IDC ANALYZE THE FUTURE

IDC EXECUTIVE BRIEF

Plataformas de Ciberseguridad: buscando la eficiencia en el negocio

Abril, 2018

Carlo Dávila

Patrocinado por: Kaspersky Lab.

La digitalización de las empresas en América Latina en la 3ª Plataforma (cloud, movilidad, social business, big data/analítica) y la adopción de Internet de las Cosas han generado un ecosistema de Tecnología de Información, donde la administración de los ambientes de seguridad se ha hecho más compleja. Los retos para el área de TI son diversos: las estrategias de seguridad tradicionales son insuficientes para las aplicaciones del negocio digital, la gestión de múltiples productos de seguridad de diferentes proveedores, la escasez y el alto costo del talento en ciberseguridad, así como también las restricciones en presupuesto y tamaño de personal especializado y certificado que son asignados a la seguridad de la infraestructura tecnológica.

En este documento analizaremos por qué las empresas deben lograr un ambiente de TI menos fragmentado y complejo de administrar mediante una plataforma de ciberseguridad gestionada en forma integral con herramientas de seguridad simplificadas.

I. OPINION DE IDC

Los productos tradicionales de seguridad y los modelos convencionales de inversión hacen más compleja la gestión de la seguridad de TI.

La Transformación Digital, entendiéndose como un proceso en que las organizaciones impulsan cambios en su arquitectura empresarial para ofrecer nuevos productos, servicios y modelos de negocio, se basa en lo que IDC define como tecnologías de la 3ª Plataforma (cloud, social business, big data & analytics y movilidad). Estos cambios disruptivos, para lograr la competitividad empresarial, han dado por resultado más retos relacionados con la ciberseguridad donde se busca proteger cargas de trabajo en ambientes híbridos (on-premises y cloud pública, privada o híbrida), donde hay más puntos vulnerables de acceso desde dispositivos móviles inteligentes y redes sociales e incluyendo ambientes de colaboración y análisis de datos dentro y fuera de la organización.

En otras palabras, el impacto de la Transformación Digital en la información y las operaciones de una empresa extiende aún más la superficie de ataque. Es por esa razón que una estrategia de seguridad tradicional es insuficiente para responder a los riesgos en los nuevos ecosistemas de TI cada vez más distribuidos, escalables y móviles.

Otro aspecto importante es que, a lo largo del tiempo, las empresas han ido invirtiendo en las mejores soluciones ("best of breed") para necesidades específicas de seguridad empresarial. El resultado de esto es la presencia de múltiples productos y herramientas de seguridad de diversos proveedores de TI, cada uno con diferentes esquemas de uso o licenciamiento y requerimientos de certificación, lo que dificulta su

administración. IDC ha identificado a más de 70 fabricantes de ciberseguridad presentes en América Latina alrededor de los siete perfiles de productos de seguridad definidos por IDC.

De acuerdo con el estudio IDC Latin America Cybersecurity Report 2017, tres de cada cinco empresas consideran que habrá una reducción del 15% en inversión en ciberseguridad. Hoy día, 50% de las empresas siguen un modelo de inversión donde se asigna menos del 10% de su presupuesto de TI para soluciones de ciberseguridad. También es importante resaltar que actualmente 31% de las empresas no implementa políticas de comunicación sobre incidentes de seguridad, lo que puede afectar a la primera línea de respuesta a las amenazas; es decir, a los empleados. Esto deja claro la necesidad de las organizaciones por desarrollar programas de concientización de amenazas cibernéticas para desarrollar las capacidades de prevención de los colaboradores, a través de la contratación de servicios especializados que les apoyen en la mitigación de riesgos en forma más eficiente.

Aunado a esto, el incremento de los ataques en redes, cargas de trabajo y aplicaciones en la web han hecho evidente la necesidad de contar con personal certificado y especializado en seguridad de TI. Si se tiene en cuenta la presencia de múltiples fabricantes en los ecosistemas de TI de las organizaciones, se entiende que el requerimiento de personal es mayor, lo que genera retos adicionales para los CIOs y CISOs en Latinoamérica donde tres de cada cuatro compañías consideran difícil hallar personal suficientemente calificado en ciberseguridad.

