LGPD – quatro letras que representam privacidade

As soluções de cibersegurança sozinhas não conseguem garantir a conformidade, mas fornecem proteção eficaz contra violações de dados e vazamento de dados sigilosos.

kaspersky BRING ON THE FUTURE

kaspersky.com.br

Pronto para LGPD

LGPD – muito mais do que assinalar “checkbox”

“Não existe privacidade sem segurança” é um princípio consagrado da proteção de dados. No momento em que a Lei Geral de Proteção de Dados (“LGPD”) brasileira torna-se realidade, é oportuno analisar como as tecnologias de cibersegurança podem dar suporte aos objetivos mais amplos de privacidade e proteção de dados da LGPD.

Dados pessoais: uma fonte de dinheiro para os cibercriminosos

Os dados pessoais estão, literalmente, em todos os lugares.

As pessoas costumam enviar informações pessoais para organizações de todos os tipos, muitas vezes sem questionar nem entender por que ou como elas serão usadas. Ou se elas serão compartilhadas com terceiros desconhecidos.

Todos nós já rolamos até o final de um Contrato de Licença de Usuário Final (EULA, End User License Agreement) impreciso e clicamos em “Eu concordo”, sem realmente saber o que acontecerá com nossos dados. Ao condicionar os serviços a essa aceitação, muitas organizações forçam os usuários a assumir o risco de que seus dados possam acabar nas mãos erradas. Infelizmente, muitas vezes, é isso que acontece.

Embora a maioria das organizações faça o possível para proteger os dados que coleta, frequentemente não há um sentido real nesse processo, além de eliminar informações que ‘possam ser úteis’.

Mesmo com as melhores intenções do mundo, a falta de processos estabelecidos, associada à consciência limitada sobre os riscos e as responsabilidades envolvidos, é comum que dados sejam coletados e armazenados sem qualquer precaução de segurança. Pior ainda, frequentemente, eles são compartilhados (ou vendidos) para terceiros sem a implementação de qualquer acordo de proteção de dados, nem o conhecimento ou consentimento explícito do titular dos dados.
Infelizmente, os tipos de dados pessoais que são úteis para a sua empresa também geram lucros para cibercriminosos: de informações de programas de fidelidade a dados de pagamento, datas de nascimento e prontuários médicos, qualquer elemento que ajuda a empresa a personalizar a experiência do cliente ou a cuidar de seus colaboradores é extremamente atraente para os criminosos. Em última análise, eles se tornam uma espécie de moeda criminosa, trocada e negociada em mercados negros da DarkNet.

A partir de 18 de setembro de 2020 quando algo desse tipo acontece, o problema não é mais apenas dos infelizes titulares dos dados, mas seu também.

59% das empresas supõem que sua segurança de TI será comprometida e reconhecem a necessidade de estarem preparadas para esses eventos.[1]

Em 2017, 23% das organizações sujeitas ao GDPR (General Data Protection Regulation ou Regulamento Geral sobre a Proteção de Dados, regulamento de proteção de dados da União Europeia) informaram ter sofrido um ataque cibernético nos 12 meses anteriores.[2]

Violação de dados? Multa

Após uma enorme violação de dados de clientes em 2019, um varejista de vestuário foi multado em R$ 500.000,00 pelo Ministério Público do Distrito Federal. O valor da multa foi correspondente ao grande número de indivíduos atacados: dois milhões.

Mesmo sem multas, a fiscalização pode resultar em auditorias, monitoramento e uma reestruturação das práticas de processamento de dados, e tudo isso custa dinheiro.

Quatro letras que representam uma grande iniciativa de proteção de dados

As manchetes envolvendo multas pesadas, no Brasil, de até 2% do faturamento anual da empresa, podendo chegar até R$ 50 Milhões, e sem limite de infrações para a notificação de violações, atraem muita atenção. Vale lembrar que a LGPD representa uma oportunidade para fazer o levantamento do que você faz com os dados pessoais que coleta e se perguntar porque o faz.

Também é o momento ideal para reconsiderar a abordagem de sua organização em relação à cibersegurança. Embora as tecnologias de segurança sozinhas não possam garantir a conformidade, elas têm uma função de suporte importante para ajudar as empresas a alcançar suas metas de proteção de dados.

O que é, o que não é...

