IDC EXECUTIVE BRIEF

Plataformas de segurança cibernética: buscando eficiência nos negócios

Abril, 2018

Carlo Dávila

Patrocinado por: Kaspersky Lab.

A digitalização de empresas na América Latina na 3ª Plataforma (nuvem, mobilidade, negócios sociais e Big Data / Analytics) e a adoção da Internet das Coisas geraram um ecossistema de Tecnologia da Informação onde a gestão de ambientes de segurança ficou muito mais complexa. Os desafios para a área de TI são diversos: estratégias de segurança tradicionais que são insuficientes para aplicativos de negócios digitais, o gerenciamento de vários produtos de segurança de diferentes provedores, a escassez e o alto custo dos talentos de segurança cibernética, bem como restrições no orçamento e na quantidade de pessoal especializado e certificado que são designados para lidar com a segurança da infraestrutura tecnológica.

Neste documento, analisaremos porque as empresas devem buscar um ambiente de TI menos fragmentado e complexo para gerenciar, por meio de uma plataforma de segurança cibernética gerenciada de maneira abrangente com ferramentas de segurança simplificadas.

I. OPINIÃO DA IDC

Os produtos de segurança tradicionais e os modelos de investimento convencionais tornam o gerenciamento de segurança de TI mais complexo.

A transformação digital, entendida como o processo no qual as organizações impulsionam mudanças em sua arquitetura de negócios para oferecer novos produtos, serviços e modelos de negócios, é baseada no que a IDC define como tecnologias da 3ª plataforma (nuvem, mobilidade, negócios sociais e Big Data / Analytics). Essas mudanças disruptivas para alcançar a competitividade dos negócios resultaram em mais desafios relacionados à segurança cibernética, que procura proteger as cargas de trabalho em ambientes híbridos (on-Premises e nuvem pública, privada ou híbrida), onde há pontos de acesso mais vulneráveis de dispositivos móveis inteligentes e redes sociais, e incluindo ambientes colaborativos e análise de dados dentro e fora da organização.

Em outras palavras, o impacto da transformação digital nas informações e operações da empresa aumenta ainda mais a superfície de ataque. É por essa razão que uma estratégia de segurança tradicional é insuficiente para responder aos riscos nos novos ecossistemas de TI que estão cada vez mais distribuídos, escaláveis e móveis.

Outro aspecto importante é que, ao longo do tempo, as empresas têm investido nas melhores soluções ("*best of breed*") para necessidades específicas de segurança empresarial. O resultado disso é a presença de vários produtos e ferramentas de segurança de vários fornecedores de TI, cada um com diferentes esquemas de uso ou licenciamento e requisitos de certificação, o que dificulta a administração. A IDC

identificou mais de 70 fabricantes de segurança cibernética presentes na América Latina em torno dos sete perfis de produtos de segurança definidos pela IDC.

De acordo com o relatório IDC Latin America Cybersecurity Report 2017, três em cada cinco empresas acreditam que haverá uma redução de 15% no investimento em segurança cibernética. Hoje, 50% das empresas seguem um modelo de investimento em que menos de 10% do orçamento de TI é alocado para soluções de segurança cibernética. Também é importante notar que atualmente 31% das empresas não implementam políticas de comunicação sobre incidentes de segurança, o que pode afetar a primeira linha de resposta a ameaças; isto é, para funcionários. Isso deixa claro a necessidade de as organizações desenvolverem programas de conscientização sobre ameaças cibernéticas para desenvolver as capacidades de prevenção dos funcionários, por meio da contratação de serviços especializados que os auxiliam na mitigação de riscos de maneira mais eficiente.

Somado a isso, o aumento de ataques a redes, cargas de trabalho e aplicativos na Web evidenciou a necessidade de pessoal certificado e especializado em segurança de TI. Se levarmos em conta a presença de vários fabricantes nos ecossistemas de TI das organizações, entende-se que a necessidade de pessoal é maior, o que gera desafios adicionais para CIOs e CISOs na América Latina, onde três de cada quatro empresas consideram difícil encontrar pessoal suficientemente qualificado em cibersegurança.