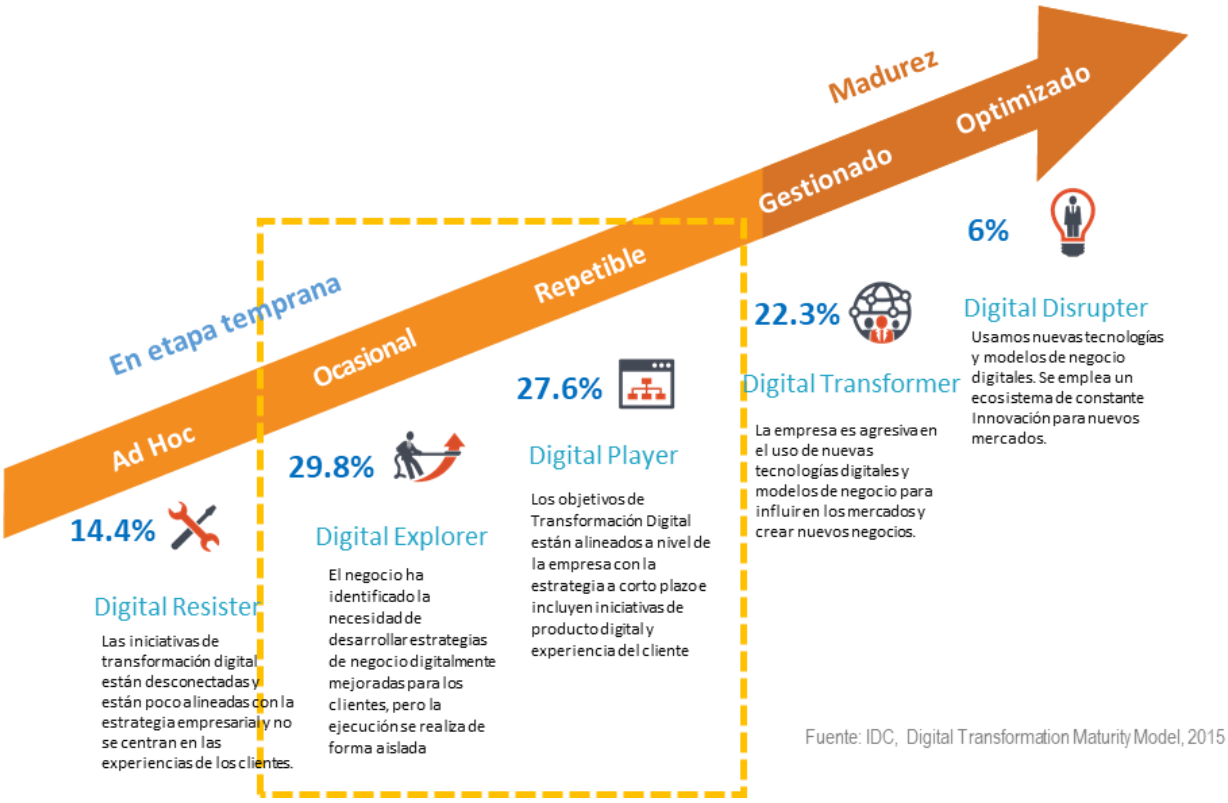
II. Cómo la Transformación Digital, Cloud y Movilidad influyen en el ecosistema de TI.

La inversión en iniciativas de Transformación Digital ha tenido un crecimiento sostenido (CAGR de 23% desde el 2015) en América Latina, esperando alcanzar los 58 mil millones de dólares al 2020. La mayoría de las empresas de la región se halla en una etapa temprana en la adopción de la Transformación Digital como puede verse en la Figura 1. El nuevo ecosistema, basado en la 3ra Plataforma y aceleradores de innovación como Internet de las Cosas (IoT), requiere de inversión en soluciones de seguridad acordes a los nuevos ecosistemas digitales. Sin embargo, solo 6% de las empresas considera la ciberseguridad como un habilitador de la transformación del negocio. Esto es preocupante dado su impacto en la operabilidad de la empresa; la sensibilidad de los datos tanto de la organización como de los socios de negocio y de sus clientes; así como también en el cumplimiento de disposiciones legales del país donde se desempeña la organización, en especial en industrias con mayor regulación tales como gobierno, finanzas y telecomunicaciones.

De acuerdo con un informe del Banco Interamericano de Desarrollo y de la Organización de los Estados Americanos, las pérdidas asociadas al ciberdelito en América Latina llegan a los 90 mil millones de dólares, en una región cuya inversión total en TI empresarial es alrededor del 45% de dicho monto.

