IDC ANALYZE THE FUTURE

I D C V E N D O R S P O T L I G H T

Ciberseguridad en los ecosistemas cloud y los desafíos alrededor de movilidad

Mayo, 2018

Carlo Dávila

Patrocinado por: Kaspersky Lab

Las tendencias en adopción de cloud en América Latina han creado entornos de tecnología de información (TI) donde datos y cargas de trabajo, ya sea on-premises o en cloud pública, privada o híbrida, son accesados desde diversos equipos y dispositivos dentro y fuera de la organización, por lo que la ciberseguridad debe ser replanteada desde el cloud y para el cloud, y de acuerdo con el perfil de riesgo de la empresa.

En el presente documento describiremos cómo la evolución de cloud y sus diferentes ecosistemas (EPC, PCS, DHPC, ODHPC, ver apartado II Definiciones) han incrementado la complejidad y la superficie de ataque en las áreas de TI de las compañías de América Latina. Del mismo modo, analizaremos la adopción de movilidad en las organizaciones de la región y el estado actual de inversión para estos ambientes. Adicionalmente, revisaremos la oferta de soluciones de Kaspersky Lab para enfrentar amenazas cada vez más sofisticadas y automatizadas, su relación con la evolución de cloud y movilidad y finalmente cómo se debe cambiar el enfoque de inversión de las organizaciones en ciberseguridad.

I. INTRODUCCIÓN

De acuerdo con el estudio IDC FutureScape: Worldwide IT Industry 2018 Predictions, LA Implications, al 2021 se espera que la inversión en cloud incluyendo servicios, hardware y software, alcance la cifra de 11,000 millones de dólares, impulsando ambientes heterogéneos, 80% de ellos en ambientes multi-cloud, incluso de diferentes proveedores.

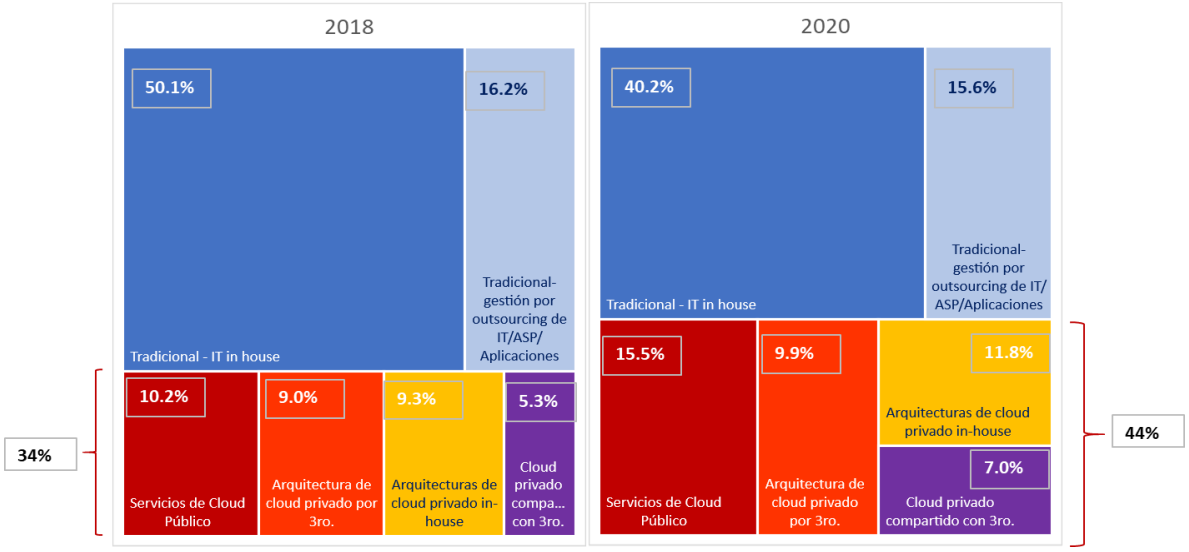
Como puede verse en la Figura 1, el reporte de IDC IT Investment Trends 2017Q4 indica que, para el año 2020, 44% de la infraestructura de TI en las empresas será gestionada en cloud.

