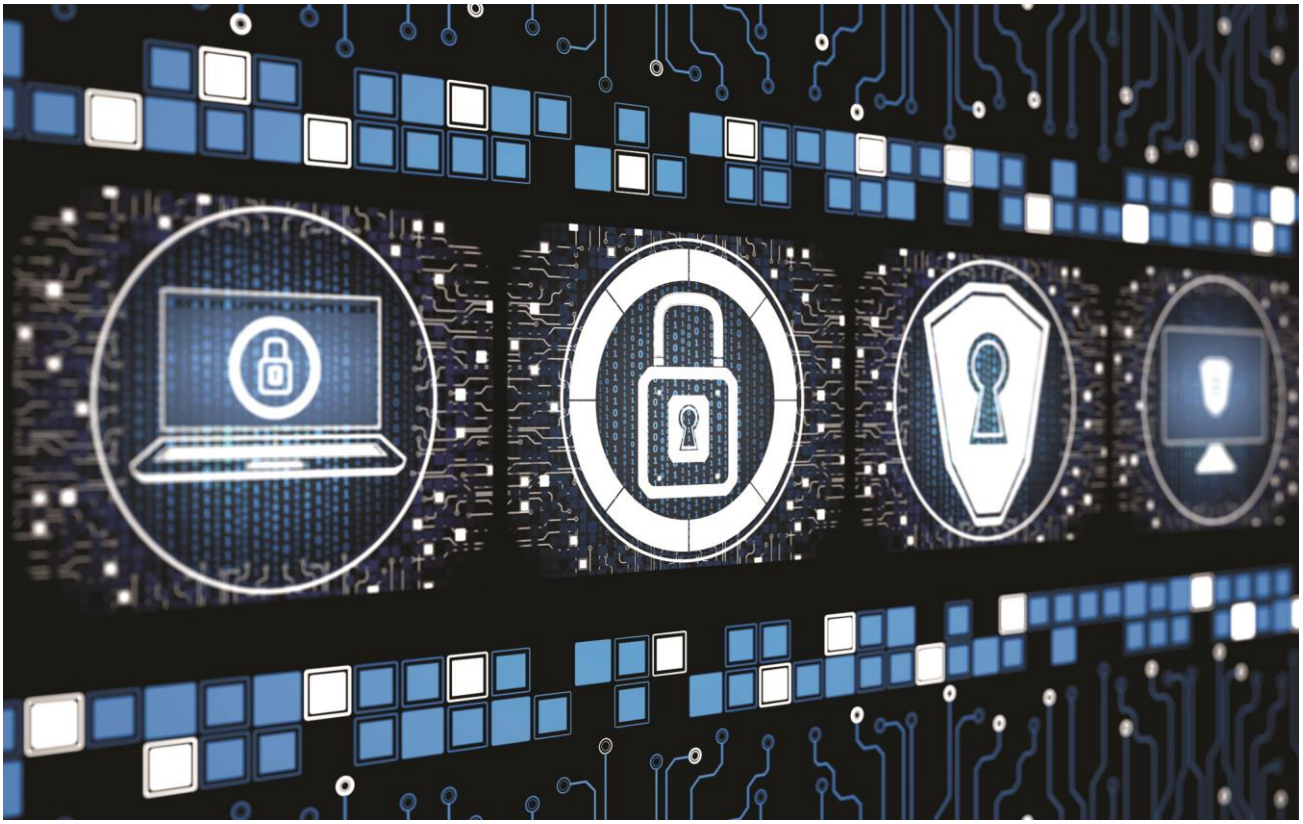
THALES

Ponemon INSTITUTE



Tendências em criptografia e gestão de chaves: Brasil

Patrocinado pela Thales e-Security

Realização independente pelo Ponemon Institute LLC

Data de publicação: abril de 2016

Relatório da pesquisa do Ponemon Institute©

Tendências em criptografia e gestão de chaves: Brasil

Tendências em criptografia e gestão de chaves: Brasil

Ponemon Institute, abril de 2016

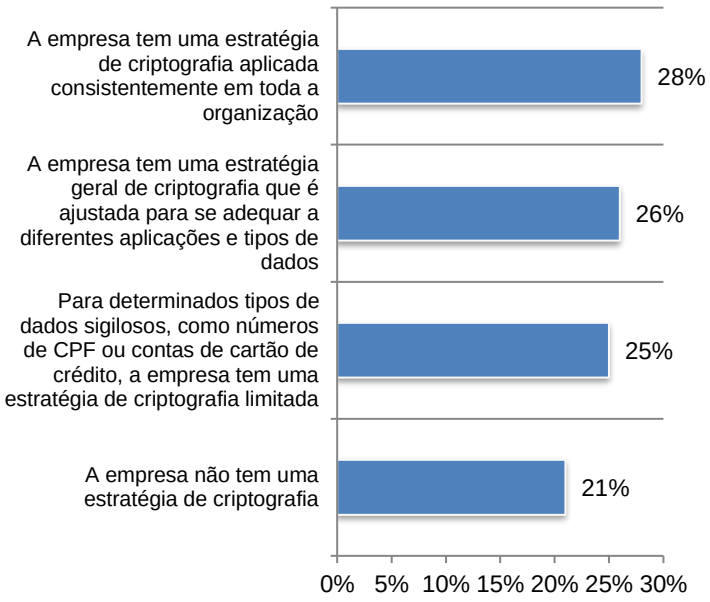
Parte 1. Resumo executivo

O Ponemon Institute tem o prazer de apresentar os resultados do estudo sobre *Tendências em criptografia e gestão de chaves: Brasil,* patrocinado pela Thales e-Security*.* Entrevistamos 460 pessoas no Brasil. A finalidade desta pesquisa é examinar o uso da criptografia e o impacto dessa tecnologia na postura de segurança das organizações. O primeiro estudo sobre tendências de criptografia foi realizado em 2005, com uma amostragem de entrevistados dos EUA. Desde então, temos expandido o escopo da pesquisa para incluir entrevistados de todas as regiões do mundo.

Grandes violações e ataques cibernéticos fizeram crescer a urgência das empresas em aprimorar sua postura de segurança. De fato, 79% das organizações representadas neste estudo adotam algum tipo de estratégia de criptografia, como mostra a Figura 1. Acreditamos que essa e outras conclusões demonstram a importância da criptografia e do gerenciamento de chaves no alcance de uma forte postura de segurança.

Veja a seguir um resumo dos nossos principais resultados. A próxima seção deste relatório fornece mais detalhes sobre cada um dos principais resultados listados abaixo.

Figura 1. O que melhor descreve a estratégia de criptografia da sua organização?



- **As operações de TI e as linhas de negócios têm a maior influência no direcionamento das estratégias de criptografia.** Embora a responsabilidade pela estratégia de criptografia esteja distribuída por toda a organização,
as operações de TI (31% dos entrevistados) e as linhas de negócios (29%) têm a maior influência. 26% dos entrevistados afirmam que não há uma única função que seja responsável pela sua estratégia de criptografia.

- **Erros de funcionários são a ameaça mais significativa a dados sigilosos.** A ameaça mais significativa que resulta na exposição de dados sigilosos ou confidenciais são os erros de funcionários, de acordo com 43% dos entrevistados. 32% dos entrevistados afirmam que a espionagem governamental é a principal ameaça. Falhas de sistema ou processo e prestadores de serviço terceirizados são considerados a principal ameaça por 28% dos entrevistados.

- **A conformidade com regulamentações e requisitos externos de privacidade ou segurança de dados é o principal fator da criptografia.** A Figura 5 apresenta oito fatores para a implantação da criptografia. 63% dos entrevistados relatam que a conformidade de privacidade e segurança é o principal fator. Outros importantes fatores são a proteção da propriedade intelectual (61% dos entrevistados) e a proteção de informações pessoais dos clientes.

- **A implantação inicial da tecnologia de criptografia e a descoberta de onde os dados sigilosos estão localizados na organização são os maiores desafios.** 57% dos entrevistados afirmam que o maior desafio é a implantação inicial da criptografia, e 47% deles afirmam que descobrir onde residem os dados sigilosos na organização é o desafio número 1.

- **Não há uma tecnologia de criptografia única dominante, pois as organizações têm necessidades muito distintas**. Comunicação pela Internet, gateway na nuvem e bancos de dados são frequentemente submetidos a uma extensiva criptografia. Em contraste, repositórios de big data têm menos probabilidade de serem submetidos à criptografia extensiva ou são parcialmente criptografados.

- **Determinados recursos de criptografia são considerados mais críticos do que outros.** Pedimos que os entrevistados classificassem os recursos de tecnologia de criptografia considerados mais importantes para a postura de segurança da organização deles. De acordo com os resultados, desempenho e latência do sistema, o suporte a algoritmos emergentes (por exemplo, ECC), gerenciamento de chaves, aplicação de políticas e suporte à implantação local e na nuvem são considerados os recursos mais importantes das soluções de tecnologia de criptografia.

- **Quais tipos de dados são criptografados com mais frequência?** Os dados de recursos humanos são o tipo com maior chance de receber criptografia, o que sugere que atualmente a criptografia alcançou um nível onde precisa ser adotada por empresas de todos os tipos. O tipo de dados com menos probabilidade de passar por criptografia são as informações de saúde.

- **Quão difícil é o gerenciamento de chaves?** Usando uma escala de 1 a 10, solicitamos que os entrevistados classificassem a "dificuldade" geral associada ao gerenciamento de chaves em sua organização, sendo 1 = impacto mínimo e 10 = impacto severo. 52% (24% + 28%) dos entrevistados atribuíram pontuações de 7 pontos ou mais, o que sugere um limiar de dificuldade bastante alto para as organizações representadas nesta pesquisa.

- **Por que o gerenciamento de chaves é difícil?** Os principais motivos são: falta de responsabilidade clara, ferramentas de gerenciamento de chaves inadequadas e falta de pessoal capacitado.

- **Quais são as chaves mais difíceis de gerenciar?** Os tipos de chaves considerados mais difíceis de gerenciar são: chaves pertencentes a aplicações (por exemplo, assinatura, autenticação, criptografia), chaves de sistemas de terceiros (por exemplo, parceiros, clientes, logon único, federação etc.) e chaves privadas para emissão de certificados.

- **Quais sistemas de gerenciamento de chaves estão atualmente em uso?** As empresas continuam usando uma variedade de sistemas de gerenciamento de chaves. Os sistemas mais comumente implantados são: processo manual (por exemplo, planilha, papel), política formal de gerenciamento de chaves (KMP) e infraestrutura formal de gerenciamento de chaves (KMI).

