IDC
Analyze the Future

Level 3 Security Index

Índice de Maturidade de Segurança na Infraestrutura Corporativa de TI

Luciano Ramos
Software Research Coordinator

Preparado para

Level (3)
COMMUNICATIONS

Preparado para Level(3) COMMUNICATIONS

International Data Corporation (IDC) é a empresa líder em inteligência de mercado e consultoria nas indústrias de tecnologia da informação, telecomunicações e mercados de consumo em massa de tecnologia. Analisa e prediz as tendências tecnológicas para que os profissionais, investidores e executivos possam tomar decisões de compra e negócios nestes setores. Nos últimos *50 anos*, IDC tem fornecido informações estratégicas aos seus clientes para ajudá-los a alcançar seus objetivos com êxito.

+50 anos de experiência em análise de mercado de TIC

1.100+ analistas, formando uma rede global de informação

110+ países abrangidos pelo mundo

Escritório no Brasil

- **Desde 1990** com escritório em São Paulo;
- **Mais de 70 funcionários,** incluindo analistas e consultores locais cobrindo os mercados de Hardware, Software, Serviços e Telecomunicações;
- Reconhecidamente o **principal provedor de informações de mercado e consultoria** para fornecedores locais, multinacionais e para toda a cadeia de valor dos segmentos de TI e Telecom;
- **Extensa base de relacionamento** com usuários finais de tecnologia, canais e fornecedores;
- **Call Center (CATI) próprio** com mais de 17 entrevistadores bilíngues (português e espanhol) especializados em pesquisas sobre TI e Telecom para toda a América Latina.

IDC América Latina

Metodologia - Destaques de 2015

95 Analistas na Região

14K Pesquisas com Usuários Finais

2.652 Entrevistas com Canais

96 Dados Oficiais de Distribuidores

476K Dados de Importação

1.323 Relatórios Oficiais de Fabricantes

78K Preços Coletados

Agenda

Definição do Índice

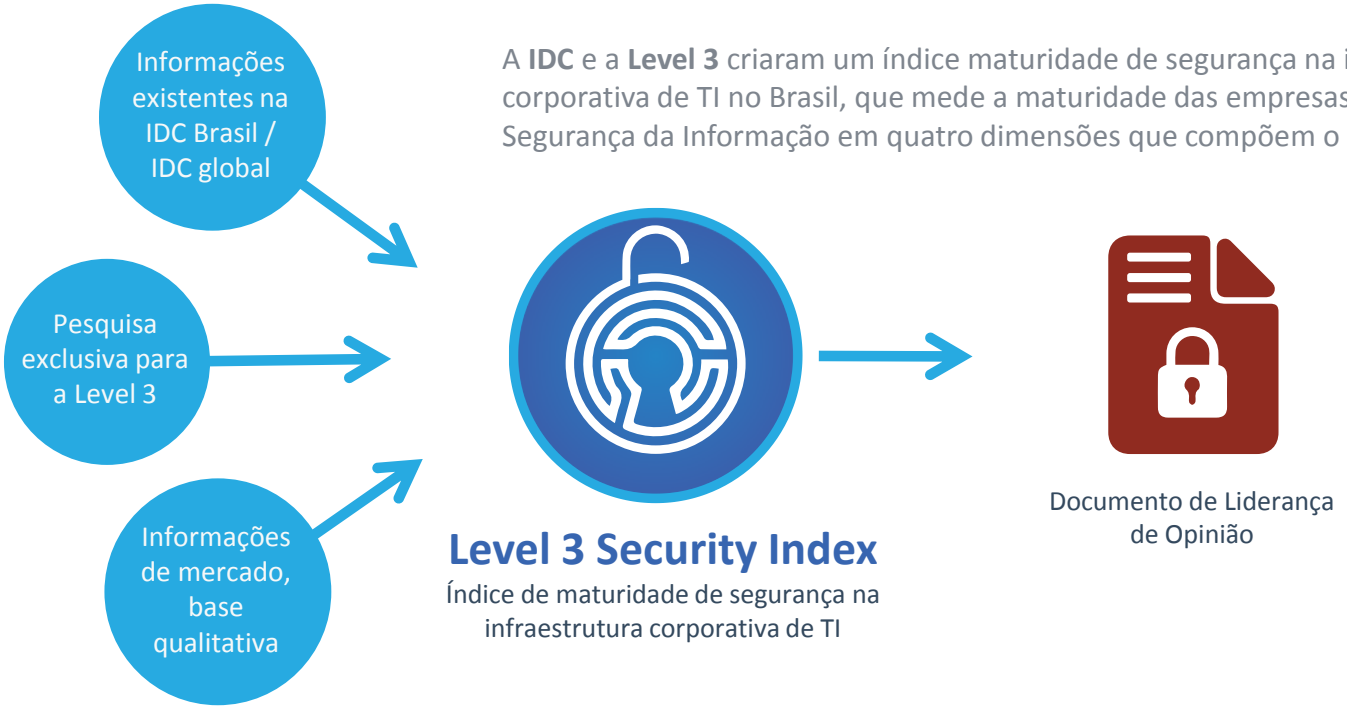
Qualificação da Amostra

Momento das Empresas

Resultado do Índice

Definição do Índice

Level 3 Security Index - Índice Level 3 de Maturidade de Segurança na Infraestrutura Corporativa de TI no Brasil



A **IDC** e a **Level 3** criaram um índice maturidade de segurança na infraestrutura corporativa de TI no Brasil, que mede a maturidade das empresas em relação à Segurança da Informação em quatro dimensões que compõem o índice.

Level 3 Security Index - Metodologia

A geração do índice englobou uma pesquisa com 100 empresas com mais de 250 funcionários, feita por meio de entrevistas conduzidas pela IDC.