Apesar do grande número de documentos, manuais e outras publicações que seguiram seu anúncio, o entendimento básico de muitos aspectos da LGPD continua vago. Alguns altos executivos continuam acreditando que a legislação não se aplica a eles porque “Não temos esse tipo de dados”. Outros acham que basta assinalar uma caixa de seleção uma vez antes de fazer negócios da maneira usual.

Infelizmente, eles estão errados:

- Vocês têm empregados e colaboradores, certo? As informações dessas pessoas que costumam ser coletadas e processadas são dados pessoais e se enquadram na LGPD. Todas as empresas que coletam, processam e/ou armazenam dados pessoais, incluindo informações de empregados e colaboradores relacionadas a transações ou atividades no Brasil, ou que terceirizam essas atividades para outras empresas, têm a obrigação de protegê-los.
- A LGPD não é prescritiva, mas um sistema de referência. Não há uma lista de tarefas a cumprir para poder chegar ao nirvana da proteção de dados.

1. Kaspersky: Relatório de Riscos Globais de Segurança de TI.
2. Marsh: GDPR Preparedness: An Indicator of Cyber Risk Management

Segurança, Boas Práticas e Governança de Dados – Artigo 50 da LGPD

O Artigo 46 da LGPD prevê medidas técnicas e organizacionais apropriadas para garantir um nível de segurança adequado ao risco durante o controle ou processamento de dados pessoais. Elas incluem:

- "Pseudonimização" e criptografia de dados pessoais
- Medidas para respaldar a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de processamento
- Capacidade de restaurar a disponibilidade e acessibilidade dos dados após um incidente
- Possibilidade de realizar testes e avaliações periódicas da capacidade técnica e organizacional de proteger os dados e sua manipulação.

A autoridade de proteção de dados brasileira também publicará requisitos de segurança de dados mais detalhados.

A cibersegurança é importante para a proteção dos dados e para garantir a resiliência do sistema.

Embora a LGPD apresente regras que devem ser seguidas para obter a conformidade, há poucos detalhes específicos de como fazer isso; em grande medida, cada organização deve decidir pelas técnicas utilizadas. O ponto fundamental é que, como a proteção de dados é um processo, as empresas deveriam trabalhar nisso continuamente.

Não existe uma abordagem padrão para medir a conformidade. Esse é o alcance máximo da marcação de caixas de seleção. As circunstâncias (e os riscos associados) mudam, e quase nunca as listas são completas; assim, alguns pontos fracos podem ser ignorados em qualquer abordagem "universal".

Em última instância, aquilo que sua empresa faz para evitar um incidente – juntamente com sua estratégia de detecção precoce e rastreamento – é o que o ajudará a ser bem-sucedido em relação à LGPD.

As tecnologias e soluções da próxima geração da Kaspersky podem ajudar sua organização a alcançar suas metas de cibersegurança como parte da estratégia geral de conformidade com a LGPD.

Vamos analisar o que isso significa do ponto de vista prático.