- **A importância de HSMs para uma estratégia de criptografia ou gerenciamento de chaves crescerá nos próximos 12 meses.** 38% dos entrevistados afirmam que HSMs são importantes, e 42% deles afirmam que serão importantes nos próximos 12 meses. Os três mais usados são SSL/TLS, criptografia no nível da aplicação e processamento de transações de pagamento. Nos próximos 12 meses, criptografia de banco de dados, emissão de credenciais de pagamento (por exemplo, dispositivos móveis e EMV) e processamento de transações de pagamento serão provavelmente os principais usos.

- **Muitas organizações estão transferindo dados confidenciais para a nuvem**. 60% dos entrevistados afirmam que suas organizações atualmente transferem dados sigilosos ou confidenciais para a nuvem (sejam ou não criptografados ou tornados ilegíveis por algum outro mecanismo) e 29% dos entrevistados planejam fazê-lo dentro dos próximos 12 a 24 meses**.** A maior parte dos entrevistados (54%) declara que é do provedor da nuvem a maior responsabilidade pela proteção dos dados sigilosos ou confidenciais transferidos para a nuvem.

- **As empresas usam criptografia ou outras formas de proteger dados em repouso?** 39% dos entrevistados dizem que utilizam a criptografia para proteger dados em repouso, enquanto 12% afirmam que os tornam ilegíveis por outros meios. 49% dos entrevistados afirmam que não protegem dados em repouso na nuvem.

- **Como os dados em repouso na nuvem são protegidos?** 44% dos entrevistados dizem que o provedor da nuvem criptografa os dados em repouso já na nuvem, enquanto 40% deles afirmam que os dados são criptografados antes de serem enviados para a nuvem. Somente 16% dizem que os dados em repouso na nuvem são criptografados pelas ferramentas da organização.

Parte 2. Principais resultados

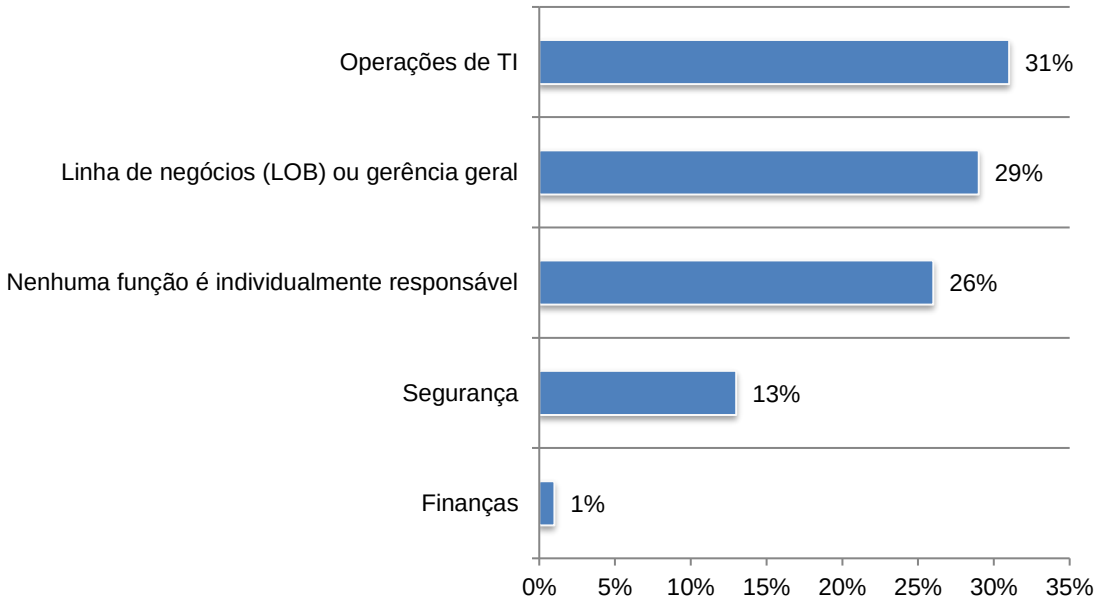
Nesta seção, apresentamos uma análise dos principais resultados. A íntegra dos resultados auditados é apresentada no anexo do relatório. Organizamos o relatório de acordo com os seguintes temas:

- Estratégia, ameaças e principais fatores
- Opções de implantação
- Atitudes relacionadas ao gerenciamento de chaves
- Importância dos módulos de segurança de hardware (HSMs)
- Alocação orçamentária
- Criptografia na nuvem

Estratégia, ameaças e principais fatores

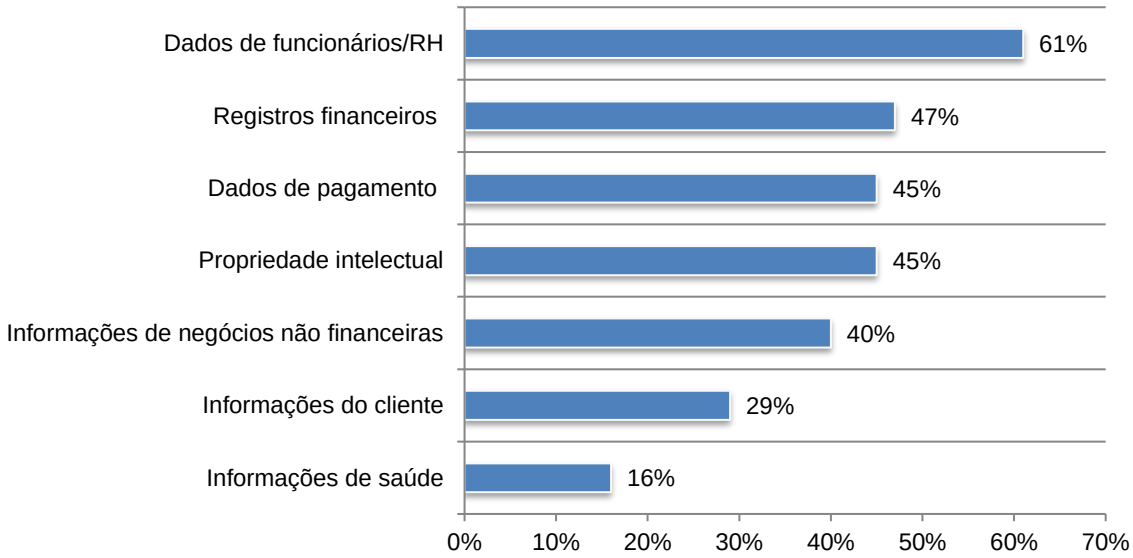
As operações de TI e as linhas de negócios têm a maior influência no direcionamento das estratégias de criptografia. Como mostra a Figura 2**,** embora a responsabilidade pela estratégia de criptografia esteja distribuída por toda a organização, as operações de TI (31% dos entrevistados) e as linhas de negócios (29%) têm a maior influência. 26% dos entrevistados afirmam que não há uma única função que seja responsável pela sua estratégia de criptografia.

Figura 2. Influência das operações de TI, das linhas de negócios e da segurança



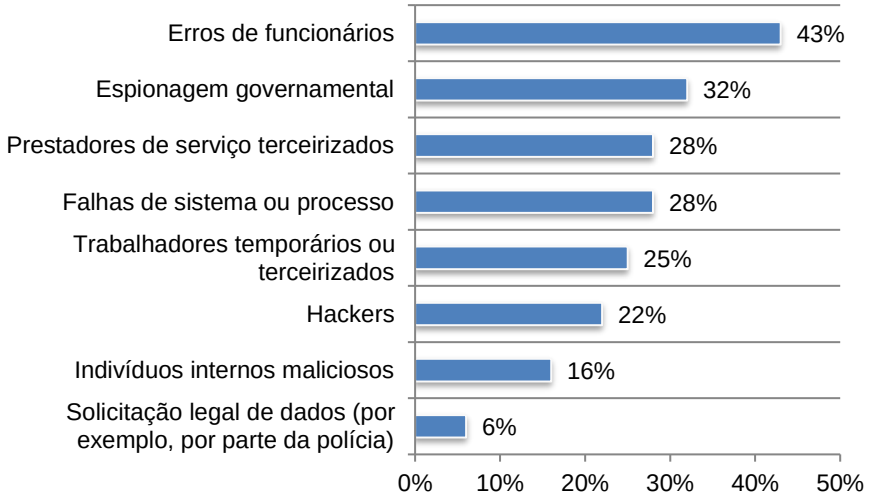
Quais tipos de dados são criptografados com mais frequência? A Figura 3 mostra uma lista de sete tipos de dados que são rotineiramente criptografados pelas organizações entrevistadas. Como é mostrado, os dados de recursos humanos são o tipo com maior chance de receber criptografia, o que sugere que atualmente a criptografia alcançou um nível onde precisa ser adotada por empresas de todos os tipos. O tipo de dados com menos probabilidade de passar por criptografia são as informações de saúde.

Figura 3. Tipos de dados rotineiramente criptografados
Mais de uma resposta permitida



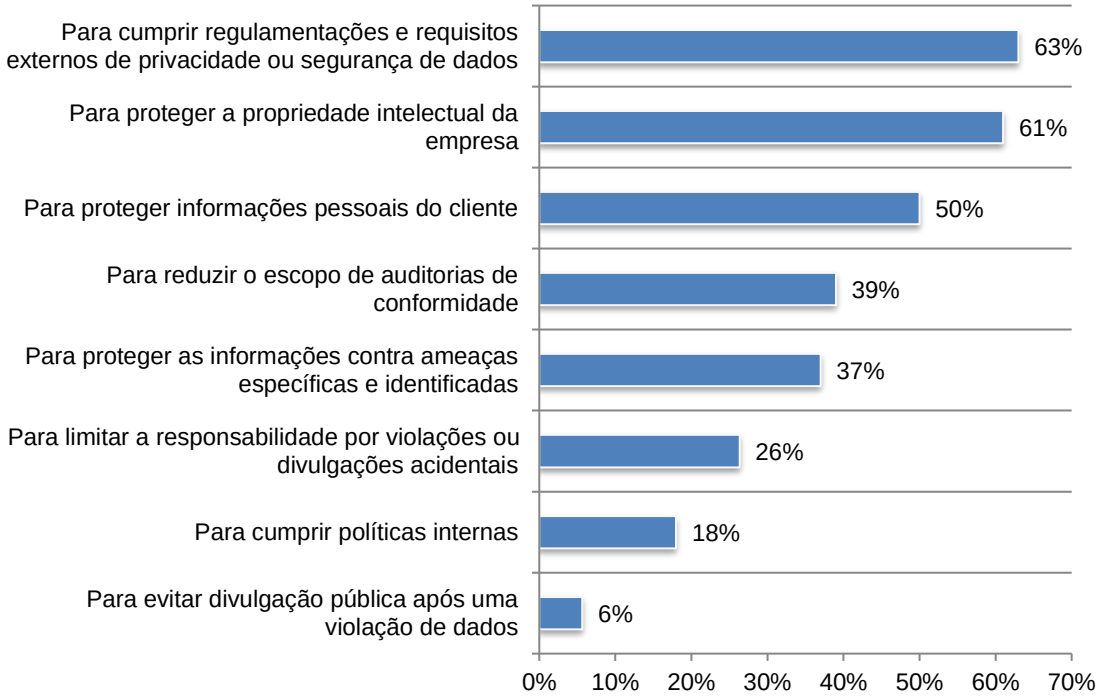
Erros de funcionários são a ameaça mais significativa a dados sigilosos. A Figura 4 revela que as ameaças mais significativas relacionadas à exposição de dados sigilosos ou confidenciais são os erros de funcionários, de acordo com 43% dos entrevistados. 32% dos entrevistados afirmam que a espionagem governamental é a principal ameaça. Falhas de sistema ou processo e prestadores de serviço terceirizados são considerados a principal ameaça por 28% dos entrevistados.