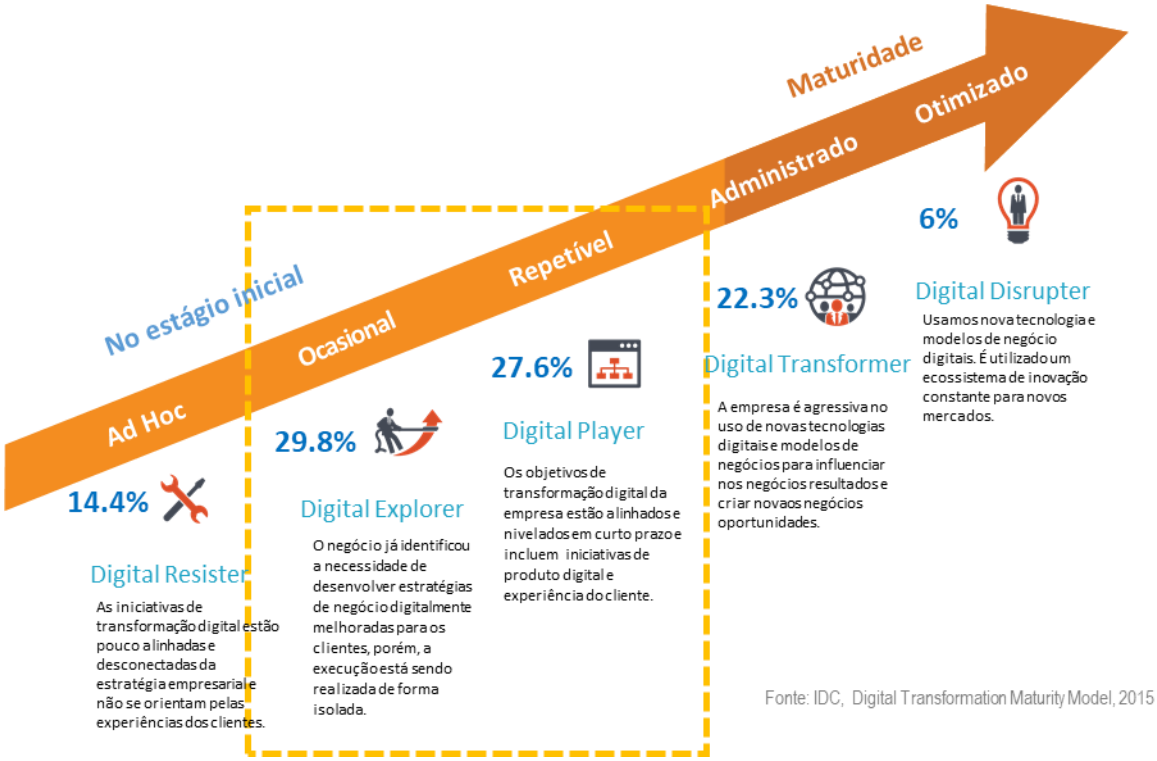
II. Como a transformação digital, a nuvem e a mobilidade influenciam o ecossistema de TI.

O investimento em iniciativas de transformação digital teve um crescimento sustentado (CAGR de 23% desde 2015) na América Latina, e deve alcançar 58 bilhões de dólares até 2020. A maioria das empresas da região está em um estágio inicial de adoção da transformação digital, como pode ser visto na Figura 1. O novo ecossistema, baseado na 3ª Plataforma e aceleradores de inovação como a Internet das Coisas (IoT), requer investimento em soluções de segurança de acordo com os novos ecossistemas digitais. Entretanto, apenas 6% das empresas consideram a segurança cibernética como um facilitador da transformação dos negócios. Isso é preocupante, dado seu impacto na operabilidade da empresa, na sensibilidade dos dados da organização e dos parceiros de negócios e seus clientes, bem como na conformidade com as disposições legais do país em que a organização opera, especialmente em setores com mais regulamentação, como governo, finanças e telecomunicações.

Segundo um relatório do Banco Interamericano de Desenvolvimento e da Organização dos Estados Americanos, as perdas associadas ao crime cibernético na América Latina chegam a 90 bilhões de dólares, em uma região cujo investimento total em TI é de cerca de 45% desse montante.