FIGURA 1

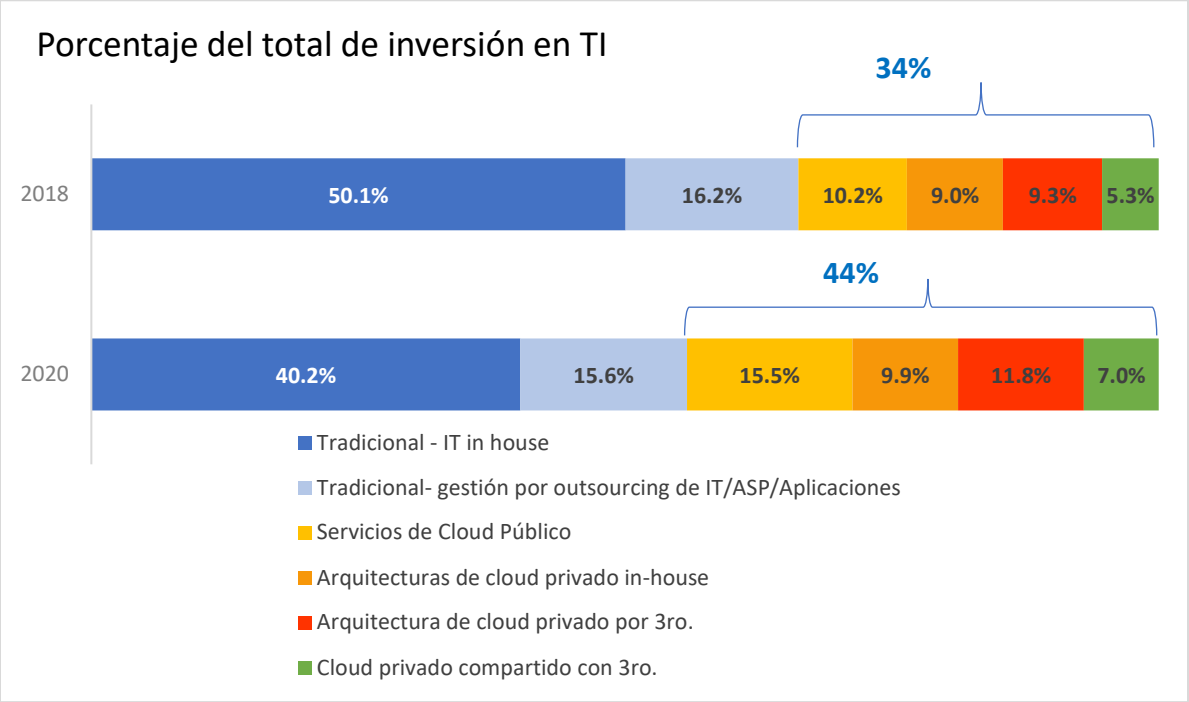
Adopción de la Transformación Digital en América Latina



De la 3ª Plataforma, cloud (Figura 2) y movilidad son los pilares más dinámicos en la transformación del negocio donde se busca hacer más eficientes los recursos del negocio y agilizar el uso de las aplicaciones, por lo que la plataforma de ciberseguridad debe ser gestionada, incorporando en la estrategia de seguridad un perfil de gestión desde la nube y para la nube, unida a la administración de los ecosistemas tradicionales de TI. Esto significa gestionar la seguridad en la premisa del cliente, en el datacenter de un proveedor de servicio, en ambientes de cloud (público, privado o híbrido) considerando el acceso a las cargas de trabajo, desde dispositivos móviles, endpoints y teléfonos inteligentes. Es decir, la estrategia de ciberseguridad debe alinearse, con un enfoque de 360 grados, a los nuevos modelos operativos y de información de la transformación digital.

FIGURA 2

Ambientes multi-cloud en América Latina



Fuente: IDC LA, IT Investment Trends Survey 2017 Q4

La movilidad está hoy día dentro de las cinco iniciativas con mayor prioridad para las empresas latinas, 31% de las organizaciones de la región así lo señalaron en el reporte de Tendencias de Inversión, del mismo modo movilidad es también la fuente de mayor preocupación para las áreas de TI. 85% de los responsables de ciberseguridad (CISOs) considera que las Laptops y desktops basados en Windows son los endpoints más vulnerables, seguidos por los teléfonos inteligentes con sistema operativo Android y los tablets del mismo sistema operativo. Considerando que la seguridad en un ecosistema de movilidad incluye productos específicos como administración de seguridad y vulnerabilidad en móviles, gestión de identidad y acceso móvil, acceso y protección a ambientes móviles, protección y control de información móvil y gestión de amenazas en movilidad[1], resulta sorprendente que solo 45% de los CISOs sí estén considerando incluir dichas soluciones dentro de sus planes de inversión en ciberseguridad.