Figura 4. As principais ameaças que podem resultar na exposição de dados sigilosos ou confidenciais
Duas respostas permitidas



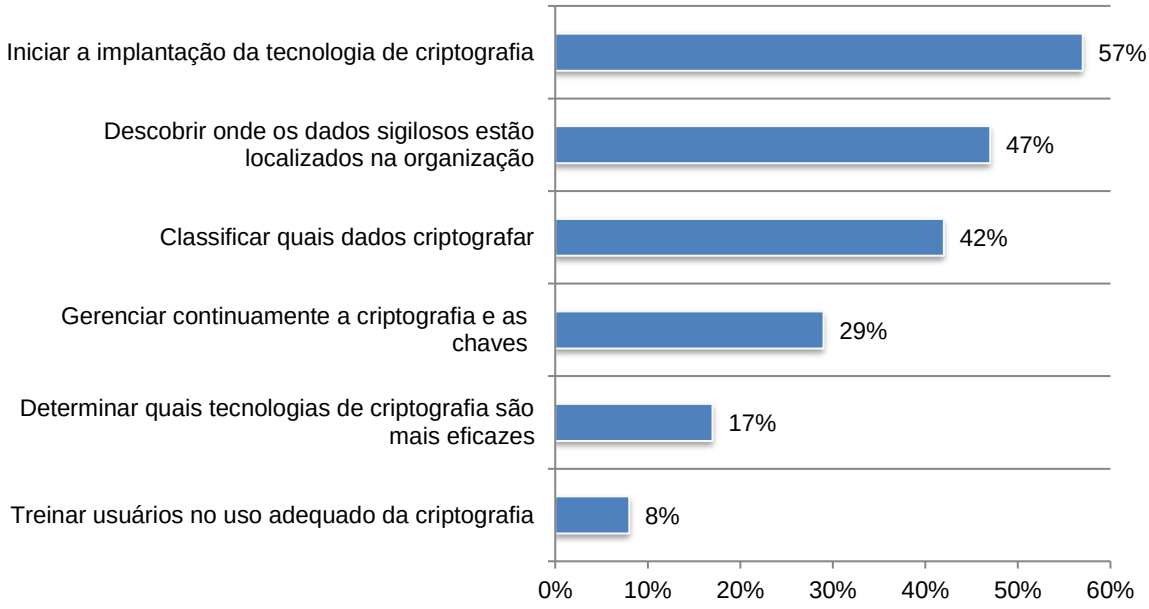
A conformidade com regulamentações e requisitos externos de privacidade ou segurança de dados é o principal fator da criptografia. A Figura 5 apresenta oito fatores para a implantação da criptografia. 63% dos entrevistados relatam que a conformidade de privacidade e segurança é o principal fator. Outros importantes fatores são a proteção da propriedade intelectual (61% dos entrevistados) e a proteção de informações pessoais dos clientes.

Figura 5. Os principais fatores para o uso de soluções de tecnologia de criptografia
Três respostas permitidas



A implantação inicial da tecnologia de criptografia e a descoberta de onde os dados sigilosos estão localizados na organização são os maiores desafios. A Figura 6 apresenta uma lista de seis desafios para uma organização executar efetivamente sua estratégia de criptografia de dados, em ordem decrescente de importância. 57% dos entrevistados afirmam que o maior desafio é a implantação inicial da criptografia, e 47% deles afirmam que descobrir onde residem os dados sigilosos na organização é o principal desafio.

Figura 6. Maiores desafios no planejamento e na execução de uma estratégia de criptografia de dados
Duas respostas permitidas

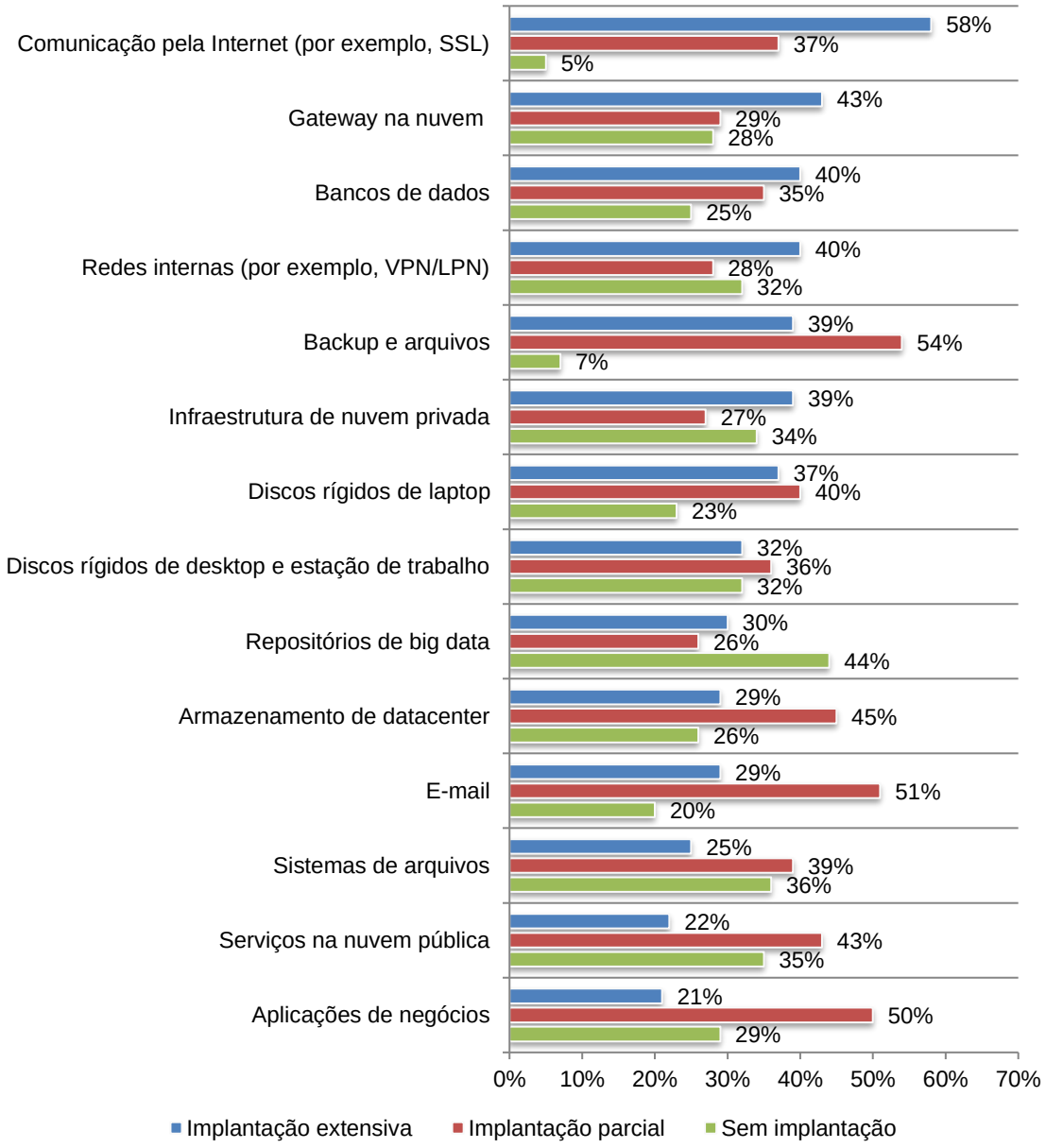


Opções de implantação

Não há uma tecnologia de criptografia única dominante nas organizações. Pedimos que os entrevistados indicassem se existem tecnologias de criptografia específicas implantadas amplamente ou apenas parcialmente em suas organizações. "Implantação extensiva" significa que a tecnologia de criptografia é implantada em toda a empresa. "Implantação parcial" significa que a tecnologia de criptografia é confinada ou limitada a uma finalidade específica (ou seja, solução pontual).

Conforme mostra a Figura 7, não há uma tecnologia única dominante, pois as organizações têm necessidades muito distintas. Comunicação pela Internet, gateway na nuvem e bancos de dados são frequentemente submetidos a uma extensiva criptografia. Em contraste, repositórios de big data têm menos probabilidade de serem submetidos à criptografia extensiva ou são parcialmente criptografados.