Esta pesquisa explorou o conhecimento e o posicionamento do gestor de segurança dessas organizações dentro das quatro dimensões do índice.

Também foram utilizadas informações existentes da IDC Brasil e da IDC global, além de informações de mercado sobre o tema para suportar e construir a base qualitativa do projeto.

O resultado do índice é uma ponderação matemática dos temas com base na pesquisa com as 100 empresas.

Level 3 Security Index - Dimensões do Índice

Level 3 Security Index

X1% **Conscientização**

Explora o entendimento da importância de Segurança da Informação para o negócio e o conhecimento do gestor de SI sobre os impactos em caso de desastre.

- Sua empresa consegue mensurar os impactos de eventual indisponibilidade de recursos ou sistemas?
- Sua empresa sabe dizer quantos incidentes de segurança foram sofridos ou mitigados nos últimos 12 meses?

X2% **Ferramental**

Explora as habilidades de detecção e capacidade de mensuração das ameaças aos sistemas.

- Sua empresa possui ferramentas para prevenir e detectar eventuais ataques?
- Sua equipe tem expertise para operacionalizar as ferramentas?

X3% **Prevenção**

Explora a maturidade empregada nas atividades de manutenção dos sistemas de segurança.

- Existe um responsável pela documentação das alterações dos parâmetros de segurança?
- Sua empresa executa algum teste de segurança em seus ambientes computacionais? Com que frequência?

X4% **Mitigação**

Explora os procedimentos adotados para redução dos riscos de Segurança da Informação existentes, e as medidas para contenção de ataques e recuperação.

- Existem condutas pré-definidas para ação em momentos de ataque?
- Há hierarquia para acionamento das equipes na ocorrência de um desastre?

IDC Analyze the Future

Preparado para Level (3) COMMUNICATIONS

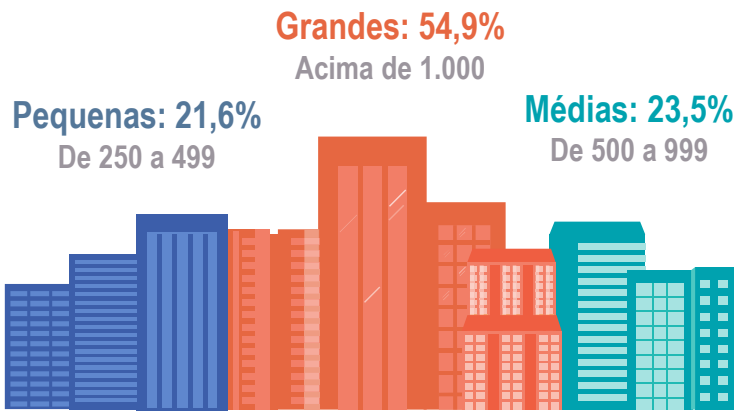
Qualificação da Amostra

Qualificação da Amostra

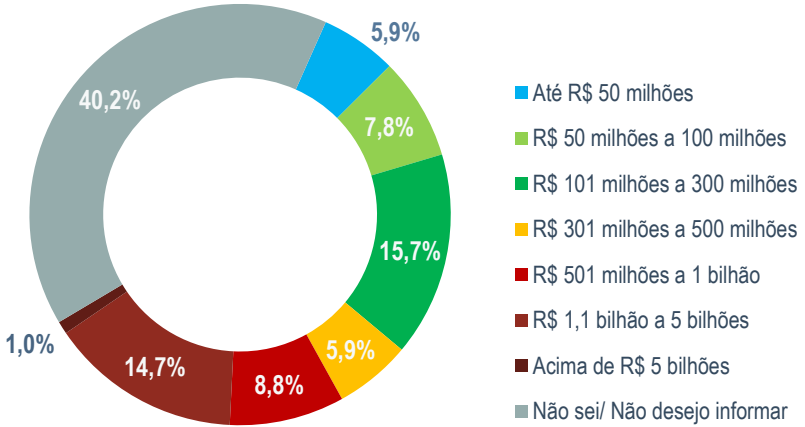
Empresas entrevistadas trazem boa representatividade do mercado brasileiro

A amostra para este estudo foi direcionada para empresas acima de 250 empregados no Brasil. Não houve restrição quanto a faturamento ou vertical de atuação, o que possibilitou cobrir uma boa gama de cenários do mercado corporativo.

F2-Quantidade de Funcionários da Empresa no Brasil



P7-Faturamento Bruto da Empresa no Brasil



Momento das Empresas

Momento das Empresas

Orçamento de SI foi menos afetado que o orçamento de TI em 2016

Os desafios trazidos pelo ano de 2015 e as incertezas de 2016 forçaram a manutenção ou retração dos orçamentos, o que comprometeu o avanço de projetos transformacionais na área de Segurança da Informação.

Iniciativas já em andamento foram preservadas, mas novos investimentos ficaram escassos, sendo postergados.

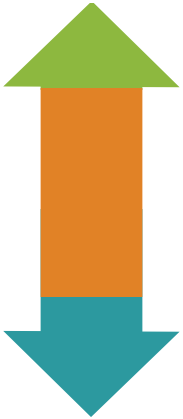
P10-Situação do orçamento de TI em 2016 comparado ao de 2015

18,6%
Aumentou

41,2%
Permaneceu o mesmo

40,2%
Diminuiu

P15-Situação do orçamento de Segurança da Informação em 2016 comparado ao de 2015



18,6%
Aumentou

50,1%
Permaneceu o mesmo

30,4%
Diminuiu

Momento das Empresas

Perspectiva mais otimista para 2017, especialmente para SI

O ano de 2017 se apresenta com um cenário de maior previsibilidade, seja do ponto de vista econômico ou político. As empresas não podem mais esperar para investir, e estão retomando seus projetos diante dos sinais de recuperação que o mercado apresenta.