É melhor prevenir do que remediar

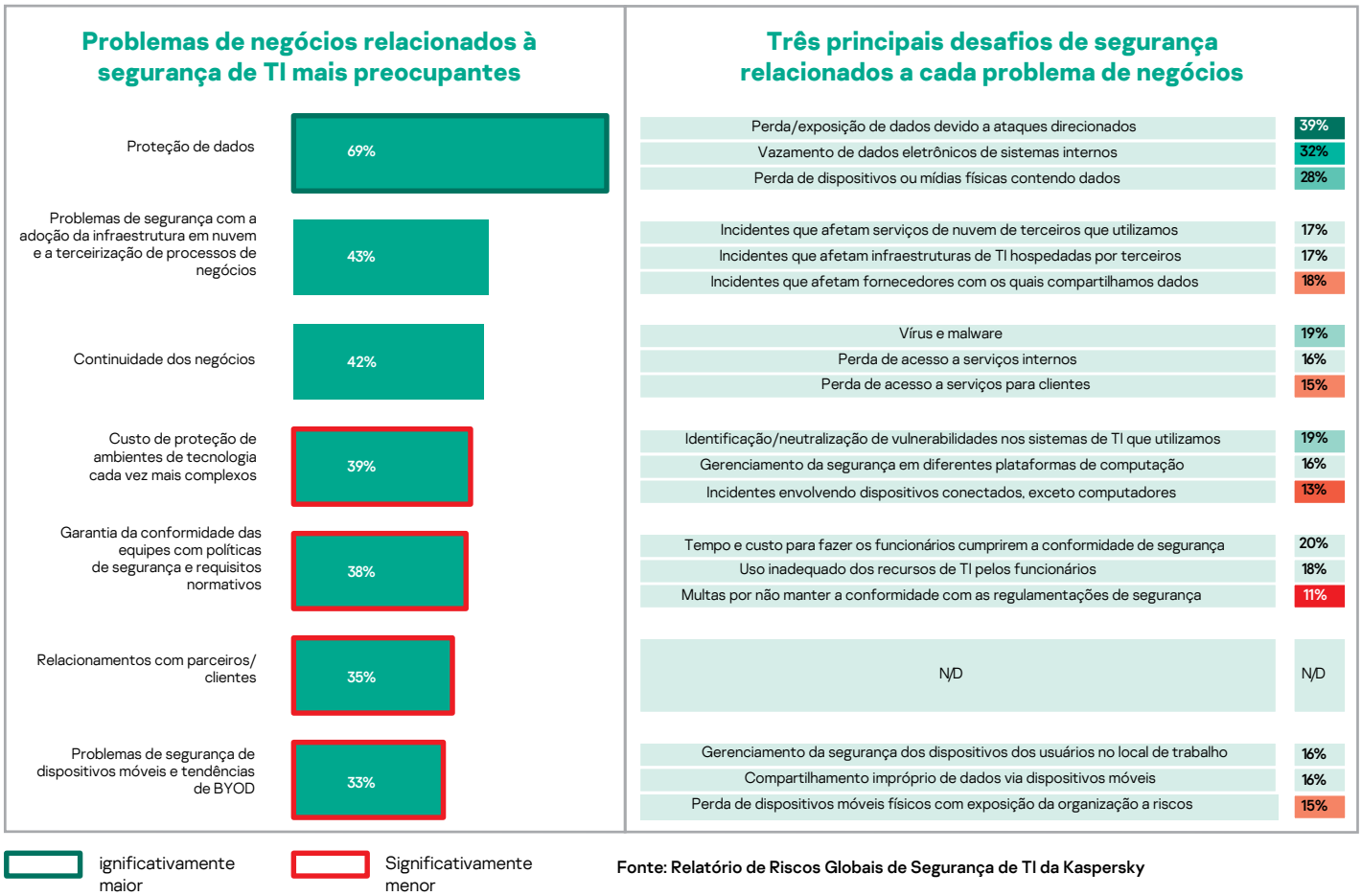
As ações humanas, tanto involuntárias quanto premeditadas, têm um papel significativo nas violações de dados pessoais. Mas a principal causa de incidentes de segurança relacionados a informações com identificação pessoal (PII, Personal Identifiable Information) continua sendo os ataques cibernéticos que, além de aumentar em volume, também mudam continuamente. Por isso a cibersegurança tem uma importância tão grande na estratégia de proteção de dados e prevenção de violações.

69% dos profissionais de TI dizem que a proteção de dados é sua maior preocupação, e 38% declaram que a garantia de conformidade das equipes com as políticas de segurança e os requisitos normativos é uma questão.

Quando consideramos que, 24% das empresas registraram perda, vazamento ou exposição de dados em decorrência de um ataque de malware[3], é fácil entender por que uma estratégia de cibersegurança eficiente
tem um papel de suporte tão importante na conformidade com a LGPD e na redução geral de riscos.

E um dos melhores lugares para começar a reforçar as defesas da TI corporativa é o endpoint. Descubra o porquê.

Principais preocupações de TI



Fonte: Relatório de Riscos Globais de Segurança de TI da Kaspersky

3. Relatório de Riscos Globais de Segurança de TI da Kaspersky

52% das empresas dizem que a falta de cuidado dos usuários finais é o maior ponto fraco de sua estratégia de segurança de TI[6].

Começando pelo endpoint

Quando se trata de reforçar a segurança de TI geral e melhorar a estratégia de proteção de dados, um ótimo lugar para começar é a proteção dos endpoints. Essa área da defesa corporativa pode ser aprimorada imediatamente, sem afetar ou depender do andamento de outros processos novos.