FIGURA 1

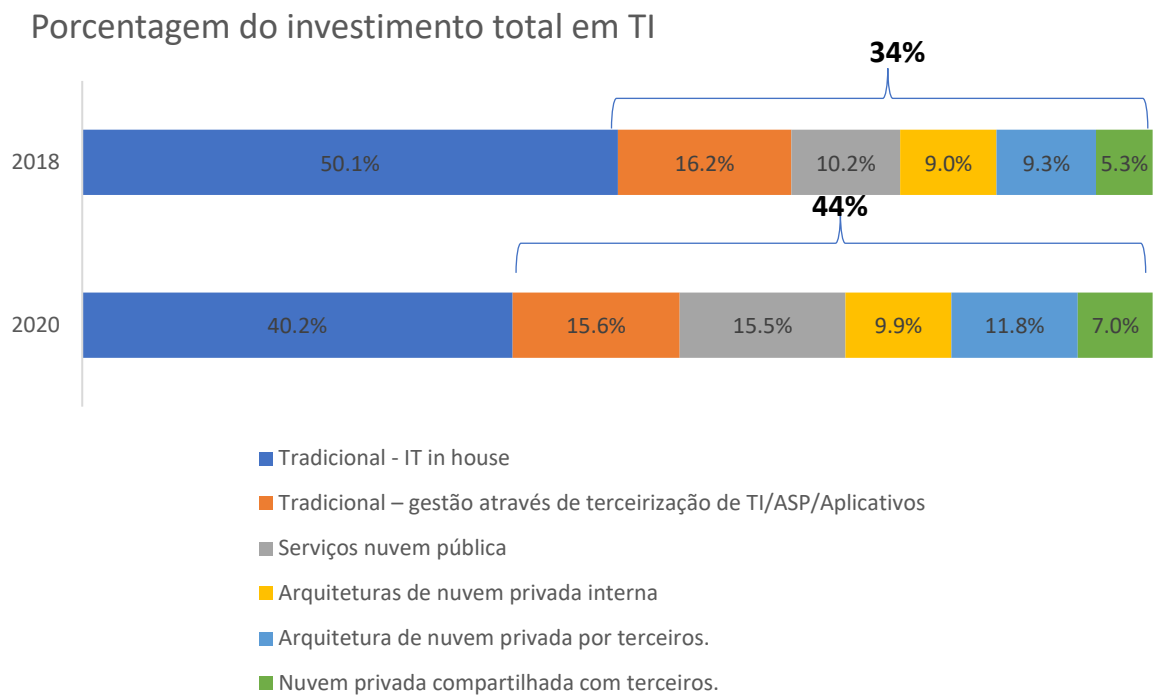
Adoção da Transformação Digital na América Latina



Da 3ª Plataforma, a nuvem (Figura 2) e a mobilidade são os pilares mais dinâmicos na transformação de negócios, pelos quais se busca tornar os recursos de negócios mais eficientes e otimizar o uso de aplicativos. Por este motivo, a plataforma de segurança cibernética deve ser gerenciada, incorporando na estratégia de segurança um perfil de gerenciamento da nuvem e para a nuvem juntamente com a administração de ecossistemas tradicionais de TI. Isso significa gerenciar a segurança nas instalações do cliente, no datacenter de um provedor de serviços, em ambientes de nuvem (pública, privada ou híbrida), considerando o acesso às cargas de trabalho a partir de dispositivos móveis, endpoints e smartphones. Em outras palavras, a estratégia de segurança cibernética deve estar alinhada, com uma abordagem de 360 graus, aos novos modelos operacionais e de informação da transformação digital.

FIGURA 2

Ambientes multi-cloud da América Latina



Fonte: IDC LA, IT Investment Trends Survey 2017 Q4

A mobilidade está hoje entre as cinco iniciativas com maior prioridade para as empresas latinas, segundo 31% das organizações da região que indicaram isso no relatório de tendências de investimento; contudo, mobilidade é também a fonte de maior preocupação para as áreas de TI. 85% dos responsáveis pela segurança cibernética (CISOs) acreditam que os laptops e desktops baseados em Windows são os endpoints mais vulneráveis, seguidos pelos smartphones com sistema operacional Android e os tablets do mesmo sistema operacional. Considerando que a segurança em um ecossistema de mobilidade inclui produtos específicos, como segurança móvel e gerenciamento de vulnerabilidades, gerenciamento de identidades e acesso móvel, acesso e proteção a ambientes móveis, proteção e controle de informações móveis e gerenciamento de ameaças móveis[1], é surpreendente que apenas 45% dos CISOs estejam considerando incluir tais soluções em seus planos de investimento em segurança cibernética.