3,5%
Percentual médio do orçamento de TI em relação ao faturamento bruto das empresas entrevistadas (P9).

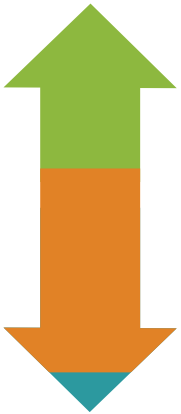
P11-Expectativa para o orçamento de TI para 2017 comparado ao de 2016

42,2%
Aumentará

39,2%
Permanecerá o mesmo

18,6%
Diminuirá

P16-Expectativa para o orçamento de Segurança da Informação para 2017 comparado ao de 2016



37,3%
Aumentará

52,9%
Permanecerá o mesmo

9,8%
Diminuirá

Momento das Empresas

A maioria das empresas ainda mantém Data Centers em suas instalações

Ainda há preocupações sobre a segurança e a conectividade com infraestruturas hospedadas fora das empresas.

O modelo de IaaS (*Infrastructure as a Service*, ou infraestrutura como serviço) vem ganhando atratividade, não apenas para computação, mas também para armazenamento - fator que acentua a preocupação com a segurança e governança das informações.

A IDC acredita que o modelo de infraestrutura que prevalecerá nos próximos anos é híbrido, integrando capacidades *on-premises* (no modelo de arquitetura tradicional ou numa arquitetura de *Cloud* privada) com capacidades de nuvens privadas e públicas em ambientes externos.

P18-Que modalidade de Data Center sua empresa utiliza?

16,7% Contratado como serviço (IaaS)

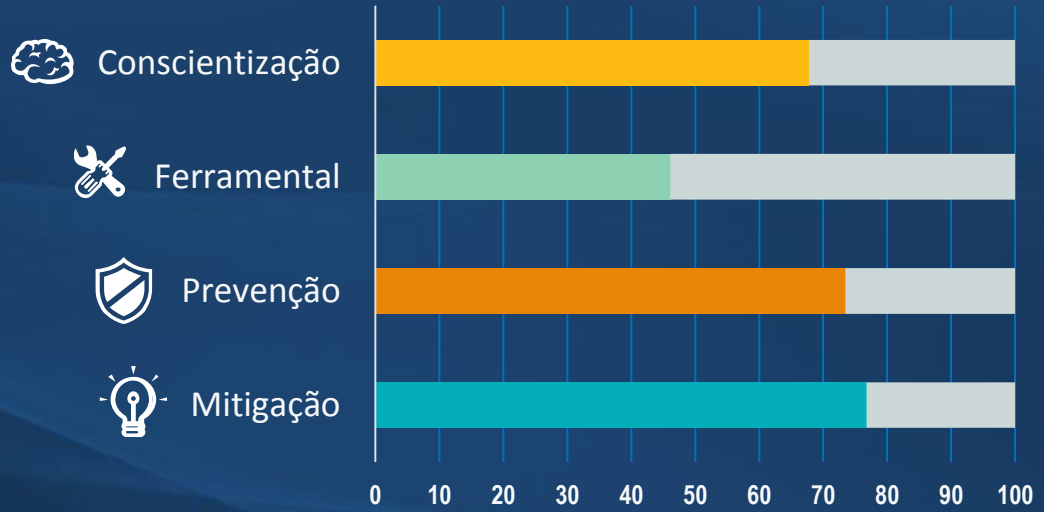
17,6% Fora da empresa (Hosting ou Colocation)

85,3% Dentro da empresa (On-premises)

Resultados do Índice

Level 3 Security Index: Brasil - Resultado

O índice para as empresas no Brasil atingiu 64,9 de 100 pontos possíveis, mostrando maturidades distintas em cada dimensão.



Level 3 Security Index - Brasil

Constatações sobre a dimensão de Conscientização

A dimensão de conscientização colocou dois temas relevantes em evidência. O primeiro tema diz respeito ao estabelecimento de uma área de Segurança da Informação (SI) efetiva e independente. A relação com a área de TI das organizações tem avançado da forma de dependência para um modelo de parceria, mas ainda há desafios. Um deles, por exemplo, refere-se à quantidade de profissionais dedicados para atuar na área de SI, ainda abaixo do que os gestores consideram ideal.

Outro tópico trazido por esta dimensão é a dificuldade de visibilidade dos impactos trazidos por algum incidente de segurança, sobretudo nas grandes empresas. Com a expansão das ofertas de ambientes hospedados e de ambientes em nuvem, a complexidade dos ambientes e sistemas dentro das organizações tem crescido consistentemente, apresentando cenários híbridos e distribuídos com grande capacidade de movimentação de cargas de trabalho.

Com recursos limitados, a área de SI nem sempre consegue mapear completamente os riscos de segurança e acompanhar seus controles, gerando esse descolamento.

Level 3 Security Index - Brasil

Estrutura da área de Segurança da Informação

O estudo feito para a elaboração do índice identificou que ainda há uma dependência grande entre a área de segurança e a área de TI nas empresas. Cerca de 51% das empresas entrevistadas afirmam ter uma área de Segurança da Informação independente, seja com equipe própria ou terceirizada. Contudo, um percentual muito maior (81%) indicou que o orçamento da área de segurança está atrelado ao orçamento de TI.

Outros dois dados trazem preocupação: 1) quase 20% das organizações não contam com uma área específica para lidar com as questões de SI; 2) em geral, as empresas contam com apenas dois profissionais dedicados para atuar com Segurança da Informação.