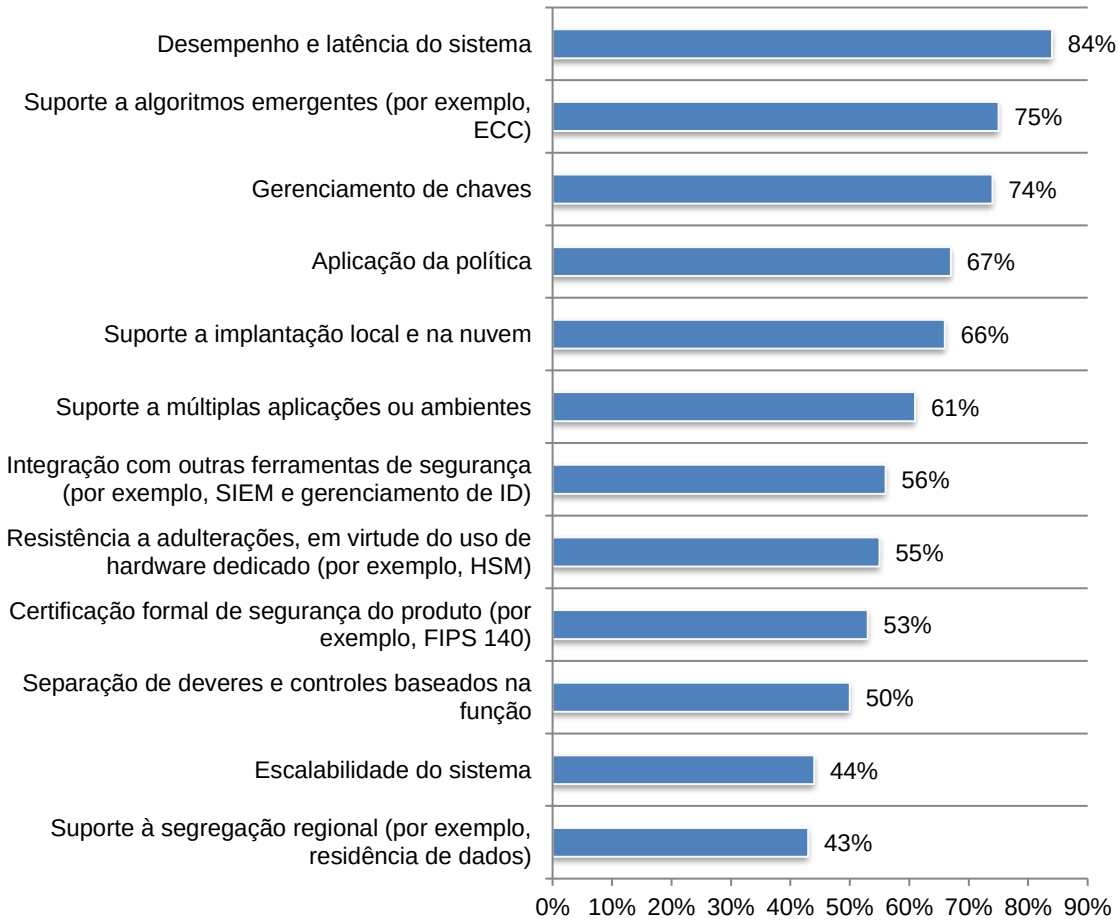
Figura 7. O uso de tecnologias de criptografia



Recursos de criptografia considerados mais importantes

Determinados recursos de criptografia são considerados mais críticos do que outros. A Figura 8 lista os recursos de tecnologia de criptografia. Cada percentual define a resposta "muito importante" (em uma escala de quatro pontos). Pedimos que os entrevistados classificassem os recursos de tecnologia de criptografia considerados mais importantes para a postura de segurança da organização deles. De acordo com os resultados, desempenho e latência do sistema, o suporte a algoritmos emergentes (por exemplo, ECC), gerenciamento de chaves, aplicação de políticas e suporte à implantação local e na nuvem são os recursos mais importantes da tecnologia de criptografia.

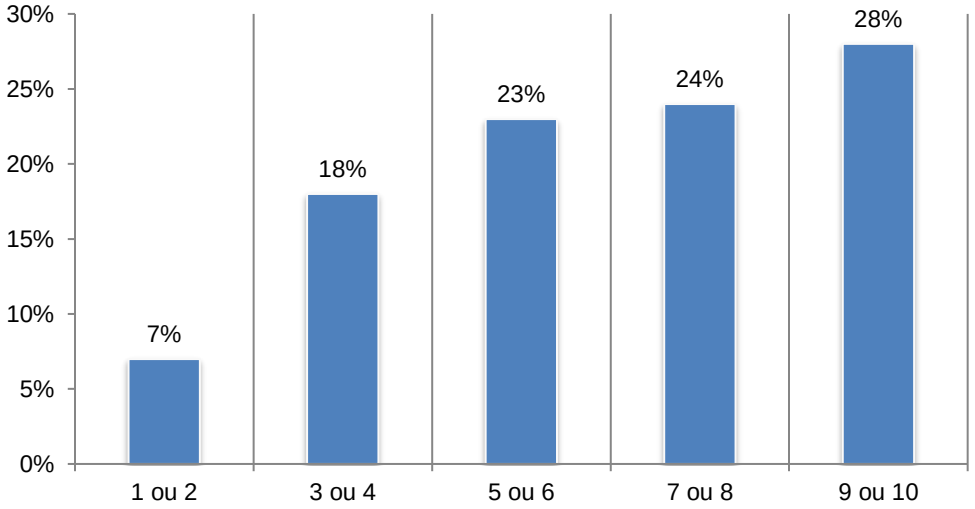
Figura 8. Recursos mais importantes das soluções de tecnologia de criptografia
Respostas "muito importante" e "importante" combinadas



Atitudes relacionadas ao gerenciamento de chaves

Quão difícil é o gerenciamento de chaves? Usando uma escala de 1 a 10, solicitamos que os entrevistados classificassem a "dificuldade" geral associada ao gerenciamento de chaves em sua organização, sendo 1 = impacto mínimo e 10 = impacto severo. A Figura 9 mostra 52% (24% + 28%) dos entrevistados atribuíram pontuações de 7 pontos ou mais, o que sugere um limiar de dificuldade bastante alto.

Figura 9. Quão difícil é o gerenciamento de chaves
1 = impacto mínimo até 10 = impacto severo

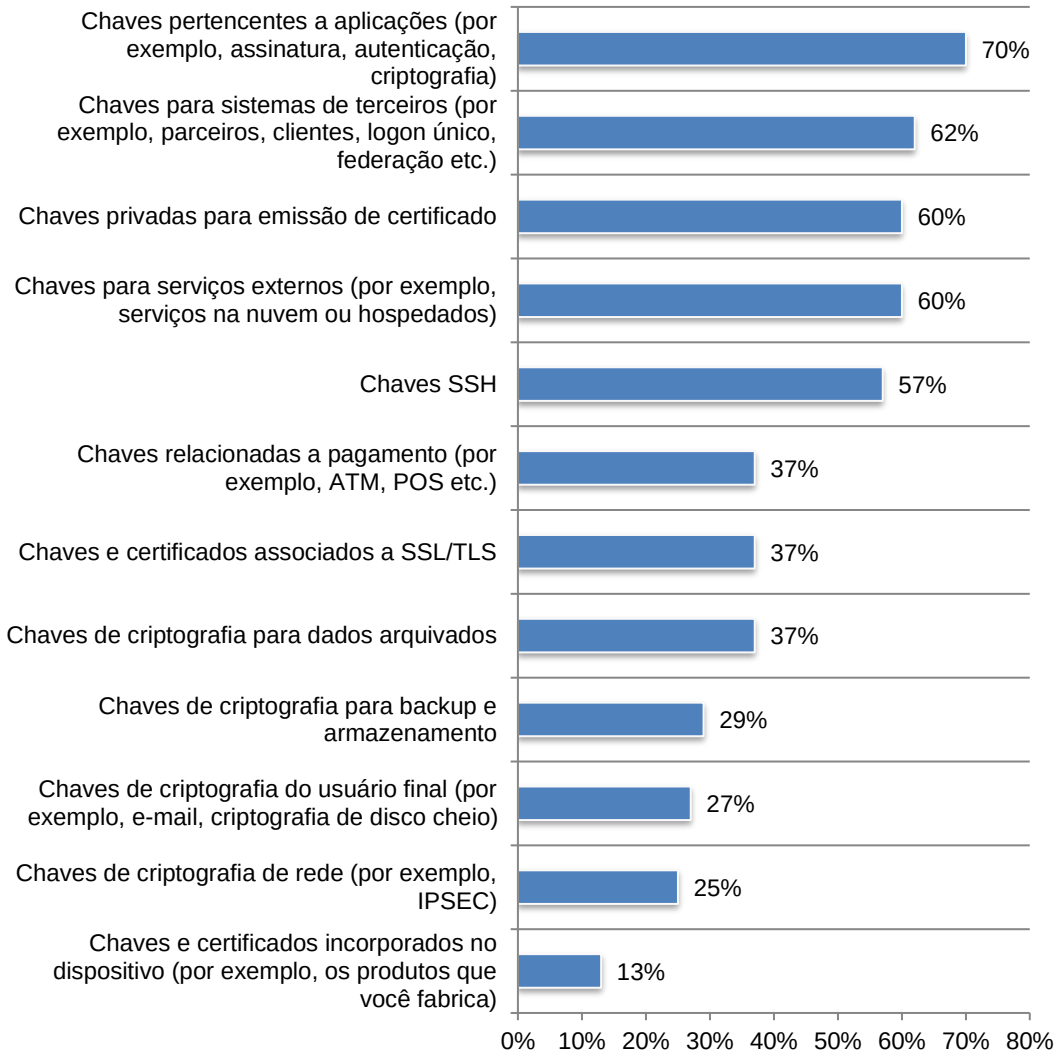


Por que o gerenciamento de chaves é difícil? A Figura 10 mostra os motivos pelos quais o gerenciamento de chaves é tão difícil. Os principais motivos são: falta de responsabilidade clara, ferramentas de gerenciamento de chaves inadequadas e falta de pessoal capacitado.