Más aún, la infraestructura (IaaS) y las aplicaciones (SaaS) en cloud se hallan dentro de las prioridades estratégicas en TI durante 2018 para más del 23% de las organizaciones de América Latina[1], con el fin de hacer más eficiente el uso de los recursos e infraestructura del negocio y agilizar el uso de las aplicaciones. De la mano con los servicios en cloud están las iniciativas de movilidad, las mismas que agregan mayor dinamismo a la utilización de aplicaciones que ya han sido migradas a ambientes de cloud con la finalidad de incrementar los niveles de eficiencia del negocio. Dichas iniciativas se hallan dentro de las prioridades para 31% de las organizaciones en la región, y es uno de los elementos que han incrementado el riesgo en la seguridad con la explosión de dispositivos y ordenadores como puntos de acceso, dentro y fuera de la organización.

[1] IDC IT Investment Trends 2017 Q4- con base en entrevistas a organizaciones de más de 100 empleados en industrias de servicios, recursos naturales, gobierno, comercio, manufactura y finanzas.

FIGURA 1

Ambientes Multi-cloud en América Latina



Fuente: IDC Latin America IT Investment Trends 2017Q4

A pesar de que la ciberseguridad es la principal preocupación de los CISOs ya que 45% de las organizaciones de la región la consideran como la principal iniciativa de inversión para 2018, el análisis de la asignación del presupuesto de TI para este concepto no está alineado al crecimiento de cloud y la movilidad empresarial. Actualmente, las compañías destinan menos del 10% del presupuesto total de TI a soluciones de seguridad, de acuerdo con el estudio IDC Latin America Cybersecurity Report 2017. El mismo reporte indica que tres de cada cinco organizaciones consideran que habrá una reducción de15% del presupuesto en ciberseguridad.

IDC, frente a este panorama de crecimiento de cloud y movilidad, y la restricción en recursos de TI, considera que las estrategias de ciberseguridad deben contemplar la protección desde:

- Los principales puntos de entrada de potenciales ataques, ordenadores y dispositivos móviles de los usuarios
- Las cargas de trabajo en ambientes heterogéneos
- El centro de datos propio o de un proveedor de servicio

Para ello, se debe conocer el perfil de riesgo corporativo y los modelos operativos y de información de la compañía, apoyándose en soluciones y herramientas avanzadas y automatizadas, agregando también capas adicionales de servicios de seguridad.

II. DEFINICIONES

Las siguientes definiciones de ecosistemas de cloud son pertinentes para el desarrollo del presente documento:

- Ecosistemas de servicios de cloud
  - Public Cloud Services, o PCS- Servicios de cloud público. Son servicios bajo demanda y consumidos en un modelo de suscripción que un proveedor distribuye a través de Internet a una empresa. Puede ser:

- Infrastructure as a Service, o IaaS- Infraestructura como Servicio, servidores o máquinas virtuales y almacenamiento desde un proveedor a quien se paga por el uso de los servicios.
- Plataform as a Service, o PaaS- Plataforma como Servicio, un ambiente bajo demanda para desarrollo, prueba, administración y entrega de aplicaciones. Incluye base de datos y herramientas de integración.
- Software as a Services, o SaaS- Software como Servicio, ofrece aplicaciones orientadas tanto al usuario como a las organizaciones tales como aplicaciones de industria, herramientas de colaboración y aplicaciones de seguridad, entre otras.