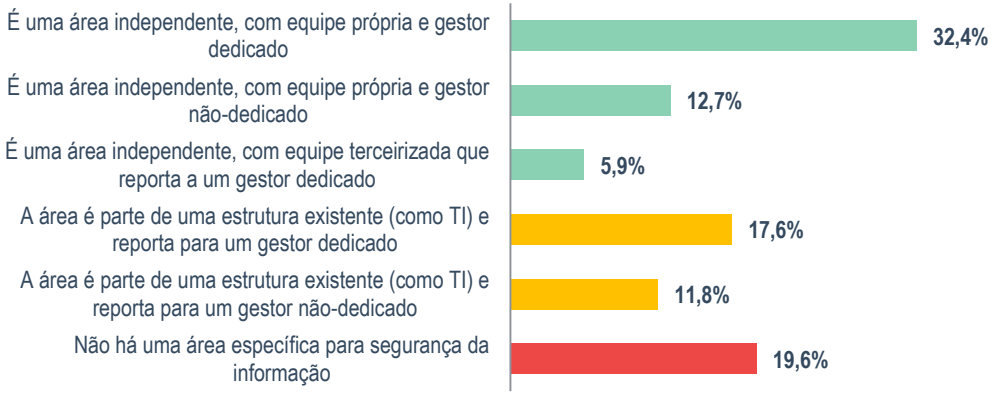
2 pessoas

Média de pessoas que trabalham de forma dedicada com Segurança da Informação na amostra (P13).

81,4%

Percentual de empresas que indicou que o orçamento de Segurança da Informação está atrelado ao orçamento de TI (P14).

P12-Sobre a Área de Segurança da Informação na Empresa



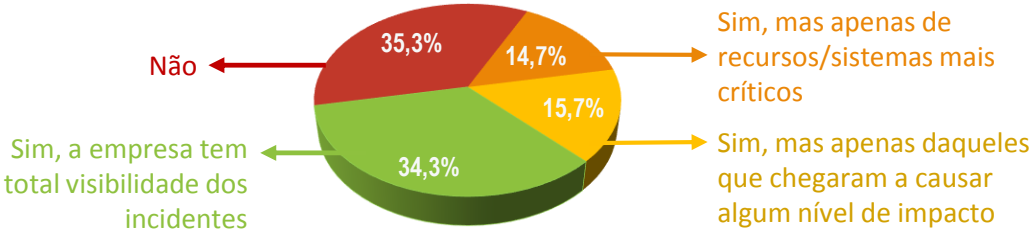
Level 3 Security Index - Brasil

Consciência sobre segurança e métricas

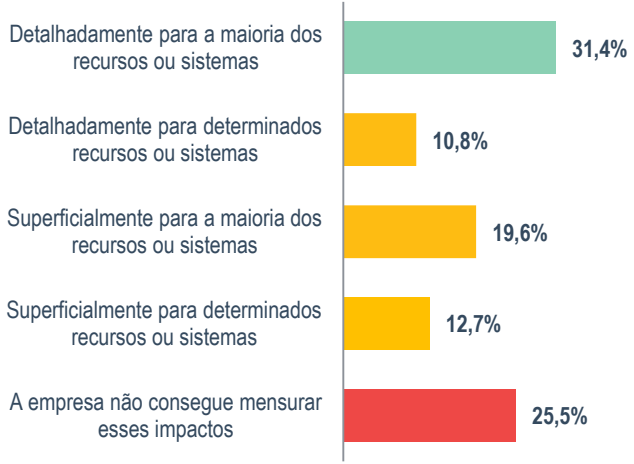
A despeito da consciência sobre a necessidade de se estabelecer uma área de Segurança da Informação bem estruturada e de ter o acompanhamento sobre este tópico na sua organização, nem sempre os controles e procedimentos apropriados são estabelecidos.

Como trazido por este estudo, ainda há uma parcela significativa de empresas que não identifica claramente os incidentes relacionados a SI (35%) e tampouco consegue medir os impactos que poderiam ser causados por esses incidentes (25%). Essa pode ser a principal oportunidade de amadurecimento nesta dimensão do índice, e que alavanca também as demais dimensões.

P20-Consciência da Quantidade de Incidentes de Segurança sofridos/mitigados no Último Ano



P19-Mensuração de Impactos que Seriam Causados pela Eventual Indisponibilidade de Recursos/Sistemas