Figura 10. O que torna o gerenciamento de chaves tão difícil?
Três respostas permitidas

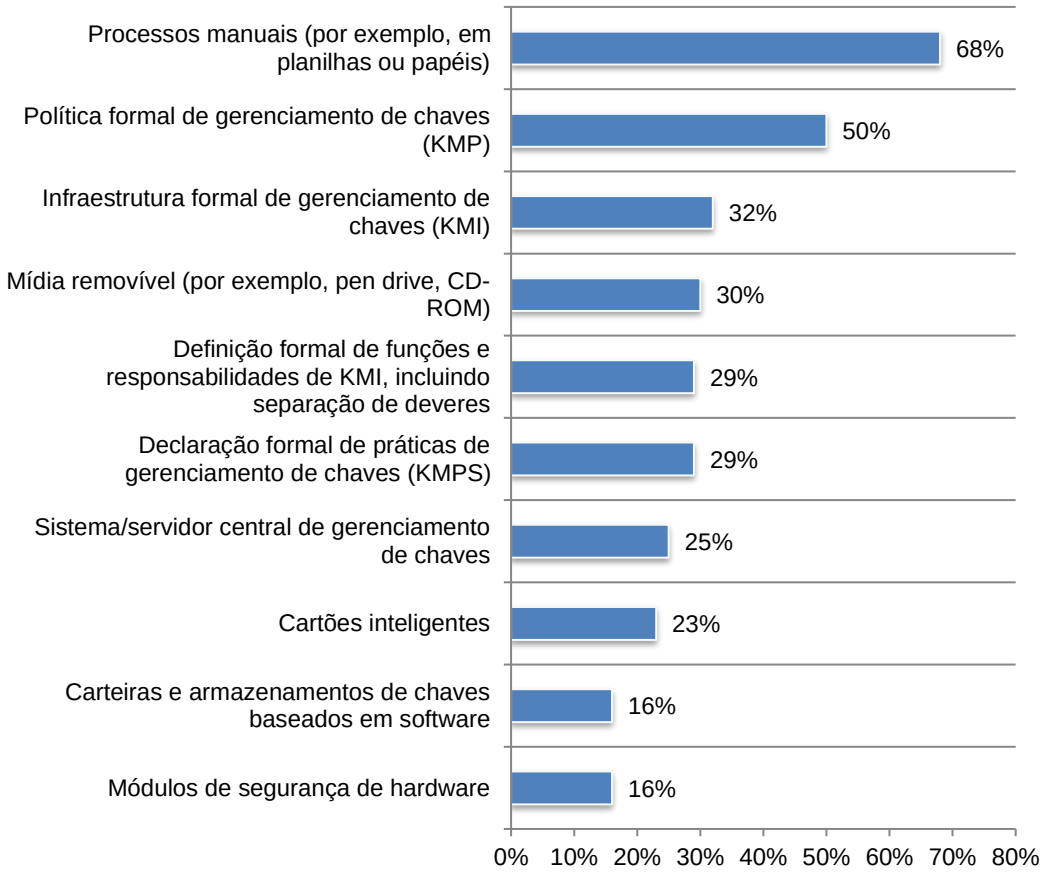
Quais são as chaves mais difíceis de gerenciar? De acordo com a Figura 11, os tipos de chaves considerados mais difíceis de gerenciar são: chaves pertencentes a aplicações (por exemplo, assinatura, autenticação, criptografia), chaves de sistemas de terceiros (por exemplo, parceiros, clientes, logon único, federação etc.) e chaves privadas para emissão de certificados.

Figura 11. Tipos de chaves mais difíceis de gerenciar
Respostas "muito difícil" e "difícil" combinadas



Conforme mostra a Figura 12, as empresas dos entrevistados continuam usando uma variedade de sistemas de gerenciamento de chaves. Os sistemas mais comumente implantados são: processo manual (por exemplo, planilha, papel), política formal de gerenciamento de chaves (KMP) e infraestrutura formal de gerenciamento de chaves (KMI).

Figura 12. Quais sistemas de gerenciamento de chaves sua organização usa atualmente?
Mais de uma resposta permitida

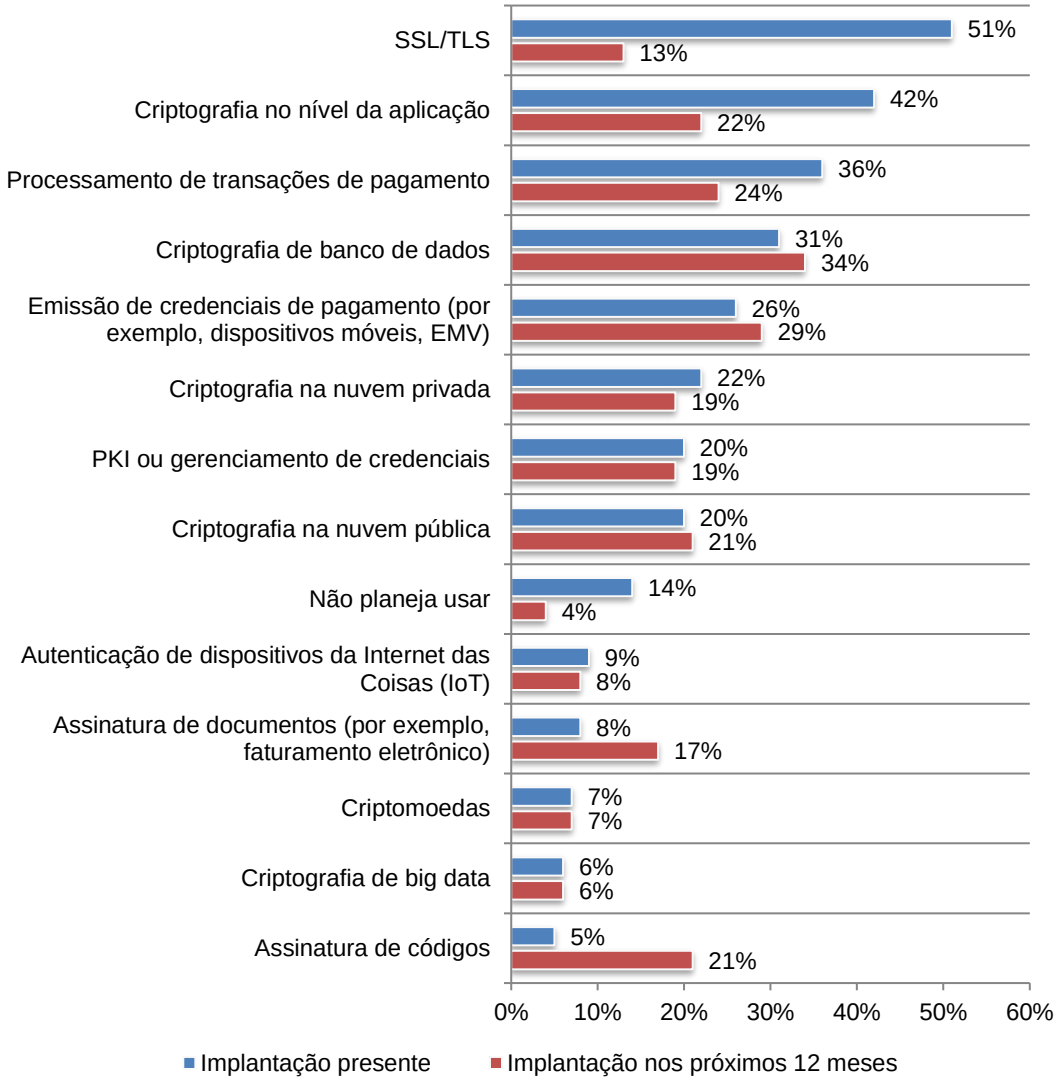


Importância dos módulos de segurança de hardware (HSMs)

A importância de HSMs para uma estratégia de criptografia ou gerenciamento de chaves crescerá nos próximos 12 meses. Perguntamos aos entrevistados de organizações que atualmente implantam HSMs qual é a importância deles para a estratégia de criptografia e gerenciamento de chaves da empresa. 38% dos entrevistados afirmam que HSMs são importantes, e 42% deles afirmam que serão importantes nos próximos 12 meses.

A Figura 13 resume os principais motivos ou casos de uso para a implantação de HSMs. Como vemos, as três opções mais usadas são SSL/TLS, criptografia no nível da aplicação e processamento de transações de pagamento. Esta figura mostra também as diferenças entre o uso atual de HSM e sua implantação nos próximos 12 meses. Nos próximos 12 meses, serão implantados criptografia de banco de dados, emissão de credenciais de pagamento (por exemplo, dispositivos móveis e EMV) e processamento de transações de pagamento.

Figura 13. Como os HSMs são ou serão implantados nos próximos 12 meses
Mais de uma resposta permitida



Alocação orçamentária

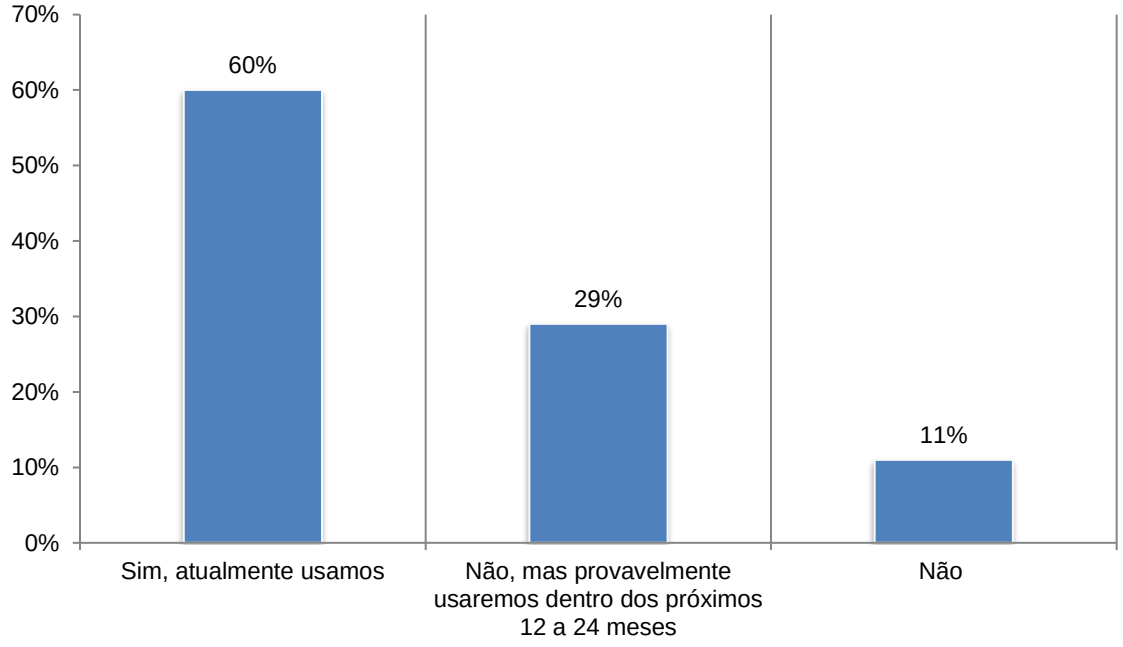
Como mostra a Tabela 1, em média, as organizações brasileiras gastam R$ 187 milhões em TI. Uma média de 8,8% é gasta em segurança da TI. Aproximadamente, 26,4% do orçamento médio de segurança de TI é alocado à proteção de dados, e 19% do orçamento de segurança de TI é gasto em criptografia.