- Os endpoints continuam sendo o principal alvo da maioria dos ataques cibernéticos de hoje, e o e-mail é o maior vetor de malware nas empresas[4].
- Eles podem se tornar uma "vitrine" dos dados sigilosos que sua empresa processa, mesmo que os próprios dados estejam localizados em um servidor remoto.
- Sendo o principal elemento básico de sua rede de TI, os endpoints do mesmo local devem ser monitorados para garantir alertas rápidos de atividade suspeita. Mesmo os endpoints que não estão diretamente envolvidos no processamento de dados pessoais podem representar uma ameaça importante quando conectados à mesma rede, pois os ataques de malware podem se propagar, comprometendo toda a infraestrutura de processamento de dados.

Neste ambiente, as taxas de detecção são realmente importantes. Com mais de 300.000 novas variações de malware detectadas a cada dia, até uma diferença de 0,9% na capacidade de detectar ameaças pode se traduzir em centenas de milhares de unidades de malware no decorrer de um ano. E, como os malwares mais avançados normalmente estão entre os últimos 1-2% dos ataques, essa parcela extra de detecção pode fazer a diferença entre enfrentar um ataque cibernético e ele derrubar a sua empresa, especialmente no caso de empresas menores.

As soluções de detecção nos endpoints mais eficazes não param em um só nível de prevenção e detecção. Elas usam várias camadas de tecnologias da última geração, capazes de detectar, bloquear e atenuar até as ameaças desconhecidas mais sofisticadas.

O Kaspersky Endpoint Security for Business combina a segurança mais testada e mais premiada do mundo[5] com várias camadas de tecnologias da última geração para proteger os endpoints da empresa de todos os tipos de ameaças. Nosso mecanismo de comportamento é acionado pela exclusiva tecnologia de Machine Learning dinâmico e pela detecção de ameaças assistida em nuvem a fim de aliviar ameaças conhecidas, desconhecidas e avançadas, além de ataques em desenvolvimento, por exemplo, de ransomware, que representam uma ameaça direta à integridade e disponibilidade de dados pessoais.

Bloquear antes do carregamento

A prevenção de um ataque antes que ele possa causar danos é um aspecto importante do fortalecimento e da resiliência do sistema. Assim, descobrir e resolver vulnerabilidades e lacunas nos principais aplicativo de software pode ajudar a evitar que cibercriminosos explorem softwares corporativos amplamente usados para acessar e roubar dados pessoais.

Por que isso é importante? Pense: ataques de phishing, ransomware, anexos maliciosos, spyware são apenas alguns exemplos de ataques cibernéticos de infração de dados que exploram a suposição de que os usuários finais vão clicar sem pensar. Um e-mail disfarçado com um anexo convincente é o que basta para causar uma violação de dados grave.

O **Sistema de Prevenção de Invasões Baseado em Host** (HIPS) do Kaspersky Endpoint Security for Business fornece uma camada adicional de resiliência. Ele detecta e bloqueia atividades de programas indesejados ou maliciosos em tempo real, sem afetar o desempenho de aplicativos legítimos. Com base nas informações de ameaças mais recentes baseadas na nuvem, os aplicativos recebem uma de quatro categorias de confiança, que determinam o tipo de acesso que têm a elementos sigilosos do sistema. Da perspectiva da LGPD, isso pode proporcionar segurança adicional, restringindo o acesso a arquivos/diretórios selecionados por aplicativos com baixo nível de confiança.

O Kaspersky Vulnerability and Patch Management (incluído no Kaspersky Endpoint Security for Business Advanced) adiciona uma camada extra de segurança a suas defesas. Ele localiza e corrige aplicativos vulneráveis antes que seja possível explorar qualquer vulnerabilidade. Como possibilita a automação, as equipes de TI são poupadas da carga operacional de implementar correções rapidamente; o agendamento permite enviar correções não urgentes por push fora do horário de expediente, reduzindo a pressão sobre a infraestrutura.

Para proporcionar a verdadeira proteção em vários níveis, a tecnologia de Prevenção contra Exploits baseada em endpoints da Kaspersky é capaz de reduzir até exploits de "dia zero" antes desconhecidas, aproveitando as funcionalidades do mecanismo de comportamento para cobrir a maior variedade de tipos de exploits.