- Cloud privado: Son servicios provistos por la propia empresa o un tercero, para la operación central y oficinas de operación extendida, con mayor restricción de acceso, un mayor nivel de dedicación de recursos con contratos a largo plazo. El cloud privado puede clasificarse como sigue:
  - Enterprise Private Cloud Services (EPC)- Servicios de cloud privado empresarial con recursos exclusivos para una misma compañía. La infraestructura, los servicios y la administración son de propiedad y responsabilidad de la empresa, y que residen en sus premisas.
  - Dedicated Hosted Private Cloud Services (DHPC)- Servicios de cloud privado hosteados en las instalaciones de un proveedor de servicios, cuyo servicio está definido bajo un contrato por un período definido de tiempo. Este modelo es esencialmente una versión en la nube de las ofertas tradicionales de hosting gestionado.
  - On-Demand Hosted Private Cloud Services (ODHPC)-Servicios de cloud privado hosteados en las instalaciones de un proveedor de servicios que provisiona recursos dinámicamente para el uso dedicado de una organización, desde un grupo compartido.

- Cloud Híbrido- Arquitectura de TI empresarial que unifica la combinación de recursos de computación heterogéneos, infraestructura de nube pública y privada (IaaS), middleware (PaaS) y recursos de base de datos/aplicaciones (SaaS), así como activos de TI no físicos, en una configuración automatizada de autoservicio basada en el consumo y políticas de uso.

FIGURA 2

Taxonomía de Cloud

Fuente: IDC Taxonomy, 2015

- 3ª Plataforma y aceleradores de innovación- existen cuatro pilares que conforman la 3ª Plataforma de tecnología actual de las empresas movilidad, cloud, social business y big data/analítica y son la base de la transformación digital de los negocios. Los aceleradores de innovación son tecnologías disruptivas como seguridad de siguiente generación (Next Generation Security), realidad virtual, Internet de las Cosas (IoT), sistemas cognitivos, robótica e impresión 3D. Figura 3.

- Transformación Digital- incluye procesos de transformación en cinco dimensiones:
  - Liderazgo para desarrollar una visión para la transformación digital del negocio.
  - Omni-presencia que le permita atraer y aumentar la lealtad del cliente.
  - Información para obtener una ventaja competitiva.
  - Modelo operativo para realizar operaciones del negocio más eficaces y con respuestas.
  - Espacios de trabajo, transformando la forma en que se accede, conecta o impulsa el talento en una economía digitalizada.

FIGURA 3

- **3ª Plataforma, base de la Transformación Digital**

III. TENDENCIAS CON IMPACTO EN LA CIBERSEGURIDAD DEL NEGOCIO

En el camino para diseñar una plataforma de ciberseguridad alineada a la estrategia de movilidad e implementación de cloud, se debe considerar los principales puntos de acceso, desde el escritorio de los usuarios hasta los dispositivos móviles, endpoints y teléfonos inteligentes, así como también el perfil de riesgo en función de la industria donde se desarrolla la empresa.

La necesidad de proteger los principales puntos de acceso para los cibercriminales

Hoy día, de acuerdo con IDC Latin America Cybersecurity Report 2017, Phishing, Malware & Malvertising y los ataques a las credenciales son los ataques más frecuentes en América, llegando a presentarse cinco a seis incidentes al año, 76% a 84% son de origen externo, en empresas de cualquier tamaño o industria. Más aún es el hecho que las amenazas se han vuelto más sofisticadas y con algunos procesos automatizados que requieren de menos acción del usuario infectado para propagarse a lo largo de una empresa. Esto se debe a que en la misma medida que las empresas han

