red gana cada vez más complejidad y criticidad, lo que también aumenta la demanda de soluciones SASE (Secure Access Service Edge). Está claro que la idea tradicional de seguridad basada en el perímetro de la red está dejando de existir. SASE surge debido a esta realidad, llevando la seguridad a los bordes de la red.

En 2021, será fundamental agregar soluciones a la red que controlen y protejan el acceso remoto, utilizando tecnología de autenticación y funciones de confianza cero para garantizar tanto la conexión remota como la seguridad de ese acceso.

Los MSSP se convertirán en socios esenciales para los clientes finales: En 2021, los presupuestos limitados, la dificultad para encontrar profesionales capacitados y especialmente en seguridad digital, así como la velocidad de los negocios aumentarán la contratación de empresas usuarias por parte de los MSSP (Managed Security Service Providers, por sus siglas en inglés).



Este perfil de socio está renovando continuamente sus centros de datos y SOC (Security Operation Center), ya sea en las instalaciones o en la nube. El objetivo es contar con la seguridad digital más avanzada, una oferta que enfrenta las amenazas actuales y futuras.

En 2021 aumentará la demanda de soluciones de seguridad llave en mano, como resultado de proyectos a medida para cada empresa usuaria. Este tipo de solución tiene una salida al mercado acelerada y ayuda a MSSP a anticipar y resolver las nuevas demandas de seguridad de los clientes finales.

2020 trajo lecciones para todos nosotros. La economía latinoamericana sufrió los giros y vueltas de la pandemia, pero también saltó a una nueva etapa. Es fundamental que los avances logrados en 2020 se consoliden, resguarden de ataques y sirvan de base a los cambios que vendrán. La prosperidad digital de nuestra región depende de ello.

*Por Arley Brogiato, Director de Ventas de SonicWall para América Latina y el Caribe*