Los CISOs enfrentan reducciones de presupuesto y escasez de personal especializado para administrar los ambientes de seguridad. Por un lado, 75% de las organizaciones están invirtiendo hasta un 20% de su presupuesto de TI en ciberseguridad; sin embargo, 69% está haciendo recortes hasta de un 40% en ese rubro. Asimismo, 14% de las organizaciones están experimentando una reducción en el ratio de personal especializado en ciberseguridad sobre el total de colaboradores del área de TI. Esto puede deberse a que 24% de los CISOs consideran que el reclutamiento de profesionales de ciberseguridad es costoso, y un 45% de los CISOs indica que no encuentra personal lo suficientemente calificado para gestionar la ciberseguridad de la compañía. Los retos se hacen más evidentes si se tiene en cuenta que al interior de

[1] Mobile Security & Vulnerability Management, Mobile Identity & Access Management, Mobile Gateway Access & Protection, Mobile Information protection & Control and Mobile Threat Management.

una misma organización se requiere administrar múltiples productos de seguridad de diferentes fabricantes. De ahí la necesidad de cambiar de un enfoque de productos específicos hacia una plataforma de soluciones de ciberseguridad, de acuerdo con el ecosistema digital de la organización y su nuevo perfil de riesgo en función de los cambios en el modelo del negocio.

Esta plataforma de soluciones de ciberseguridad permitirá reducir el impacto de algunas de las principales preocupaciones de los CIOs/CISOs; ya que, al integrar y automatizar determinados procesos de la gestión de ciberseguridad, utilizando herramientas de machine learning entre otras, se simplifica la administración y se contribuye a reducir la necesidad de contar con un mayor número de especialistas en ciberseguridad.

III. PANORAMA A FUTURO

En América Latina, el mercado de soluciones de seguridad se estima con un valor de tres mil millones de dólares al finalizar 2018. Para 2020, se estima un valor de 4.2 mil millones de dólares, con una tasa de crecimiento de 12% en 5 años (CAGR). De esta última cifra, se estima que 62% provendrá de la adopción de servicios de seguridad gestionados por terceros.

El crecimiento de los servicios de seguridad está definido por la búsqueda de eficiencia en la utilización de recursos escasos tanto económicos como de capital humano por parte de las organizaciones. El 14% de los CISOs en la región está considerando tercerizar el manejo de la ciberseguridad. Las razones son:

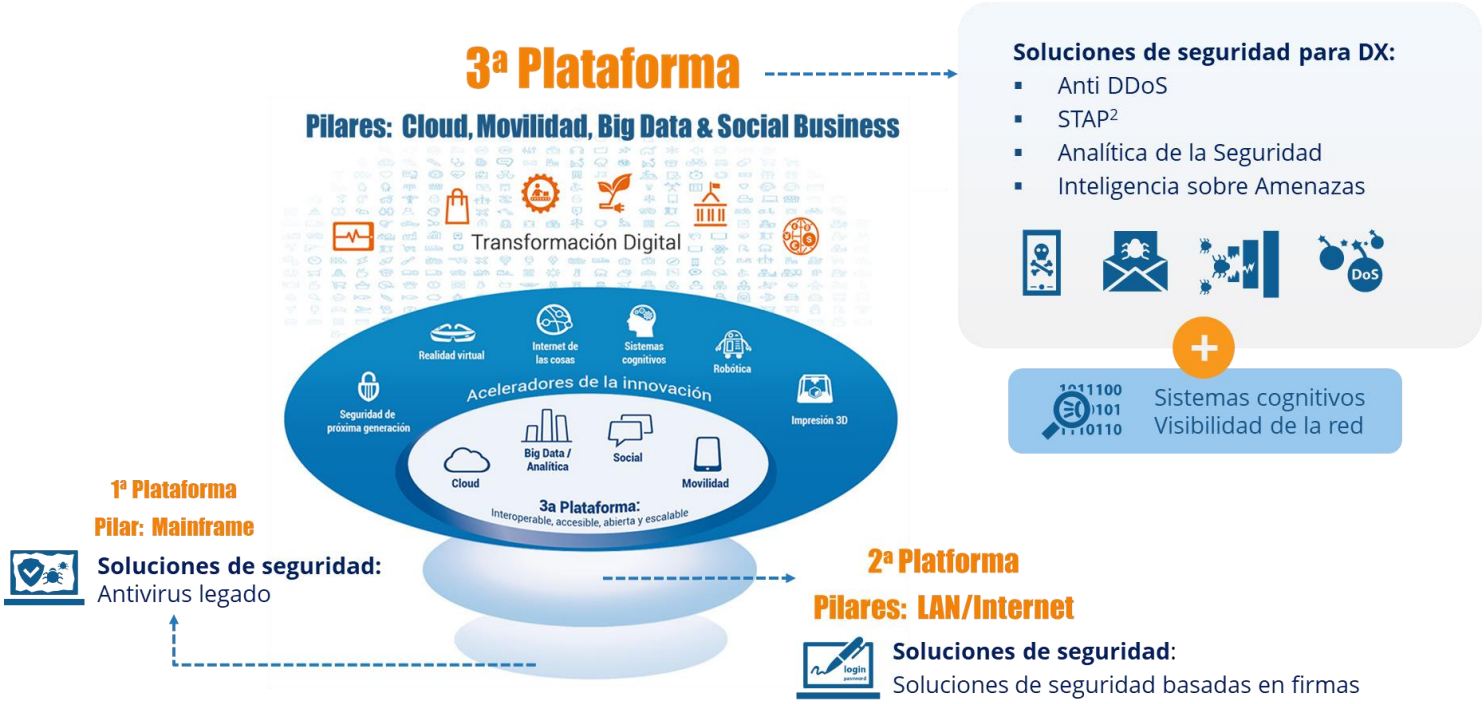
- La complejidad de administrar múltiples productos de seguridad de diferentes proveedores en una misma infraestructura tecnológica.
- El costo de certificaciones y capacitación en productos de seguridad.
- La escasez del personal calificado para gestionar las soluciones desplegadas.
- El reto de mantenerse actualizados sobre nuevas amenazas que son cada vez más sofisticadas, complejas, distribuidas y que evolucionan hacia procesos automatizados.