4. Relatório das Investigações sobre Violações de Dados da Verizon
5. https://www.kaspersky.com/top3
6. Relatório de Riscos Globais de Segurança de TI da Kaspersky
7. Relatório de Riscos Globais de Segurança de TI da Kaspersky
8. Boletim de Segurança da Kaspersky: História do Ano

- 8% das empresas já sofreram perdas de dados devido à perda de dispositivos ou mídias removíveis.
- 16% tiveram dados expostos por causa de dispositivos móveis perdidos.
- 15% das empresas tiveram dados compartilhados inadequadamente via dispositivos móveis.[13]

Se você não consegue proteger, não colete; armazene

Os endpoints são o lugar em que dados pessoais e pessoas se encontram, e os riscos associados precisam ser reduzidos. Mas, mesmo depois que o número de funcionários confiáveis que podem lidar com PII é reduzido (de acordo com os processos alinhados com a LGPD), ainda há riscos associados ao local e à maneira como os dados são armazenados. Para ter uma segurança mais sólida e uma visibilidade melhor, são atribuídas instalações de armazenamento regulamentadas (como servidores de arquivos ou armazenamentos conectados), sujeitas a políticas de acesso rígidas e monitoramento contínuo. Infelizmente, essa função extremamente sigilosa as torna alvos lucrativos para ladrões de dados, enfatizando a necessidade de segurança eficiente.

O **Kaspersky Security for File Servers** (disponível como parte do Kaspersky Endpoint Security e do Kaspersky Total Security for Business) e o **Kaspersky Security for Storage** oferecem proteção abrangente de armazenamentos de dados regulamentados. Além da proteção eficiente em vários níveis, essas soluções foram criadas considerando especificamente as necessidades de servidores e armazenamentos de dados, garantindo o menor impacto possível sobre seu desempenho e estabilidade, independentemente da carga de trabalho. Eles também incluem um mecanismo Anti-Cryptor[9] exclusivo, que bloqueia os efeitos de ransomware executado remotamente. Esse tipo de ameaça pode causar danos permanentes importantes, se executado em uma máquina com acesso de rede a armazenamentos ou servidores que processam dados de PII.

Segurança dos gargalos

Os servidores proxy e de e-mail são dois gateways pelos quais os ataques cibernéticos podem chegar à rede de TI corporativa, ou por onde os dados pessoais podem sair. Mesmos dados enviados acidentalmente por conta de falha humana constituem uma violação. A segurança desses dois gargalos no perímetro de defesa corporativa é crucial.

O Kaspersky Security for Mail Servers e o Kaspersky Security for Internet Gateways[10] ajudam a reduzir esses riscos consideravelmente, interrompendo até 95% das ameaças recebidas antes que elas alcancem o endpoint, eliminando o fator humano e os ataques que visam endpoints. Além disso, o risco que a entrada ou saída de dados pessoais dos sistemas representam pode ser administrado impedindo que determinados tipos de arquivos entrem ou saiam.

Dispositivos móveis – alvos em movimento

Graças a sua adequação para armazenamento, transferência e compartilhamento de dados, os dispositivos móveis têm uma função importante no processamento de dados pessoais e, assim como outras tecnologias, deve-se prestar atenção especificamente a sua proteção.

O Kaspersky Security for Mobile faz parte do Kaspersky Endpoint Security for Business, combinando proteção eficiente contra ameaças com medidas de segurança de dados, como criptografia e separação de dados corporativos, além de ferramentas de gerenciamento remoto.

Tudo isso cria uma base sólida para garantir o uso de dispositivos móveis, incluindo os que fazem parte da cadeia de processamento de PII.

O lado positivo da nuvem

43% das empresas dizem que os problemas de segurança relacionados à infraestrutura em nuvem são sua maior preocupação com a segurança de TI.[11] O Kaspersky Hybrid Cloud Security facilita a proteção de cargas de processamento de dados – inclusive PII – independentemente de seu estado físico/virtual ou de sua localização (no local/na nuvem). Ele proporciona a mesma segurança abrangente para a infraestrutura com virtualização habilitada, servidores e áreas de trabalho virtuais. A maioria das camadas de segurança apresentada em aplicativos para cargas de trabalho físicas também está disponível, em formatos criados especificamente para sistemas virtuais.