Os CISOs enfrentam reduções orçamentárias e falta de pessoal especializado para gerenciar ambientes de segurança. Por um lado, 75% das organizações estão investindo até 20% de seu orçamento de TI em segurança cibernética; entretanto, 69% estão fazendo cortes de até 40% nessa área. Da mesma forma, 14% das organizações estão experimentando uma redução na proporção de pessoal de segurança cibernética em relação ao número total de funcionários na área de TI. Isso pode ser devido ao fato de que 24% dos CISOs consideram que o recrutamento de profissionais de segurança cibernética é caro, e 45% dos CISOs indicam que não encontram pessoal qualificado o suficiente para gerenciar a segurança cibernética da empresa. Os desafios tornam-se mais evidentes se levarmos em conta que dentro da mesma organização é necessário administrar vários produtos de segurança de diferentes fabricantes. Daí vem a necessidade de mudar tirar o foco de produtos específicos e olhar para uma plataforma de soluções

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

de segurança cibernética que esteja em linha com o ecossistema digital da organização e seu novo perfil de risco baseado em mudanças no modelo de negócios.

Essa plataforma de soluções de segurança cibernética reduzirá o impacto de algumas das principais preocupações dos CIOs/CISOs já que, integrando e automatizando certos processos de gerenciamento da segurança cibernética, usando ferramentas de aprendizado de máquina, entre outros, a administração é simplificada e ajuda a reduzir a necessidade de um número maior de especialistas em segurança cibernética.

III. PANORAMA AO FUTURO

Na América Latina, o mercado de soluções de segurança é estimado em um valor de três bilhões de dólares no final de 2018. Até 2020, esse valor deve atingir 4,2 bilhões de dólares, com uma taxa de crescimento de 12% em 5 anos (CAGR). Deste último número, estima-se que 62% virão da adoção de serviços de segurança gerenciados por terceiros.

O crescimento dos serviços de segurança é definido pela busca de eficiência no uso de recursos escassos de capital econômico e humano pelas organizações. 14% dos CISOs da região estão considerando terceirizar o gerenciamento da segurança cibernética. As razões são:

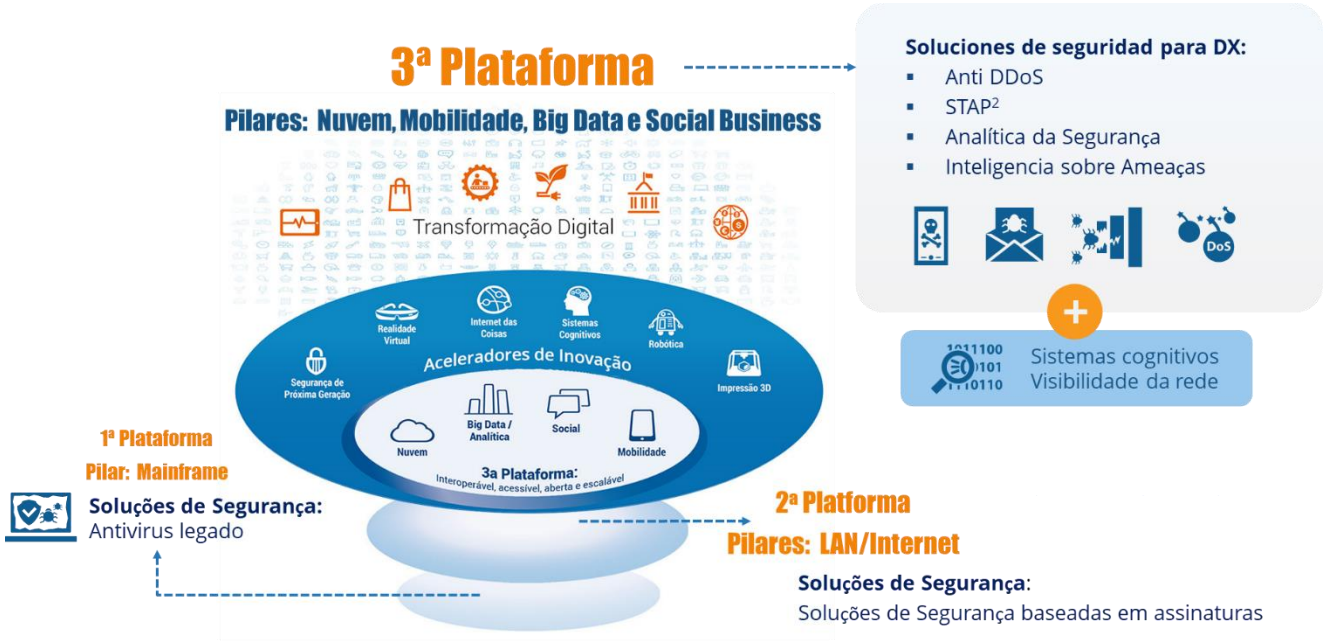
- A complexidade do gerenciamento de vários produtos de segurança de diferentes provedores na mesma infraestrutura tecnológica.
- O custo de certificações e treinamento em produtos de segurança.
- A falta de pessoal qualificado para gerenciar as soluções implantadas.
- O desafio de ficar atualizado sobre novas ameaças cada vez mais sofisticadas, complexas, distribuídas e evoluindo para processos automatizados.