IV. GUÍA ESENCIAL

A medida que las empresas emprenden proyectos de Transformación Digital deben implementar un análisis para conocer su perfil de riesgo corporativo y definir una estrategia de seguridad acorde al ecosistema de la 3ª Plataforma y a los aceleradores de la innovación, como la automatización y el Internet de las Cosas, al mismo tiempo de buscar la optimización de los recursos y presupuestos de TI- Figura 3.

FIGURA 3

Soluciones de seguridad acordes a la Transformación Digital



[2]Specialized Threat Analysis & Protection (STAP)

Más sobre la 3a.Plataforma: http://www.idc.com/promo/thirdplatform

Fuente: IDC, 2018

Para implementar una plataforma más eficiente de ciberseguridad, IDC enumera las siguientes recomendaciones:

- Recuerde que la transformación digital se basa en la 3ª Plataforma, por lo que no se puede seguir invirtiendo en soluciones tradicionales, usualmente diseñadas para la 2ª Plataforma.
- Incluya un análisis de la ciberseguridad a la par de sus proyectos de transformación del negocio identificando los nuevos elementos en el ecosistema de TI.
- Recuerde que las tecnologías disruptivas como robótica, automatización e Internet de las Cosas resultan en un mayor número de puntos de acceso que requieren de soluciones de ciberseguridad con capacidades de visibilidad, inteligencia, analítica avanzada y el uso de sistemas cognitivos.
- Analice el consumo de servicios de nube y la ejecución de proyectos de movilidad considerando en la estrategia de seguridad:
  - La administración de los ambientes de su premisa.
  - El perfil de las cargas de trabajo que se mueve a la nube y/o hacia ambientes híbridos.
  - Los ecosistemas móviles desde los cuales se accede a las plataformas de negocio de la compañía.

- Evalúe y compare en su plan estratégico de seguridad, el uso de una plataforma en la premisa versus la contratación de un servicio tercerizado de ciberseguridad considerando los costos de actualizaciones, certificaciones y capacitación en nuevas soluciones de seguridad.
- Emprenda un modelo de seguridad proactivo e integral para una adecuada 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.

Y, finalmente, cambie el enfoque de la inversión en ciberseguridad considerando una estrategia de 360 grados, acorde a los nuevos modelos operativos y de información del negocio digital, apoyándose en herramientas y servicios que simplifiquen su gestión.

Fuentes y Referencias

IDC Latin America Cybersecurity Report 2017.

IDC Worldwide Security Products Taxonomy 2018.

IDC Digital Transformation Maturity Model, 2017.

IDC Worldwide Semiannual Digital Transformation Spending Guide, 2017.

IDC Web Application Firewalls: Critical Component of API security.

IDC Latin America Investment Trends, 2017Q4.

2016 Cybersecurity Report Inter American Development Bank & Organization of American States

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