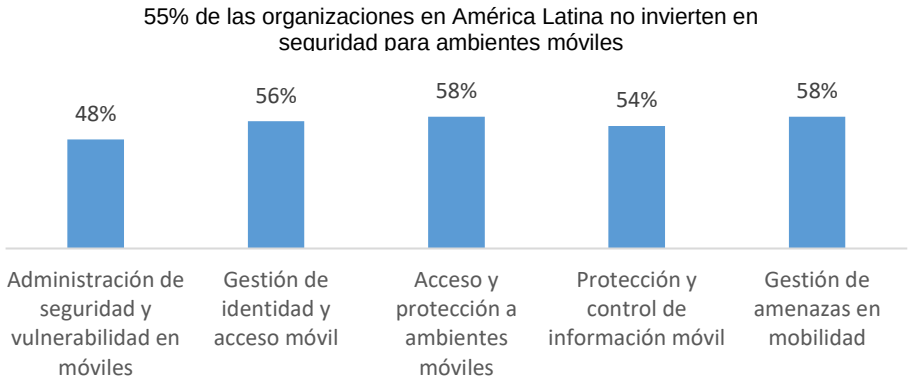
ido digitalizándose, los ciberdelincuentes aprovechan los mercados negros para hacerse de herramientas automatizadas y compartir información privilegiada que les permite filtrarse en los ambientes de la organización más rápidamente a través de los empleados, quienes inadvertidamente pueden haber recibido algún correo electrónico en su ordenador de escritorio o dispositivo móvil (endpoints) con archivos maliciosos. Una acción tan simple como dar click en un archivo o enlace sospechoso puede resultar en la propagación de virus o el secuestro de la infraestructura tecnológica y datos de la empresa. Cabe resaltar que 31% de las organizaciones no ha implementado programas internos de comunicación sobre potenciales eventos de seguridad, y 27% de las compañías sigue un protocolo de comunicación restringida a niveles gerenciales. Este enfoque impacta negativamente en la primera línea de defensa de una compañía: los empleados, ya que Latinoamérica no es una región que esté invirtiendo activamente en servicios de seguridad orientados a la concientización en los riesgos y ataques al negocio mismo.

Los retos de la seguridad en entornos móviles

De acuerdo con el estudio IDC IT Investment Trends, publicado recientemente; actualmente, 43% de los empleados de empresas medianas en América Latina trabaja fuera de escritorio y se apoya en dispositivos móviles para trabajar. De las empresas medianas y grandes, 80% permiten a los empleados conectarse desde dispositivos móviles (propios o financiados por la organización) a plataformas y aplicativos del negocio. Cuando hablamos de movilidad, nos referimos a la posibilidad de acceso a la red y los servicios de la infraestructura tecnológica de la empresa desde una laptop, tablet, teléfonos inteligentes o celulares, ya sea de uso corporativo o personal. Lo cual deja claro el desafío de gestionar el acceso y la seguridad de múltiples dispositivos que pueden ser usados por empleados, socios de negocio y clientes que también interactúan con datos e información de la empresa. Derivado de esta situación, la mayoría de quienes están a cargo de la seguridad de TI (Chief Information Security Officer, CISOs) muestran su preocupación cuando la movilidad se halla dentro de las iniciativas de mayor prioridad para las empresas. Adicionalmente, y de acuerdo con el estudio IDC Latin America Cybersecurity Report 2017, 85% de los CISOs consideran que las Laptops y desktops con sistemas operativos Windows son los endpoints más vulnerables; le siguen los teléfonos inteligentes (43%) y los tablets (23%) con sistema operativo Android. A pesar de estar conscientes de los riesgos en seguridad de la movilidad, 55% de las compañías en la región no están contemplando inversiones específicas de seguridad para ambientes móviles- Ver Figura 4.

FIGURA 4

¿Cuál es el estado de inversión en seguridad para ambientes móviles?



Fuente: IDC Latin America Cybersecurity Report, 2017

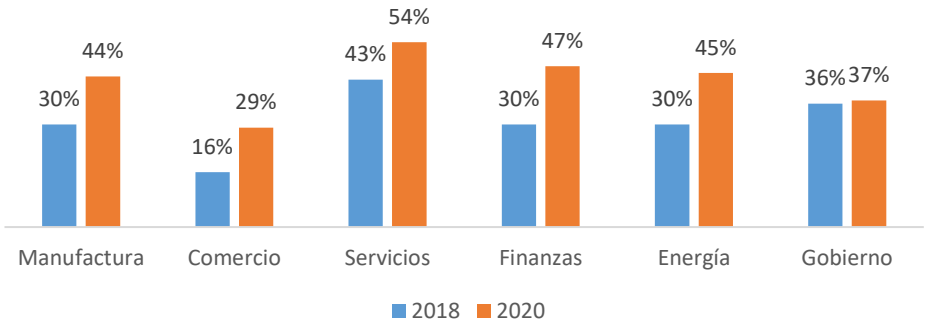
La adopción de cloud y ciberseguridad en las industrias de América Latina