67,8
Conscientização

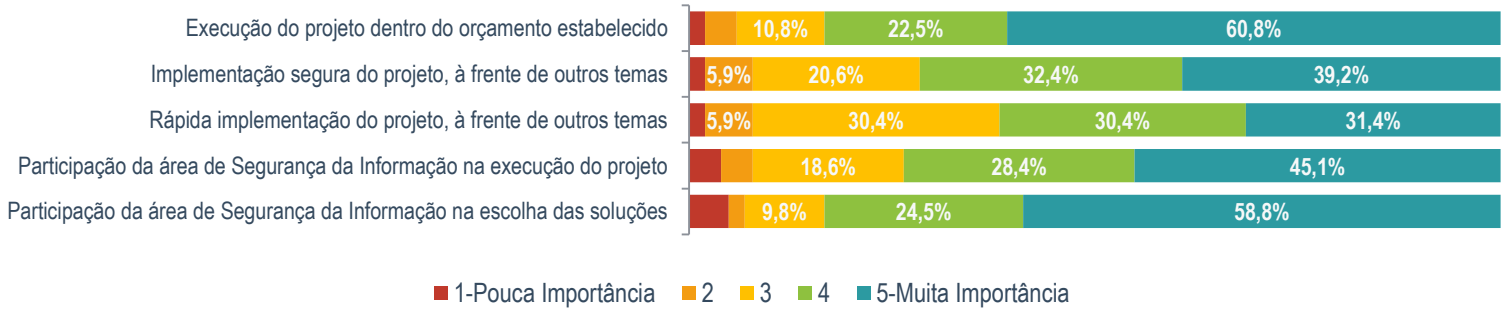
Level 3 Security Index - Brasil

Fazer de forma segura e dentro do orçamento

As empresas entrevistadas deram altos níveis de importância para tópicos relacionados à Segurança da Informação nos novos projetos de TI. Entretanto, o item ligado ao cumprimento do orçamento foi o que apresentou maior relevância - mais de 83% das empresas consideram o tema importante ou muito importante. Isso indica que, avaliando todos as afirmações na visão dessas organizações, novas iniciativas podem até tomar um pouco mais de tempo para serem implementadas, desde que sigam suas previsões de gastos e sejam conduzidas de forma segura na sua execução.

No entanto, essa visão se torna um tanto mais crítica quando se trata de projetos executados por terceiros. Nesses casos, a pressão por rapidez de implementação com segurança se acentua; de fato, segurança já é considerada como um componente intrínseco de um serviço contratado e precisa permear em todas as etapas de projeto.

P21-Grau de Importância Pensando na Implementação de um Novo Projeto de TI



Level 3 Security Index - Brasil

Comunicação para melhorar o engajamento

As organizações reconhecem a importância do envolvimento das pessoas no aculturamento sobre Segurança da Informação. E a comunicação tem papel fundamental neste tema.

Quase 85% das empresas acessadas pelo estudo indicaram que lançam mão de iniciativas para melhorar o engajamento de seus colaboradores nas práticas de segurança. A principal ferramenta para isso ainda é o lançamento de campanhas internas de conscientização sobre o tema - utilizada por mais de 66% dos respondentes. Contudo, é importante levar em consideração que a qualidade e a frequência desse tipo de comunicação pode variar muito de empresa para empresa.

Uma estratégia efetiva de engajamento pode ajudar a reduzir os riscos de Segurança da Informação, criando nas pessoas a primeira barreira contra quaisquer tipos de ataques.

P22-Iniciativas Colocadas em Prática para Obter Maior Engajamento dos Colaboradores nas Práticas de SI

15,7%
Empresas que não têm iniciativas vigentes para acentuar o engajamento nas práticas de SI (P22).

Level 3 Security Index - Brasil

Constatações sobre a dimensão de Ferramental

A dimensão de Ferramental se configurou como o tema mais desafiador do índice, obtendo a menor pontuação entre as quatro dimensões que compõem o *Level 3 Security Index*.

Por um lado, o estudo constatou que a penetração do ferramental técnico utilizado para assegurar a Segurança da Informação em ambientes computacionais é relativamente baixa.

Isso é especialmente percebido no segmento de empresas pequenas. A disposição de ferramental está, em certa medida, atrelada à capacidade de investimento das organizações. Empresas menores, por vezes, não dispõem dos recursos para investir, optando então por acelerar outros aspectos de proteção.

Além da questão de investimentos, a disponibilidade de mão de obra capacitada para operar as ferramentas se mostra como desafio e, ao mesmo tempo, como oportunidade de amadurecimento para as empresas entrevistadas por meio de serviços gerenciados.

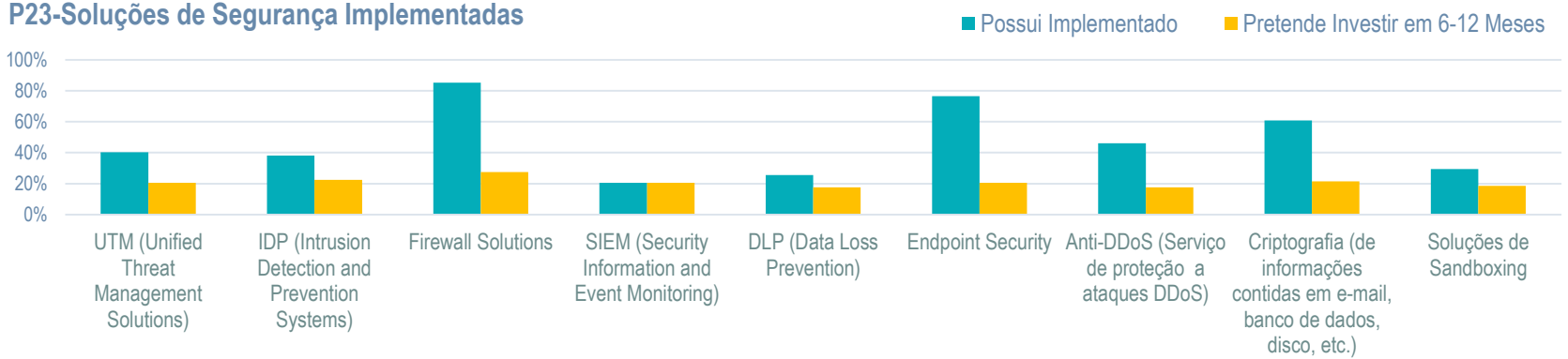
Level 3 Security Index - Brasil

Básico e, nem sempre, suficiente: é preciso investir

O estudo avaliou que o ferramental considerado mais "básico" é o que apresenta maior nível de penetração na amostra. De fato, isso traduz a percepção da indústria sobre um perfil de gestor de SI que acredita que o conjunto "Firewall + Antivírus + Criptografia" é o suficiente para garantir a segurança da empresa dele. Isso, no entanto, pode não ser verdade, e ainda contribui para a questão da correta visibilidade do ambiente que abordamos na dimensão de conscientização do *Level 3 Security Index*.