IV. GUIA ESSENCIAL

Na medida em que as empresas realizam projetos de transformação digital, elas devem executar uma análise para conhecer seu perfil de risco corporativo e definir uma estratégia de segurança de acordo com o ecossistema da 3ª Plataforma e os aceleradores de inovação (como automação e Internet da Coisas), ao mesmo tempo em que procura a otimização de recursos e orçamentos de TI - Figura 3.

FIGURA 3

Soluções de segurança de acordo com a transformação digital



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

[2]Specialized Threat Analysis & Protection (STAP)

Fonte: IDC, 2018

Para implementar uma plataforma de segurança cibernética mais eficiente, a IDC lista as seguintes recomendações:

- Lembre-se que a transformação digital é baseada na 3ª Plataforma, portanto, você não pode continuar investindo em soluções tradicionais, geralmente projetadas para a 2ª Plataforma.
- Inclua uma análise de segurança cibernética junto com seus projetos de transformação de negócios, identificando os novos elementos no ecossistema de TI.
- Lembre-se de que tecnologias disruptivas, como robótica, automação e Internet das Coisas, resultam em um maior número de pontos de acesso que exigem soluções de segurança cibernética com visibilidade, inteligência, recursos analíticos avançados e uso de sistemas cognitivos.
- Analise o consumo de serviços em nuvem e a execução de projetos de mobilidade considerando a estratégia de segurança:
  - A administração do ambiente On-Premises.
  - O perfil de cargas de trabalho que se movem para a nuvem e/ou para ambientes híbridos.
  - Os ecossistemas móveis dos quais as plataformas de negócios da empresa são acessadas.
- Avalie e compare em seu plano estratégico de segurança o uso de uma plataforma no local versus a contratação de um serviço terceirizado de segurança cibernética, considerando os custos de atualizações, certificações e treinamento em novas soluções de segurança.

- Empreenda um modelo de segurança proativo e abrangente para uma interpretação adequada dos riscos, a determinação de ações oportunas e a implementação de um programa de resposta a incidentes, seja interno ou contratado como um serviço.

E, finalmente, mude o foco do investimento em cibersegurança considerando uma estratégia de 360 graus, alinhada aos novos modelos operacionais e de informação do negócio digital, baseados em ferramentas e serviços que simplificam sua gestão.

FONTES E REFERÊNCIAS

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.

Sobre a IDC

International Data Corporation (IDC) é a principal empresa de inteligência de mercado global, serviços de consultoria e eventos para os mercados de Tecnologia da Informação, Telecomunicações e Tecnologia de Consumo. Com mais de 1.100 analistas em todo o mundo, a IDC fornece conhecimentos globais, regionais e locais sobre tendências e oportunidades em tecnologia e indústria em 110 países.

A análise e o conhecimento da IDC ajudam os profissionais de TI, executivos e a comunidade de investimentos a tomar decisões informadas sobre a tecnologia e atingir os principais objetivos comerciais.

Fundada em 1964, a IDC é uma subsidiária da IDG, a principal empresa de mídia de tecnologia, pesquisa e eventos. Para saber mais sobre a IDC, visite www.idc.com e www.idclatin.com.

Siga-nos no 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