A pesar de que el año 2018 es un año de elecciones o cambios de administración federal, persiste un ambiente de optimismo en inversión de TI en América Latina. Más del 36% de los países de la región consideran que la inversión será mayor al 2020. De manera particular, como puede verse en la Figura 5, las industrias que más invierten actualmente en cloud son Servicios y Gobierno. Sin embargo, de cara al futuro, los sectores Finanzas, Manufactura y Energía son los que tendrán mayor dinamismo en la inversión en cloud al 2020 hasta en 17 puntos porcentuales. Las cifras mostradas incluyen ambientes multi-cloud:

- Servicios de Cloud Público
- Arquitecturas de cloud privado administrado in-house
- Arquitecturas de cloud privado gestionado por un tercero
- Servicios de cloud privado compartido con terceros

FIGURA 5

Presupuesto de Cloud del Total Anual de TI por Industria

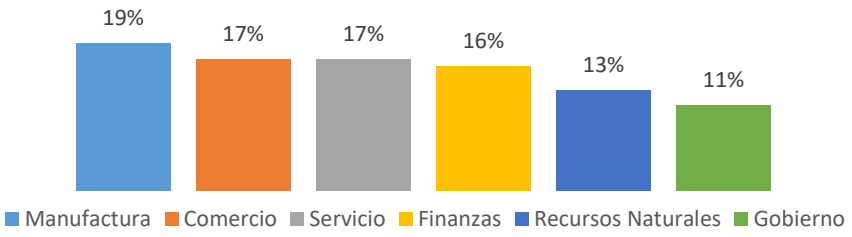


Fuente: IDC IT Investment Trends 2017Q4

Desde la perspectiva de seguridad, nuevamente refiriéndonos al estudio de IDC Latin America Cybersecurity Report 2017, las empresas que asignan un mayor porcentaje del presupuesto total de TI a la ciberseguridad son Manufactura (19%), Comercio (17%), Servicios (17%) y Finanzas (16%)- Figura 6.

FIGURA 6

¿Qué porcentaje del presupuesto de TI se asigna a soluciones de ciberseguridad?



Fuente: IDC Latin America Cybersecurity Report, 2017

Es importante resaltar que el sector financiero es el que más invierte en seguridad en endpoints y analítica de seguridad, más del doble que cualquier otro, siendo una de las industrias con mayores requerimientos y regulaciones en términos de seguridad. El contraste en inversión es el sector de Gobierno, con 11% de gasto en seguridad sobre el total de presupuesto de TI. Los ataques que más preocupan a este sector, al igual que Finanzas, son Phishing y Malware.

Para Manufactura, los ataques más frecuentes son Phishing, Malware y Malvertising, y secuestro de datos (Ransonware) en el orden correspondiente. Uno de los desafíos para esta industria es la adopción de tecnologías disruptivas, como el Internet de las Cosas; y, por otro lado, los riesgos específicos de industria como las amenazas a los sistemas SCADA.

Como puede entenderse a partir de los párrafos anteriores, cada industria tendrá diferentes ritmos de adopción de cloud y movilidad, así como desafíos diferentes sobre seguridad empresarial. Por lo que debe implementarse un análisis del ecosistema total de TI que permita definir una estrategia de ciberseguridad acorde al perfil de riesgo de la empresa y sus modelos de negocio.