Outra dicotomia trazida pela entrevistas realizadas para o estudo refere-se à relação entre o comportamento do orçamento de SI em oposição às intenções de investimento em ferramental. Com o orçamento em alta e os investimentos em ferramental em baixa, vamos nos deparar com uma situação de "mais do mesmo", ou seja, ao invés de investir em recursos que possam viabilizar melhor controle, automação de recursos e maior visibilidade, o gestor manterá seu parque (ou fará pequenas atualizações) e investirá em outras dimensões, como prevenção ou mitigação.

P23-Soluções de Segurança Implementadas

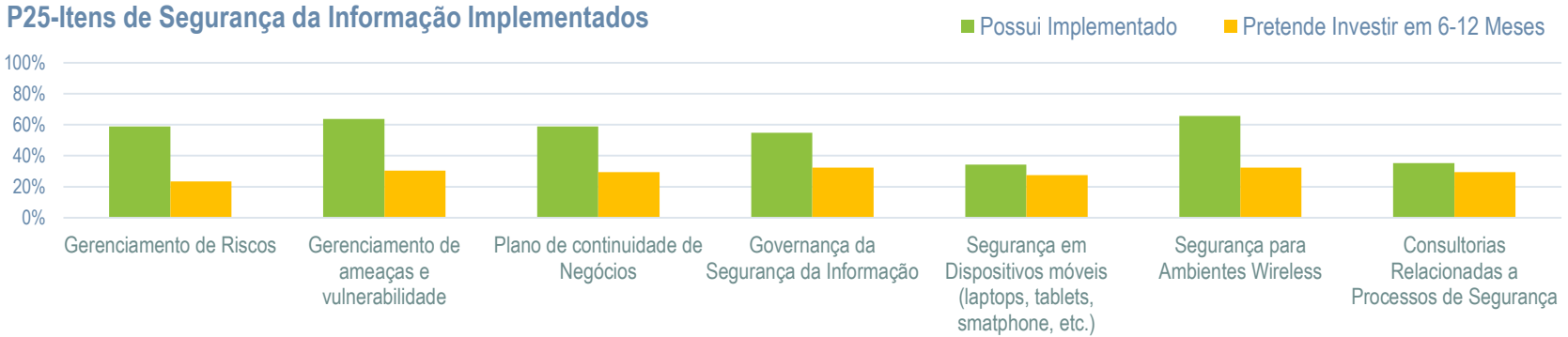


Level 3 Security Index - Brasil

Controles formais abrem espaço para as demais dimensões

Quando pensamos nos elementos de Segurança da Informação mais ligados a aspectos formais de controle, vemos um interesse mais uniforme vindo das organizações. As respostas obtidas no *Level 3 Security Index* apontam para o fato de que essas iniciativas dependem menos de investimento de capital e mais da definição de processos e procedimentos, o que, num cenário de mercado mais adverso, se configura como algo viável.

Isto posto, foi confirmado pelo estudo que a intenção de investimentos nesses itens é sensivelmente maior do que no ferramental técnico, o que contribui para a preparação de um cenário mais propenso às ações de prevenção e mitigação.



Level 3 Security Index - Brasil

Capacitação dos profissionais é um tema a endereçar

Outro aspecto importante na dimensão de Ferramental diz respeito à capacitação dos profissionais de Segurança da Informação. A baixa disponibilidade de profissionais qualificados está refletida na afirmação de quase 62% das empresas entrevistadas para o *Level 3 Security Index*, que indicaram que suas equipes estão aquém do desejado em termos de capacidades para operar os ferramentais disponíveis ou que apenas alguns profissionais tem o conhecimento necessário.

Adicionalmente, a despeito da percepção de que a oferta de profissionais está aumentando, está claro para os decisores de SI que capacitação técnica precisa ser acompanhada de vivência para formar um profissional eficaz.

Este ponto tem íntima relação com a adoção das ferramentas comentadas anteriormente, pois os investimentos também podem estar sendo postergados por conta da ausência de pessoas preparadas para configurá-las, operá-las e gerar indicadores.

66,1% Percentual de empresas que indicou percebe algum aumento de oferta de profissionais com perfis técnicos na área de Segurança da Informação.

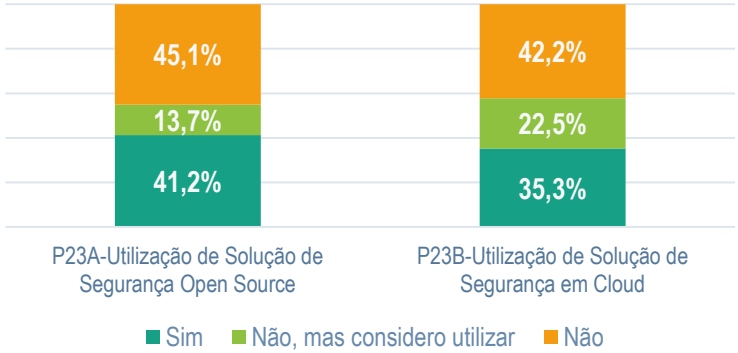
P24-Grau de Conhecimento/Capacitação da Equipe de SI para Utilizar o Ferramental Disponível