Tabela 1. O orçamento de TI para segurança de TI, proteção de dados e criptografia	Valor extrapolado
Orçamento de TI da organização para 2015	R$ 187 milhões
Orçamento de TI para 2016 destinado a atividades de segurança de TI	8,8%
Orçamento de segurança de TI para 2016 destinado a atividades de proteção de dados	26,4%
Orçamento de segurança de TI para 2016 destinado a atividades de criptografia	19,0%

Criptografia na nuvem

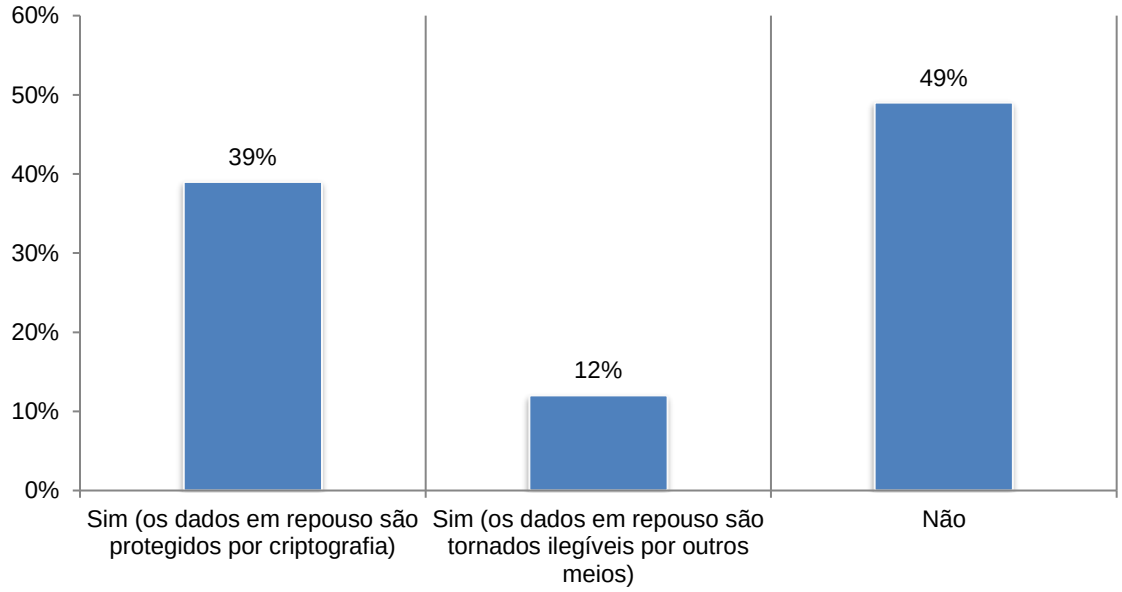
Muitas organizações estão transferindo dados confidenciais para a nuvem. Como vemos na Figura 14, 60% dos entrevistados afirmam que suas organizações atualmente transferem dados sigilosos ou confidenciais para a nuvem (sejam ou não criptografados ou tornados ilegíveis por algum outro mecanismo), e 29% dos entrevistados planejam fazê-lo dentro dos próximos 12 a 24 meses**.** A maior parte dos entrevistados (54%) declara que é do provedor da nuvem a maior responsabilidade pela proteção dos dados sigilosos ou confidenciais transferidos para a nuvem.

Figura 14. Atualmente, você transfere dados sigilosos ou confidenciais para a nuvem?



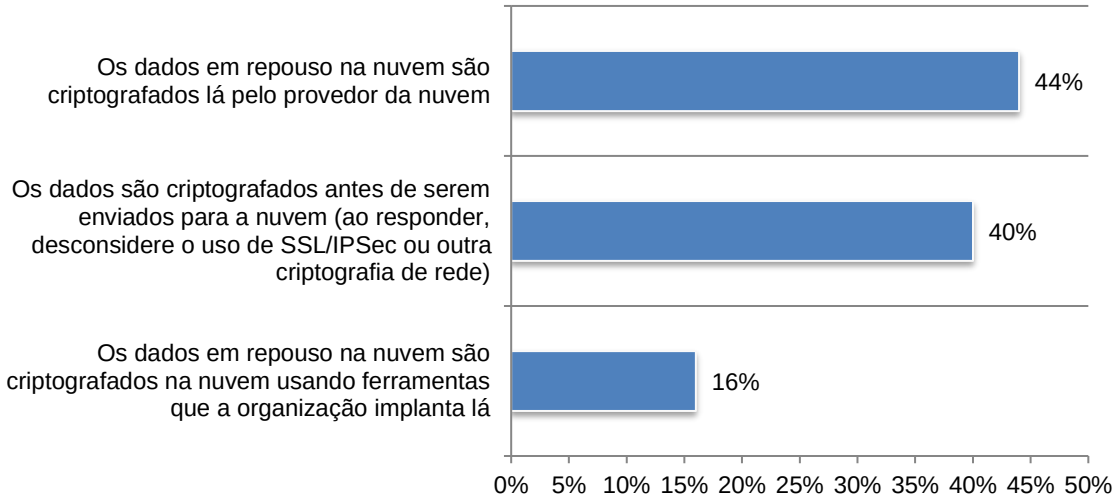
As empresas usam criptografia ou outras formas de proteger dados em repouso na nuvem? Segundo a Figura 15, 51% dos entrevistados dizem que utilizam a criptografia para proteger dados em repouso (39% dos entrevistados) ou utilizam outros meios para torná-los ilegíveis (12% dos entrevistados). 49% dos entrevistados afirmam que suas organizações não protegem dados em repouso na nuvem.

Figura 15. Sua organização protege dados em repouso na nuvem por meio de criptografia ou alguma outra forma de tornar os dados ilegíveis?



Como os dados em repouso na nuvem são protegidos? 44% dos entrevistados dizem que o provedor da nuvem criptografa os dados em repouso já na nuvem, como mostra a Figura 16. 40% deles afirmam que os dados são criptografados antes de serem enviados para a nuvem. Somente 16% dizem que os dados em repouso na nuvem são criptografados na nuvem usando ferramentas que a organização implanta lá.

Figura 16. Se os dados em repouso são protegidos por criptografia, como essa proteção é aplicada?



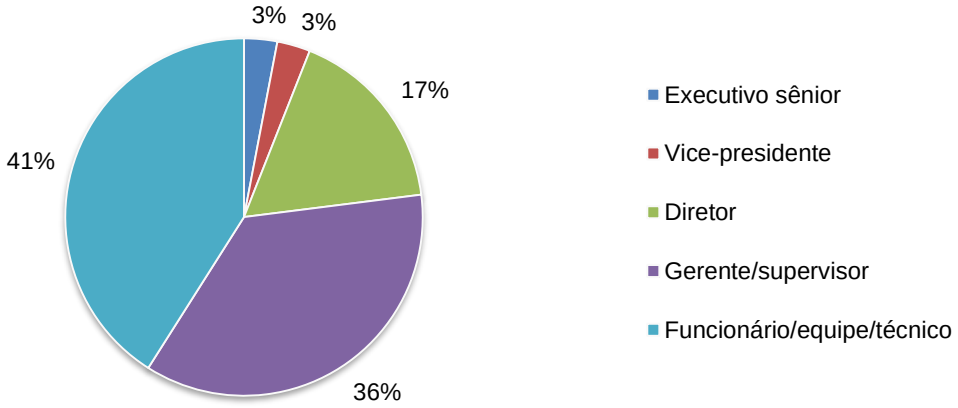
Anexo 1. Métodos e limitações

A Tabela 2 relata a resposta amostral no Brasil. A resposta amostral para este estudo foi conduzida durante um período de 49 dias, que se encerrou em fevereiro de 2016. Nossa consolidada estrutura de amostragem de profissionais no Brasil consistiu em 13.577 indivíduos que possuem credibilidade nos campos de TI ou segurança. Dessa estrutura de amostragem, capturamos 512 retornos, dos quais 52 foram rejeitados devido a problemas de confiabilidade. Nossa amostra final consolidada em 2016 foi de 460, resultando assim em uma taxa de resposta geral de 3,4%.

Tabela 2. Resposta da amostra	Freq.	Percentual
Estrutura total de amostragem	13.577	100%
Total de retornos	512	3,8%
Pesquisas rejeitadas ou filtradas	52	0,38%
Amostra final	460	3,4%

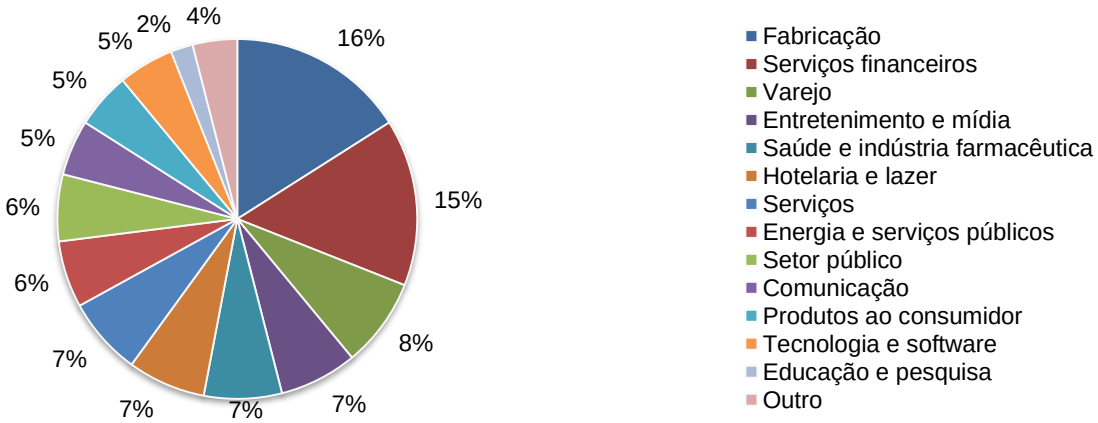
A Figura 17 resume os níveis aproximados da posição dos entrevistados em nosso estudo. Como podemos ver, a maioria dos entrevistados (59%) ocupa um nível de supervisão ou superior.

Figura 17. Distribuição dos entrevistados de acordo com o nível da posição



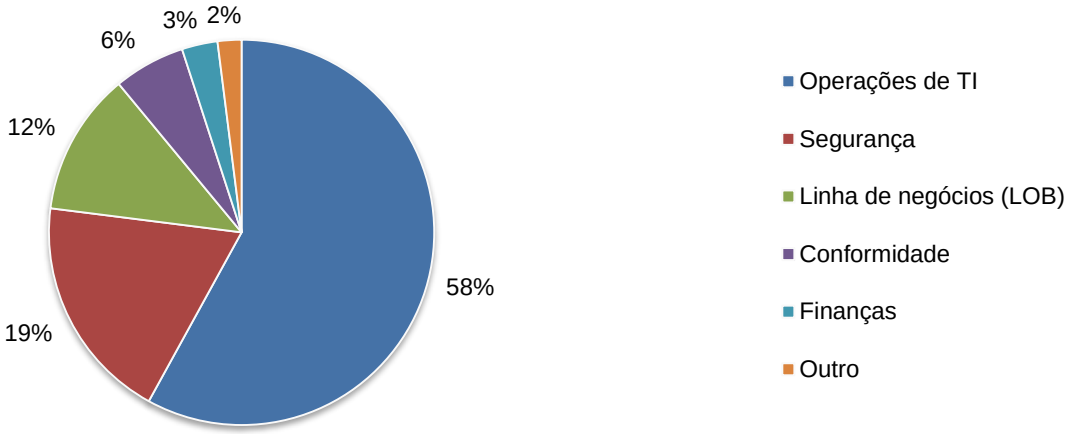
A Figura 18 informa os principais segmentos representados pelas organizações dos entrevistados. Como vemos, 16% dos entrevistados estão no setor de fabricação. 15% deles estão no setor de serviços financeiros, o que inclui bancos, gestão de investimentos, seguros, corretagem, pagamentos e cartões de crédito. 8% deles estão localizados no setor de varejo.