IV. VENTAJAS DE UNA PLATAFORMA DE CIBERSEGURIDAD DESDE LA NUBE Y PARA LA NUBE

La tendencia en América Latina de ambientes multi-cloud ciertamente hacen imperativo crear una estrategia que considere la utilización de una plataforma de ciberseguridad integrada y gestionada desde la nube y para la nube. A lo que nos referimos es a poder gestionar la seguridad con una visión de 360 grados, apoyándose en la analítica de seguridad, inteligencia sobre amenazas, automatización de procesos, sistemas cognitivos y de visibilidad en la red para proteger cada capa e instancia de cloud (público o privado), el data center propio y las cargas de trabajo hosteadas en un proveedor de servicios, los dispositivos móviles, endpoints y teléfonos inteligentes.

Cuando una organización define dentro de su estrategia de seguridad un cambio en los modelos de inversión, alejándose de productos específicos y orientándose más hacia el consumo de soluciones de plataformas, consigue reducir el impacto de ciertas preocupaciones del CISO con relación a:

- Infraestructura fragmentada
- Presupuestos con perfiles de CAPEX
- Necesidad de un importante número de profesionales en ciberseguridad
- Costos asociados a capacitación y certificaciones

Si una compañía, además de orientarse hacia plataformas de ciberseguridad, busca establecer un contrato con un modelo de servicios, puede encontrar ventajas adicionales relacionadas con:

- Presupuestos con perfiles de OPEX
- Pago por uso
- Prescindir de costos asociados a actualizaciones de plataforma
- Escalamiento de capacidades
- Orquestación, consolidación y centralización de la gestión de seguridad
- Automatización de procesos
- Reducción de costos asociados a instalación en premisas, energía, capacidad de cómputo

V. OFERTA Y DESAFÍOS DE KASPERSKY LAB EN LATINOAMÉRICA

Kaspersky Lab es una compañía mundial de seguridad cibernética con más de 20 años de trayectoria en el mercado. Kaspersky Lab utiliza su experiencia en inteligencia de amenazas y seguridad para desarrollar soluciones de seguridad y servicios para proteger a empresas, infraestructura crítica, gobiernos y consumidores de todo el mundo.

El enfoque de Kaspersky Lab es el de detectar y neutralizar cualquier forma de malware, basándose en el conocimiento sobre amenazas en cualquier parte del mundo y en cualquier idioma, por lo que cuenta con un equipo de investigadores en seguridad ubicados en Europa, Medio Oriente, Asia, EUA y Latinoamérica llamado GReAT (Global Research and Analysis Team). Recientemente, y como parte de su iniciativa de transparencia global, la empresa ha anunciado para finales del 2019 la apertura de su primer centro de transparencia, Transparency Center, en la ciudad de Zurich Suiza, donde se reubicará el almacenamiento y procesamiento de datos de sus clientes de, en una primera fase, Europa, Norte América, Japón, Singapur, Australia y Corea del Sur. Adicionalmente, Kaspersky Lab reubicará en las mismas instalaciones las herramientas de programación para desarrollar software basado en su código fuente e iniciará la construcción de bases de datos de antivirus firmadas digitalmente en Suiza previa a su distribución en los endpoints de los clientes a nivel mundial. Kaspersky Lab buscará que estas iniciativas sean supervisadas por una organización independiente, sin fines de lucro y con la calificación necesaria para llevar a cabo evaluaciones técnicas y auditorías de software.

Los clientes de Kaspersky Lab son diversos, desde usuarios en el hogar y microempresas, hasta organizaciones medianas y grandes corporativos, en prácticamente de cualquier industria. Su base instalada es de 400 millones de usuarios y 270 000 clientes corporativos.