Level 3 Security Index - Brasil

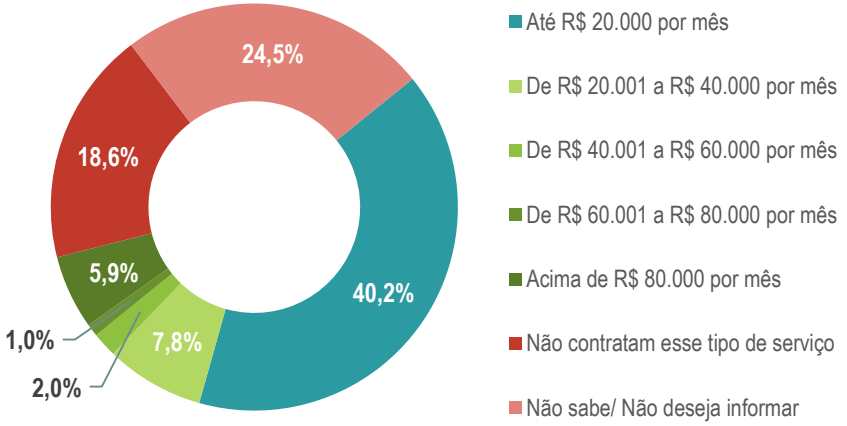
Serviços gerenciados se apresentam como opção importante

Num cenário complexo e com escassez de qualificação, as empresas passam a olhar para os serviços gerenciados com opção relevante para seus negócios. Cerca de 57% das organizações entrevistas no *Level 3 Security Index* indicaram que já contratam MSS.

As empresas também reconhecem as capacidades de soluções de segurança no modelo Open Source e avaliam que estas podem ser uma alternativa a um investimento inicial mais intenso para viabilizar aspectos de segurança. As soluções de segurança em Cloud também são vistas como oportunidade, sendo contratadas como serviço em um modelo de pagamento por uso.



P26-Gastos Atuais com Serviços Gerenciados de Segurança (Managed Security Services – MSS)



Level 3 Security Index - Brasil

Constatações sobre a dimensão de Prevenção

A dimensão de prevenção se desenha como uma das mais maduras do índice. As empresas entrevistadas afirmaram que estabelecem práticas de segurança, documentando-as e revalidando-as periodicamente. Em especial, as empresas de maior porte estabelecem e acompanham os controles com maior assiduidade, garantindo um melhor nível de manutenção.

Contudo, considerando o comportamento das demais dimensões que formam o *Level 3 Security Index*, podemos afirmar que essa avaliação não é totalmente positiva. Isso se deve ao fato de que, com razoável frequência, as organizações optam em compensar sua deficiência em outras dimensões com uma atuação mais forte no quesito de prevenção.

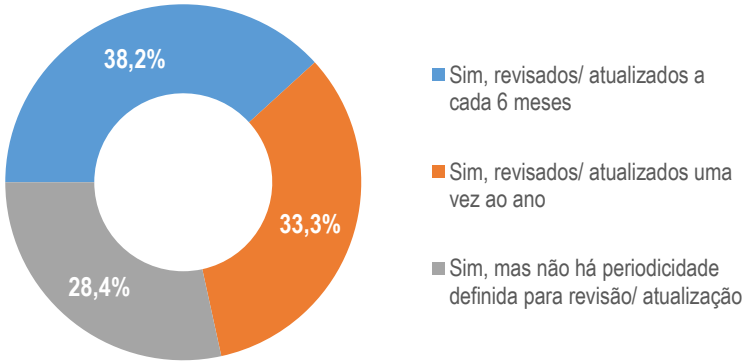
Para um avanço na pontuação geral do índice de segurança, é importante que todas as dimensões tenham a atenção e os recursos necessários para cumprir o seu papel nos cenários das empresas. Não é possível compensar uma dimensão com a aceleração de outra, o que só geraria uma falsa sensação de que o tema de Segurança da Informação está endereçado quando, na verdade, ainda há espaço para amadurecimento.

Level 3 Security Index - Brasil

Documentação colocada em prática

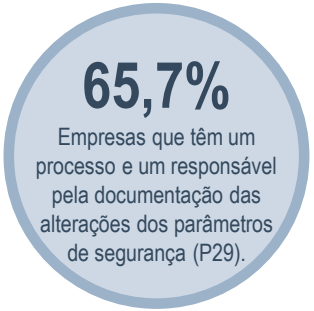
O estudo trazido pelo *Level 3 Security Index* mostra que as empresas têm documentado de maneira mais efetiva as suas práticas de segurança. Cerca de 71% das companhias entrevistadas afirmaram que revisam as políticas e padrões de SI ao menos uma vez ao ano. Isso evidencia a capacidade de manter essa documentação em linha com a evolução constante dos processos de negócios, em especial em empresas cujo cenário competitivo se mostra agressivo e as mudanças são constantes.

P28-Existência e Manutenção de Políticas e Padrões de Segurança da Informação Estabelecidos e Documentados



Nesse contexto, a necessidade de definir um papel para assegurar essas atualizações é percebida pelas organizações. Mais de 65% delas mantêm uma pessoa com esta função.

Políticas, padrões e procedimentos documentados são chave para que o conhecimento e as práticas de Segurança da Informação não fiquem limitadas a apenas um grupo de pessoas, mas possam ser replicadas sempre que necessário dentro da companhia, de forma uniforme e consistente em todas as ocasiões.