Figura 18. Distribuição dos entrevistados de acordo com a principal classificação do setor



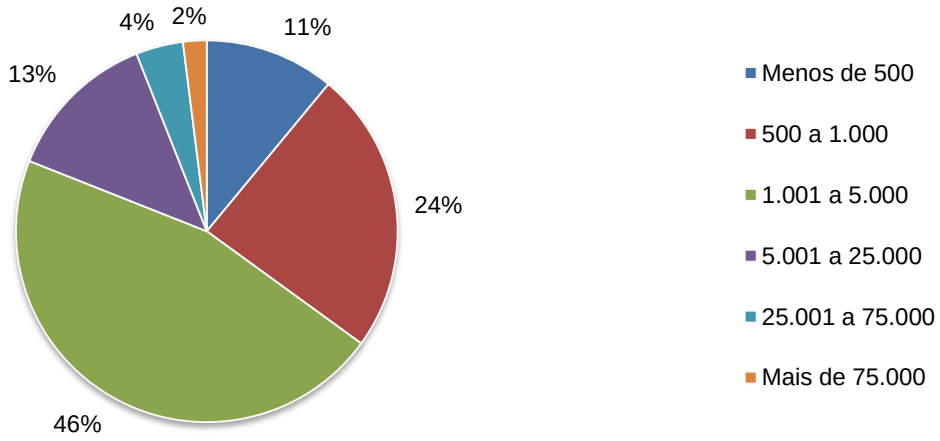
A Figura 19 informa a área funcional dos entrevistados. Como vemos, 58% dos entrevistados estão nas operações de TI, enquanto 19% estão na segurança e outros 12% em linhas de negócios.

Figura 19. Distribuição dos entrevistados de acordo a área funcional



Conforme mostra a Figura 20, a maior parte dos entrevistados (65%) está situada em organizações de maior porte, com uma mão de obra global de mais de 1.000 funcionários.

Figura 20. Distribuição dos entrevistados de acordo a quantidade de funcionários da organização
Amostras do país consolidadas



Limitações

Uma pesquisa de opinião tem limitações inerentes que precisam ser cuidadosamente consideradas antes de estabelecermos inferências a partir dos resultados apresentados. Os itens a seguir são limitações específicas que estão amplamente relacionadas à maioria dos estudos baseados em pesquisa de opinião.

- Tendência de não resposta: os resultados atuais são baseados em uma amostra de retornos da pesquisa. Enviamos pesquisas a uma amostra representativa de profissionais de TI e segurança de TI em 11 países, resultando em um grande número de respostas retornadas aptas ao uso. Apesar dos testes sem resposta, é sempre possível que os indivíduos que não participaram tenham crenças subjacentes substancialmente distintas das daqueles que preencheram a pesquisa.

- Tendência da estrutura de amostragem: a precisão dos resultados da pesquisa depende da medida em que nossas estruturas de amostragem são representativas dos indivíduos que são profissionais de TI ou de segurança de TI, dentro da amostra dos 11 países selecionados.

- Resultados autorrelatados: a qualidade da pesquisa de opinião é baseada na integridade das respostas confidenciais que recebemos dos entrevistados. Embora determinadas verificações tenham sido incorporadas em nosso processo de avaliação da pesquisa, incluindo controles de conformidade, sempre existe a possibilidade de que alguns entrevistados não tenham fornecido respostas verdadeiras.

Anexo 2. Tabelas de dados da pesquisa

As tabelas a seguir apresentam os resultados consolidados da amostra do Brasil.

Resposta à pesquisa	BR
Estrutura de amostragem	13.577
Total de retornos	512
Pesquisas rejeitadas ou filtradas	52
Amostra final	460
Taxa de resposta	3,4%
Pesos da amostra	0,09

Parte 1. Postura de criptografia

P1. Selecione a afirmação que melhor descreve a abordagem da sua organização no que diz respeito à implementação de criptografia em toda a empresa.	BR
Temos um plano ou estratégia geral de criptografia que é aplicado consistentemente em toda a empresa	28%
Temos um plano ou estratégia geral de criptografia que é ajustado para se adequar a diferentes aplicações e tipos de dados	26%
Para determinados tipos de dados sigilosos ou confidenciais, como números de CPF ou contas de cartão de crédito, temos um plano ou estratégia de criptografia limitado	25%
Não temos um plano ou estratégia de criptografia	21%
Total	100%

P2. A lista a seguir mostra 14 áreas em que as tecnologias de criptografia podem ser implantadas. Marque as áreas em que a criptografia está extensivamente implantada, está parcialmente implantada ou ainda não foi implantada pela sua organização. Alem disso, marque se você está diretamente envolvido na implantação de cada área apresentada.

P2a-1 Backup e arquivos	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2b-1. Repositórios de big data	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2c-1. Aplicações de negócios	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2d-1. Armazenamento de datacenter	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2e-1. Bancos de dados	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2f-1. Discos rígidos de desktop e estação de trabalho	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2g-1. E-mail	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2h-1. Serviços na nuvem pública	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2i-1. Sistemas de arquivos	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2j-1. Comunicação pela Internet (por exemplo, SSL)	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2k-1. Redes internas (por exemplo, VPN/LPN)	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2l-1. Discos rígidos de laptop	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

P2m-1 Infraestrutura de nuvem privada	BR
Implantação extensiva	39%
Implantação parcial	39%
Sem implantação	22%
Total	100%

Q2n-1 Gateway na nuvem (somente 2016)	BR
Implantação extensiva	33%
Implantação parcial	35%
Sem implantação	32%
Total	100%

P4. Na sua organização, quem é responsável ou tem mais influência no direcionamento da estratégia de criptografia da empresa? Selecione a melhor opção.	BR
Nenhuma função é individualmente responsável	26%
Operações de TI	31%
Finanças	1%
Linha de negócios (LOB) ou gerência geral	29%
Segurança	13%
Conformidade	0%
Total	100%

P5. Por quais motivos sua organização criptografa dados sigilosos e confidenciais? Selecione os três principais motivos.	BR
Para evitar divulgação pública após uma violação de dados	6%
Para proteger as informações contra ameaças específicas e identificadas	37%
Para cumprir políticas internas	18%
Para cumprir regulamentações e requisitos externos de privacidade ou segurança de dados	63%
Para reduzir o escopo de auditorias de conformidade	39%
Para proteger a propriedade intelectual da empresa	61%
Para proteger informações pessoais do cliente	50%
Para limitar a responsabilidade por violações ou divulgações acidentais	26%
Total	300%

P7. Quais são os maiores desafios no planejamento e na execução de uma estratégia de criptografia de dados? Selecione os dois principais motivos.	BR
Descobrir onde os dados sigilosos estão localizados na organização	47%
Classificar quais dados criptografar	42%
Determinar quais tecnologias de criptografia são mais eficazes	17%
Iniciar a implantação da tecnologia de criptografia	57%
Gerenciar continuamente a criptografia e as chaves	29%
Treinar usuários no uso adequado da criptografia	8%
Total	200%

P8. Qual é a importância dos seguintes recursos associados às soluções de criptografia que podem ser usadas pela sua organização? Respostas "muito importante" e "importante" combinadas.	BR
Aplicação da política	67%
Gerenciamento de chaves	74%
Suporte a múltiplas aplicações ou ambientes	61%
Separação de deveres e controles baseados na função	50%
Escalabilidade do sistema	44%
Resistência a falsificações, graças a hardware dedicado (por exemplo, HSM)	55%
Integração com outras ferramentas de segurança (por exemplo, SIEM e gerenciamento de ID)	56%
Suporte à segregação regional (por exemplo, residência de dados)	43%
Desempenho e latência do sistema	84%
Suporte a algoritmos emergentes (por exemplo, ECC)	75%
Suporte a implantação local e na nuvem	66%
Certificação formal de segurança do produto (por exemplo, FIPS 140)	53%

P9. Quais tipos de dados sua organização criptografa? Selecione todas as opções aplicáveis.	BR
Informações do cliente	29%
Informações de negócios não financeiras	40%
Propriedade intelectual	45%
Registros financeiros	47%
Dados de funcionários/RH	61%
Dados de pagamento	45%
Informações de saúde	16%

P10. Quais são as principais ameaças que podem resultar na exposição de dados sigilosos ou confidenciais? Selecione as duas principais opções.	BR
Hackers	22%
Indivíduos internos maliciosos	16%
Falhas de sistema ou processo	28%
Erros de funcionários	43%
Trabalhadores temporários ou terceirizados	25%
Prestadores de serviço terceirizados	28%
Solicitação legal de dados (por exemplo, por parte da polícia)	6%
Espionagem governamental	32%
Total	200%

Parte 2. Gerenciamento de chaves

P12. Classifique a "dificuldade" geral associada ao gerenciamento de chaves ou certificados em sua organização, sendo 1 = impacto mínimo e 10 = impacto severo.	BR
1 ou 2	7%
3 ou 4	18%
5 ou 6	23%
7 ou 8	24%
9 ou 10	28%
Total	100%

P13. O que torna o gerenciamento de chaves e certificados tão difícil? Selecione os três principais motivos.	BR
Ausência de responsabilidade clara	54%
Recursos insuficientes (tempo/dinheiro)	19%
Falta de pessoal capacitado	49%
Falta de claro entendimento dos requisitos	15%
Excesso de mudanças e incertezas	33%
As ferramentas de gerenciamento de chaves são inadequadas	53%
Sistemas isolados e fragmentados	48%
Tecnologia e padrões imaturos	13%
Processos manuais tendem a erros e não são confiáveis	16%
Total	300%