La cartera de seguridad de la compañía es extensa, incluyendo protección de terminales y otras soluciones de seguridad, como también servicios especializados para combatir las amenazas digitales más avanzadas y en evolución, En respuesta a las necesidades de seguridad en endpoints y ambientes híbridos, Kaspersky Lab disponibiliza sus consolas de gestión de seguridad basadas en la nube:

- Protección a los principales puntos de entrada
  - Kaspersky Security for Microsoft Office 365- consola de seguridad, que al igual que Microsoft Office 365, reside también en la nube. Se basa en tecnologías avanzadas como sistemas de detección automatizada, sandboxing, información sobre amenazas en tiempo real y machine learning para proteger la entrada a través de emails (Exchange Online) de ransomware, archivos maliciosos, spam, phishing, business email compromiso (BEC), entre otros, al mismo tiempo que previene el bloqueo o eliminación de correos legítimos.
- Seguridad para ambientes móviles
  - Kaspersky Cloud Endpoint Security - protección para endpoints en Windows, Linux, Mac y dispositivos móviles, ya sean para uso personal o del negocio, que acceden a datos e información de la empresa que residen en aplicativos, folders compartidos y servidores en plataformas on-premises o cloud, conforme al Reglamento General de Protección de Datos (GDPR), de la Unión Europea. La configuración de la seguridad se hace en forma centralizada desde cloud mediante una consola de gestión en línea y en forma remota.
- Seguridad para ambientes heterogéneos y multi-cloud.
  - Kaspersky Hybrid Cloud Security-solución de seguridad integrada con Amazon Web Services y Microsoft Azure para data center definidos por software (Linux o Windows), protegiendo datos, redes, sistemas y cargas de trabajo en ambientes físicos, virtuales o en cloud mediante técnicas de orquestación, higiene operacional y protección de ciberataques mediante el análisis de comportamiento inteligente y algoritmos de aprendizaje automático, basados en machine learning e inteligencia artificial.
  - Soluciones verticalizadas para las industrias con requerimientos regulatorios y de cumplimiento en ciberseguridad bastante específicos como Finanzas, Telecomunicaciones, Salud, Gobierno y Manufactura.

- Seguridad corporativa digital.
  - Estrategia de continuidad del negocio, gestión de amenazas y defensa basada en tecnologías de seguridad y servicios de ciberseguridad de acuerdo con el perfil de riesgo de la organización, desde la identificación de ataques, investigación de incidentes, hasta la

respuesta y remediación a riesgos en funcionalidad en cada capa de la infraestructura empresarial.

- Programas de profesionales de concientización de seguridad corporativa, sandboxing como servicio, soporte estándar y premium, así como también servicios calificados en seguridad desde el diseño e implementación, actualizaciones, evaluación y configuración de soluciones por perfil de riesgo, hasta el monitoreo y evaluación de la administración de los sistemas de seguridad en forma remota o en sitio.

Kaspersky Lab acerca sus soluciones a través de más de 60 distribuidores certificados en 19 países de América Latina. La capacitación técnica y comercial para sus socios de negocio es gratuita a través del Portal de Socios que incluye videos interactivos, seminarios web y exámenes en línea, lo que les permite una educación y actualización continua.

Los Desafíos en Latin America

Kaspersky Lab, al igual que otros proveedores de soluciones de ciberseguridad, se enfrenta a desafíos en América Latina. En primer lugar, está la insuficiente inversión y recursos de las organizaciones para proteger a los puntos de acceso objetivos del ciberdelincuente que son los escritorios o dispositivos de los usuarios finales de la organización, constantemente expuestos a ataques cada vez más inteligentes y automatizados. Se requiere implementar programas de concientización sobre la seguridad empresarial junto con la adopción de herramientas más automatizadas e inteligentes para la detección oportuna de amenazas.

En segundo lugar, las iniciativas de movilidad han creado la necesidad de gestionar y proteger localmente y en la nube los numerosos endpoints desde los cuales se tiene acceso a datos e información de las empresas. Esto también ha detonado la necesidad de un staff de seguridad especializado y constantemente actualizado sobre la evolución de las ciberamenazas. La realidad en la región es que no es fácil hallar expertos en seguridad con las certificaciones adecuadas, capaces de administrar múltiples productos de seguridad e incluso de diferentes fabricantes.