Treinamento – prevenido e equipado

A LGPD exige que se promova a conscientização dos empregados e colaboradores em relação à privacidade e segurança de dados, incluindo, quando apropriado, treinamentos para garantir as práticas recomendadas e os padrões de proteção de dados. Embora os aspectos do manuseio de dados relacionados a processos, como proporcionalidade, finalidade, *privacy by design* formarão o pilar do alinhamento com a LGPD para a maioria das empresas, a conscientização mais ampla sobre cibersegurança, ameaças de e-mail e outras ameaças on-line à segurança de dados também tem um papel muito importante.

O treinamento em conscientização sobre segurança da Kaspersky dá suporte à promoção e conscientização sobre práticas recomendadas de proteção de dados no local de trabalho usando cenários em forma de jogos para facilitar o entendimento de ameaças cibernéticas e sua prevenção. Ao reduzir os riscos de dados associados à falha humana, as empresas podem estender sua conformidade além das caixas de seleção e promover a conscientização geral e práticas mais seguras.[12]

9. O Kaspersky Security for Storage dá suporte à funcionalidade Anti-Cryptor somente para armazenamentos conectados NetApp
10. Também disponível como parte do Kaspersky Total Security for Business
11. Relatório de Riscos Globais de Segurança de TI da Kaspersky
12. A oferta da Kaspersky complementa o treinamento relacionado ao processo e não o substitui
13. Relatório de Riscos Globais de Segurança de TI da Kaspersky

Compreensão dos riscos

O artigo 46 da LGPD exige a adoção de medidas de segurança técnicas e administrativas adequadas à proteção de dados pessoais do acesso não autorizado e outros processamentos impróprios ou ilegais.

Da perspectiva de cibersegurança, isso pode incluir a avaliação de qualquer software de processamento de dados em relação a vulnerabilidades ou riscos associados com a forma como ele foi implementado. Quando o processamento de dados pessoais é um elemento crítico dos processos de negócios, a visualização de toda a infraestrutura de TI como uma "instalação de processamento de dados pessoais" unificada é uma abordagem útil para a avaliação de riscos bem-sucedida. A experiência em cibersegurança necessária para executar essa tarefa raramente está disponível em equipes internas.

Assim, para conseguir isso, muitas organizações trabalham com especialistas em cibersegurança terceirizados.

Os Serviços de avaliação de segurança Kaspersky podem ajudar com a avaliação de segurança de aplicativos, verificando se o software usado no processamento de dados é vulnerável a irregularidades e exploração. Os especialistas da Kaspersky também podem realizar testes de penetração para descobrir os pontos fracos de sua rede de TI e fornecer recomendações para reduzi-los. Isso ajuda a garantir que os sistemas e processos sejam ajustados para melhorar a segurança, facilitando avaliação de impacto sobre a proteção de dados.

A cibersegurança dá suporte à LGPD

Em seu cerne, a LGPD foi criada para proteger e possibilitar a privacidade de dados em um mundo onde a tecnologia transformou a maneira como informações pessoais são coletadas, compartilhadas e armazenadas.