P14. A seguir há uma ampla variedade de chaves que podem ser gerenciadas pela sua organização. Classifique a "dificuldade" geral associada ao gerenciamento de cada tipo de chave. Respostas "muito difícil" e "difícil" combinadas.	BR
Chaves de criptografia para backup e armazenamento	29%
Chaves de criptografia para dados arquivados	37%
Chaves e certificados associados a SSL/TLS	37%
Chaves SSH	57%
Chaves de criptografia do usuário final (por exemplo, e-mail, criptografia de disco cheio)	27%
Chaves de criptografia de rede (por exemplo, IPSEC)	25%
Chaves pertencentes a aplicações (por exemplo, assinatura, autenticação, criptografia)	70%
Chaves relacionadas a pagamento (por exemplo, ATM, POS etc.)	37%
Chaves e certificados incorporados no dispositivo (por exemplo, os produtos que você fabrica)	13%
Chaves para serviços externos (por exemplo, serviços na nuvem ou hospedados)	60%
Chaves para sistemas de terceiros (por exemplo, parceiros, clientes, logon único, federação etc.)	62%
Chaves privadas para emissão de certificado	60%

P15a. Quais sistemas de gerenciamento de chaves sua organização usa atualmente?	BR
Política formal de gerenciamento de chaves (KMP)	50%
Declaração formal de práticas de gerenciamento de chaves (KMPS)	29%
Infraestrutura formal de gerenciamento de chaves (KMI)	32%
Definição formal de funções e responsabilidades de KMI, incluindo separação de deveres	29%
Processos manuais (por exemplo, em planilhas ou papéis)	68%
Sistema/servidor central de gerenciamento de chaves	25%
Módulos de segurança de hardware	16%
Mídia removível (por exemplo, pen drive, CD-ROM)	30%
Carteiras e armazenamentos de chaves baseados em software	16%
Cartões inteligentes	23%
Total	318%

Parte 3. Módulos de segurança de hardware

P16. Qual opção melhor descreve seu nível de conhecimento sobre HSMs?	BR
Conhecimento avançado	16%
Conhecimento razoável	32%
Nenhum conhecimento (pule para P19)	52%
Total	100%

P17a. Sua organização implanta HSMs?	BR
Sim	25%
Não (pule para P19)	75%
Total	100%

P17b. Para qual finalidade sua organização atualmente implanta ou planeja implantar HSMs? Selecione todas as opções aplicáveis.	
P17b-1. HSMs implantados atualmente	**BR**
Criptografia no nível da aplicação	42%
Criptografia de banco de dados	31%
Criptografia de big data	6%
Criptografia na nuvem pública	20%
Criptografia na nuvem privada	22%
SSL/TLS	51%
PKI ou gerenciamento de credenciais	20%
Autenticação de dispositivos da Internet das Coisas (IoT)	9%
Assinatura de documentos (por exemplo, faturamento eletrônico)	8%
Assinatura de códigos	5%
Processamento de transações de pagamento	36%
Emissão de credenciais de pagamento (por exemplo, dispositivos móveis, EMV)	26%
Criptomoedas	7%
Não planeja usar	14%
Total	297%

P17b-2. HSMs com implantação planejada nos próximos 12 meses	**BR**
Criptografia no nível da aplicação	22%
Criptografia de banco de dados	34%
Criptografia de big data	6%
Criptografia na nuvem pública	21%
Criptografia na nuvem privada	19%
SSL/TLS	13%
PKI ou gerenciamento de credenciais	19%
Autenticação de dispositivos da Internet das Coisas (IoT)	8%
Assinatura de documentos (por exemplo, faturamento eletrônico)	17%
Assinatura de códigos	21%
Processamento de transações de pagamento	24%
Emissão de credenciais de pagamento (por exemplo, dispositivos móveis, EMV)	29%
Criptomoedas	7%
Não planeja usar	4%
Total	244%

P18. Em sua opinião, qual é a importância de HSMs para sua estratégia de criptografia ou gerenciamento de chaves? Respostas "muito importante" e "importante" combinadas	**BR**
P18a. Importância hoje	38%
P18b. Importância nos próximos 12 meses	42%

Parte 4. Perguntas sobre orçamento

P19a. Neste ano, você é responsável por gerenciar todo ou parte do orçamento de TI da sua organização?	**BR**
Sim	59%
Não (pule para P20)	41%
Total	100%

P19b. Aproximadamente, qual é a faixa que melhor descreve o orçamento de TI da sua organização para 2015?	**BRL**
Valores extrapolados mostrados em milhões (bilhões para JPY, RUB, Rúpias e Peso)	187

P19c. Aproximadamente, qual percentual do orçamento de TI para 2016 será destinado a atividades de segurança de TI?	BR
Valor extrapolado	8,8%

P19d. Aproximadamente, qual percentual do orçamento de segurança TI para 2016 será destinado a atividades de proteção de dados?	BR
Valor extrapolado	26,4%

P19e. Aproximadamente, qual percentual do orçamento de segurança TI para 2016 será destinado a atividades de criptografia?	BR
Valor extrapolado	19,0%

Parte 6: Criptografia na nuvem: Ao responder às perguntas a seguir, suponha que elas se referem somente aos serviços na nuvem pública.	
P37a. Sua organização atualmente usa serviços computacionais na nuvem para qualquer classe de dados ou aplicações – sigilosos ou não?	BR
Sim, atualmente usamos	66%
Não, mas provavelmente usaremos dentro dos próximos 12 a 24 meses	21%
Não (vá para a Parte 7 caso você não use serviços na nuvem para qualquer classe de dados ou aplicações)	13%
Total	100%

P37b. Atualmente, você transfere dados sigilosos ou confidenciais para a nuvem (sejam ou não criptografados ou tornados ilegíveis por algum outro mecanismo)?	BR
Sim, atualmente usamos	60%
Não, mas provavelmente usaremos dentro dos próximos 12 a 24 meses	29%
Não (vá para a Parte 7 caso você não use nem planeje usar nenhum serviço na nuvem para dados sigilosos ou confidenciais)	11%
Total	100%

P37c. Em sua opinião, quem tem a maior responsabilidade pela proteção dos dados sigilosos ou confidenciais transferidos para a nuvem?	BR
O provedor da nuvem	54%
O usuário da nuvem	16%
Responsabilidade compartilhada	30%
Total	100%

P37d. Sua organização protege dados em repouso na nuvem por meio de criptografia ou alguma outra forma de tornar os dados ilegíveis (por exemplo, tokenização)?	BR
Sim (os dados em repouso são protegidos por criptografia)	39%
Sim (os dados em repouso são tornados ilegíveis por outros meios)	12%
Não	49%
Total	100%

P37e. Se os dados em repouso na nuvem são protegidos por criptografia, como essa proteção é aplicada?	BR
Os dados são criptografados antes de serem enviados para a nuvem (ao responder, desconsidere o uso de SSL/IPSec ou outra criptografia de rede)	40%
Os dados em repouso na nuvem são criptografados na nuvem usando ferramentas que a organização implanta lá	16%
Os dados em repouso na nuvem são criptografados lá pelo provedor da nuvem	44%
Total	100%

P37f. Para a criptografia de dados em repouso na nuvem, a estratégia da minha organização é...	BR
Usar apenas chaves controladas pela minha organização	34%
Usar apenas chaves controladas pelo provedor da nuvem	15%
Usar uma combinação de chaves controladas pela minha organização e pelo provedor da nuvem	51%
Total	100%

Parte 7: Função e características organizacionais

D1. Qual nível organizacional melhor descreve sua posição atual?	BR
Executivo sênior	3%
Vice-presidente	3%
Diretor	17%
Gerente/supervisor	36%
Funcionário/equipe/técnico	41%
Outro	0%
Total	100%

D2. Marque a área funcional que melhor descreve a sua organização.	BR
Operações de TI	58%
Segurança	19%
Conformidade	6%
Finanças	3%
Linha de negócios (LOB)	12%
Outro	2%
Total	100%

D3. Qual setor melhor descreve o foco da sua organização?	BR
Agricultura e serviços alimentícios	1%
Comunicação	5%
Produtos ao consumidor	5%
Defesa	0%
Educação e pesquisa	2%
Energia e serviços públicos	6%
Entretenimento e mídia	7%
Serviços financeiros	15%
Saúde e indústria farmacêutica	7%
Hotelaria e lazer	7%
Fabricação	16%
Setor público	6%
Varejo	8%
Serviços	7%
Tecnologia e software	5%
Transporte	1%
Outro	2%
Total	100%

D4. Qual é a quantidade global de funcionários da sua organização?	BR
Menos de 500	11%
500 a 1.000	24%
1.001 a 5.000	46%
5.001 a 25.000	13%
25.001 a 75.000	4%
Mais de 75.000	2%
Total	100%

Sobre o Ponemon Institute
O Ponemon Institute© dedica-se ao avanço de práticas responsáveis de gerenciamento de informações e privacidade nas áreas empresarial e governamental. Para alcançar esse objetivo, o Instituto conduz pesquisas independentes, treina líderes dos setores público e privado e verifica as práticas de privacidade e proteção de dados utilizadas por organizações em uma variedade de indústrias.

Sobre a Thales e-Security
A Thales e-Security é líder mundial no fornecimento de soluções de proteção de dados e gestão de confiança que protegem as aplicações e informações mais sigilosas do mundo. As soluções da Thales respondem a desafios de identidade e privacidade com criptografia baseada em software, assinatura digital e recursos de gerenciamento. No mundo cada vez mais conectado de hoje, nossas soluções ajudam a impedir ataques direcionados e a reduzir o risco de exposição de dados sigilosos que é trazido pela computação na nuvem e virtualização, uso de dispositivos de consumidor no local de trabalho, aumento da mobilidade, big data e por diversos outros fatores. www.thales-esecurity.com

Sobre a Thales
A Thales lidera a tecnologia global para os mercados aeroespacial, de transporte, defesa e segurança. Com 62.000 funcionários em 56 países, a Thales registrou € 14 bilhões em vendas no ano de 2015. Com mais de 22.000 engenheiros e pesquisadores, a Thales tem uma capacidade exclusiva de projetar e implantar equipamentos, sistemas e serviços para atender aos mais complexos requisitos de segurança. Sua excepcional presença internacional permite que a Thales trabalhe junto a clientes de todo o mundo.

Posicionada como uma integradora de sistemas, fornecedora de equipamentos e prestadora de serviços de valor agregado, a Thales é um dos principais nomes do mercado de segurança na Europa. As equipes de segurança do Grupo trabalham junto a agências governamentais, autoridades locais e clientes corporativos no intuito de desenvolver e implantar soluções integradas e resilientes, a fim de proteger cidadãos, dados sigilosos e infraestruturas críticas.