Por último, tenemos las diferentes instancias de cloud, desde servicios públicos de cloud hasta arquitecturas de cloud privadas administradas por la empresa o por un proveedor de servicios y ambientes híbridos; el resultado es un ambiente complejo y bastante heterogéneo. Los CISOs deben seguir administrando la seguridad de los ambientes tradicionales de TI y, al mismo tiempo, crear una estrategia de seguridad nativa de cloud y de acuerdo con el perfil de riesgo de la organización.

VI. CONCLUSIONES Y RECOMENDACIONES

Las pérdidas asociadas a los ciberataques en América Latina llegan a los 90,000 millones de dólares, mientras que la inversión total de TI en la región representa solamente el 45% de dicho monto, de acuerdo con un informe del Banco Interamericano de Desarrollo y de la Organización de los Estados Americanos (2016). Esto nos da una dimensión de los desafíos en América Latina, región donde la inversión y recursos en seguridad, y las estrategias de prevención y concientización de riesgos son aún insuficientes ante el aumento de proyectos en la nube y movilidad.

IDC considera que las empresas deben analizar la utilización de una plataforma de soluciones de ciberseguridad, de acuerdo con su ecosistema de TI y perfil de riesgo, en función de los cambios en el modelo del negocio y su infraestructura física, virtual y en la nube.

- Emprenda programas de concientización sobre amenazas en seguridad a lo largo de la organización y diseñe políticas de comunicación sobre incidentes de ciberseguridad.
- Analice las diferentes capas de la infraestructura de TI, las cargas de trabajo, redes y servicios, así como también los diferentes puntos de acceso tanto locales como en la nube.

- Adopte un modelo de seguridad proactivo e integral para la interpretación de los riesgos, la determinación de acciones oportunas y la implementación de un programa de respuesta a incidentes, ya sea interno o contratado como servicio.
- Apóyese en herramientas de seguridad de próxima generación que pueden ser nativas en cloud y basadas en analítica de seguridad e inteligencia sobre amenazas, y complementadas con sistemas cognitivos y de visibilidad en la red que agilicen la labor del staff de TI y habiliten la respuesta inmediata, automatizada e inteligente frente a nuevas amenazas.
- Evalúe costos de actualizaciones, certificaciones y capacitación de su personal en soluciones de ciberseguridad con recursos propios de la empresa y compárelos contra los servicios contratados de proveedores de soluciones de seguridad.
- Apóyese en servicios de profesionales en seguridad para directivos del negocio y el área de TI que les permita construir casos de uso y justificación de soluciones de seguridad de acuerdo con los requerimientos y regulaciones de la industria en que se desarrolla la organización.

Es también importante considerar que los ataques a la seguridad son cada vez más sofisticados e inteligentes, por lo que es importante apoyarse en servicios de consultoría de expertos en ciberseguridad para el diseño y evaluación de una estrategia de seguridad adecuada, el constante monitoreo y rastreo de amenazas e indicadores de riesgo, así como también la auditoría de la seguridad corporativa que garanticen la continuidad del negocio.

Acerca de IDC

International Data Corporation (IDC) es la principal firma mundial de inteligencia de mercado, servicios de consultoría, y eventos para los mercados de Tecnologías de la Información, Telecomunicaciones y Tecnología de Consumo.

Con más de 1,100 analistas alrededor del mundo, IDC provee experiencia mundial, regional y local sobre las tendencias y oportunidades en tecnología e industria en 110 países.

El análisis y conocimiento de IDC ayuda a los profesionales de TI, ejecutivos de negocios y la comunidad de inversión, a tomar decisiones fundamentadas sobre tecnología y a alcanzar los objetivos clave de negocio.

Fundada en 1964, IDC es una subsidiaria de IDG, la empresa líder en medios de tecnología, investigación y eventos.

Para conocer más acerca de IDC, por favor visita www.idc.com y www.idclatin.com

Síguenos en Twitter como @IDCLatin / @IDC

IDC Latinoamérica

4090 NW 97th Avenue Suite 350,
Doral, FL, USA 33178
+1-305-351-3020
Twitter: @IDCLatin
www.idclatin.com
www.idc.com

Aviso de Derechos de Autor