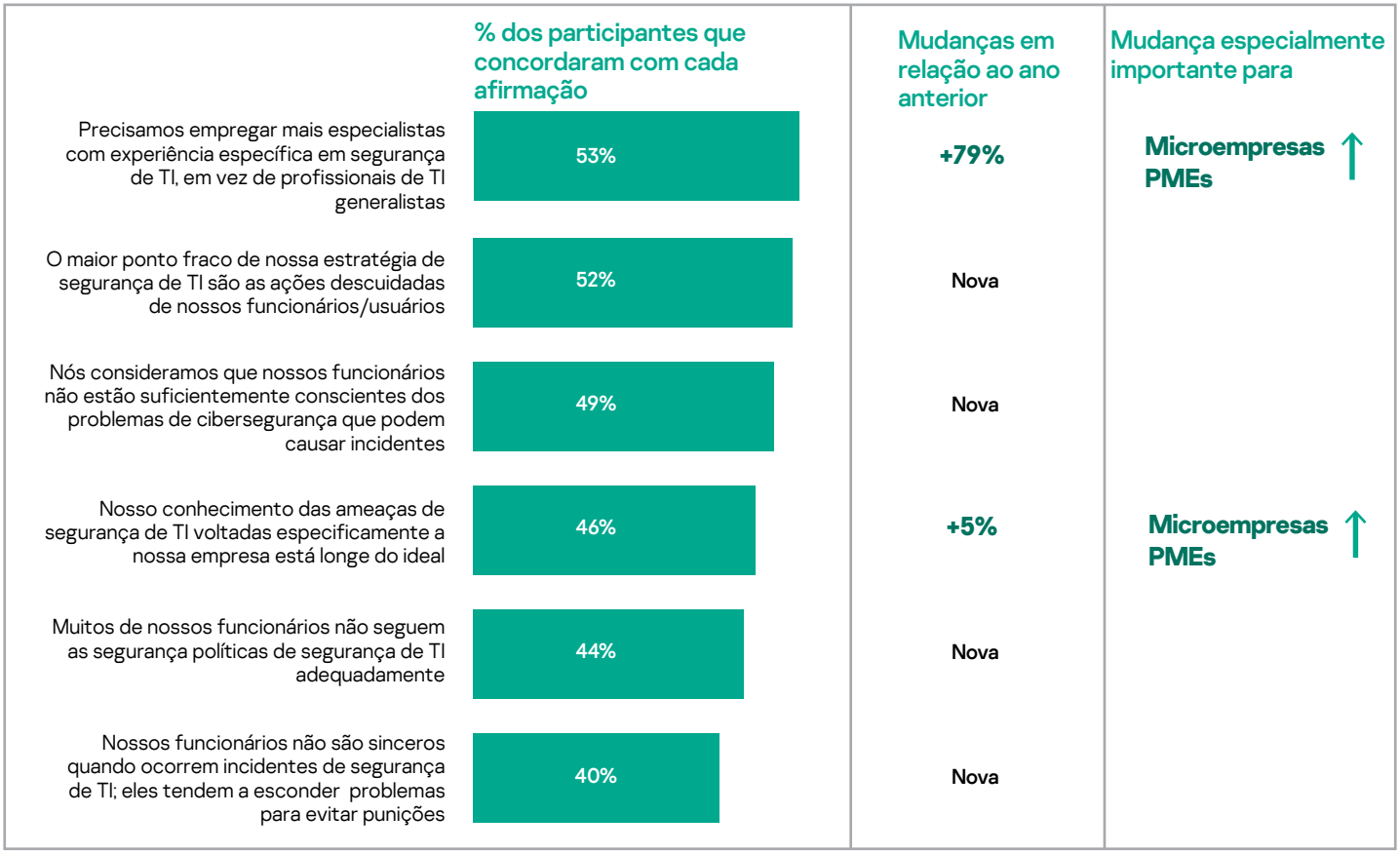
Embora a LGPD tenha entrado em vigor em 18 de Setembro de 2020, o longo período de introdução permitiu que as organizações fizessem um levantamento de sua abordagem de processamento de dados e implementassem mudanças nas tecnologias que usam e nos tipos de dados que coletam e gerenciam.

Para a maioria das organizações, a LGPD apresentou uma oportunidade de analisar e melhorar o processamento de dados e, por extensão, a cibersegurança. Por si só, essas são ótimas notícias para os especialistas em cibersegurança, que reclamam do descuido das empresas em relação à segurança e aos processos que utilizam para proteger seus dados e sistemas. A LGPD oferece às empresas uma ótima oportunidade de analisar sua conduta de cibersegurança da perspectiva de segurança dos dados. No final, o que serve à segurança de dados pessoais também pode servir à segurança de muitos outros aspectos dos negócios de sua empresa. Embora não garanta a conformidade com a LGPD, o portfólio de soluções da Kaspersky está à disposição para reduzir os riscos de processamento de PII de sua empresa, além de todas as outras ameaças cibernéticas que você enfrenta.

Demais, por ora?! O caso da educação sobre segurança

Mais de metade das empresas concordou que as ações de funcionários descuidados foram seu maior problema de segurança de TI. É fundamental instruir as equipes sobre as ameaças que existem e como se proteger delas!

Isso é especialmente verdadeiro no caso de empresas maiores, significativamente mais propensas a concordar com essas afirmações.



Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com/
Portal de inteligência de ameaças: opentip.kaspersky.com

www.kaspersky.com.br

kaspersky BRING ON THE FUTURE