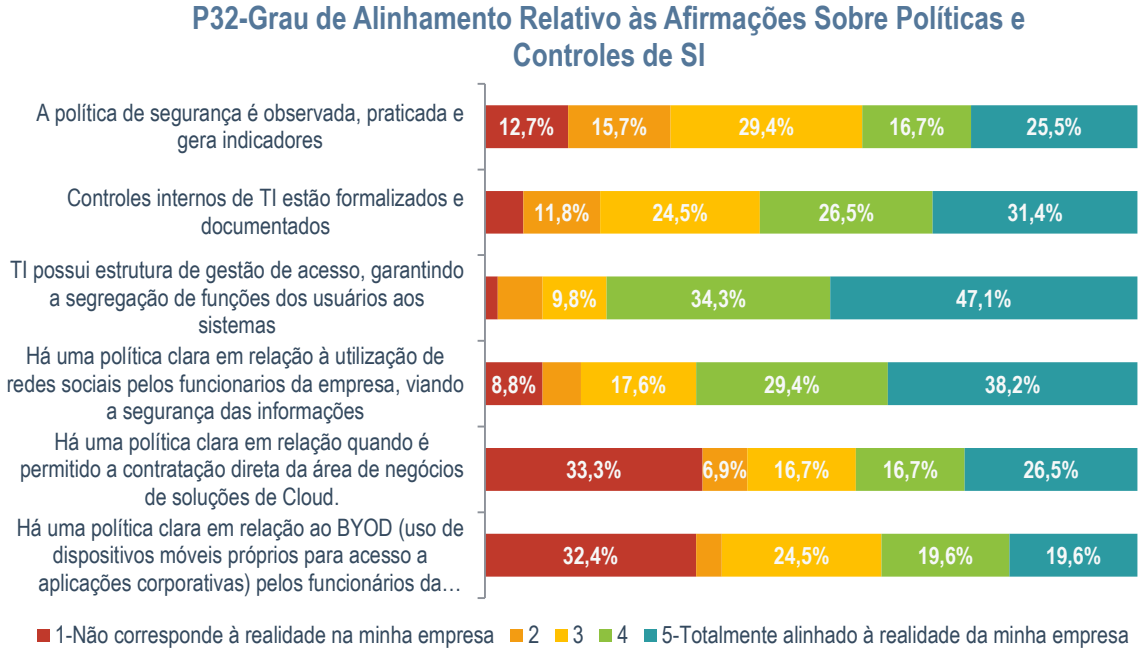


Level 3 Security Index - Brasil

Temas como Cloud e BYOD ainda carecem de definição

Mesmo com a documentação em dia, gerar indicadores de Segurança da Informação ainda é uma tarefa relativamente distante da realidade das empresas. Enquanto a maioria (58%) dispõem de controles formalizados e documentados, apenas cerca de 42% das organizações afirmam praticar e gerar métricas sobre a observância de suas políticas de SI.

Entre os temas pesquisados no índice *Level 3 Security Index*, foi identificado que a contratação de soluções no modelo de Cloud pública e a adoção de BYOD ainda são temas que necessitam de maior clareza; nesse sentido, a proximidade da área de SI com as áreas de negócios é essencial, de forma a entender suas necessidades e estabelecer os padrões para a utilização desses recursos de maneira controlada e segura para a empresa.



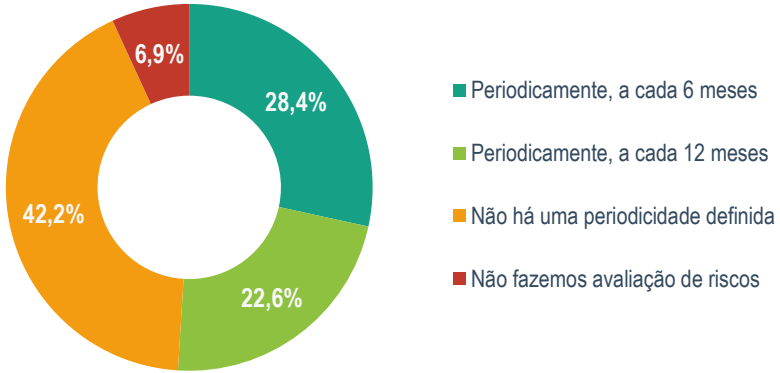
Level 3 Security Index - Brasil

É preciso avaliar e testar para garantir os controles

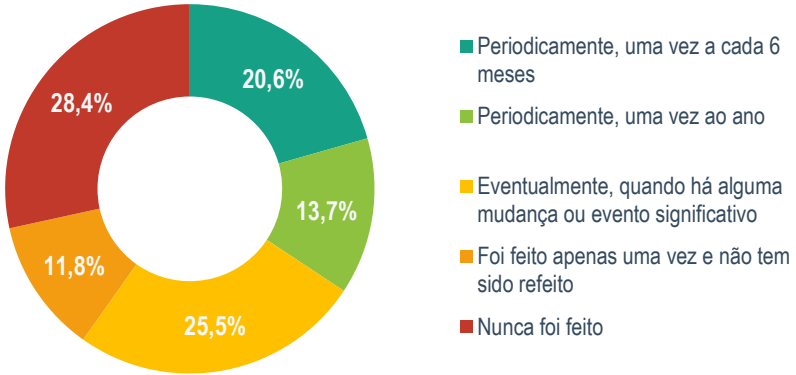
Entre as empresas entrevistadas para elaboração do *Level 3 Security Index*, é relativamente baixa a frequência com que os riscos de SI são avaliados: apenas pouco mais da metade dessas empresas (51%) faz uma avaliação anual.

Quando pensamos em testes de segurança, a situação é ainda mais desafiadora, com somente 34% dos respondentes mantendo a frequência de avaliação em até 12 meses. Em especial, este item sofre uma resistência por parte dos executivos de TI ou de SI, que temem - equivocadamente - em ter os resultados desta iniciativa interpretados como desabono ao seu trabalho.

P30-Frequência de Avaliação de Riscos de Segurança da Informação



P31-Execução de Testes de Segurança nos Ambientes Computacionais



Level 3 Security Index - Brasil

Constatações sobre a dimensão de Mitigação

O tema da mitigação recebeu a melhor avaliação no *Level 3 Security Index*. Segundo a avaliação da amostra, as empresas se prepararam para se recuperar de situações adversas de maneira organizada e documentada, minimizando assim os impactos percebidos na ocorrência de um desastre em seus ambientes.

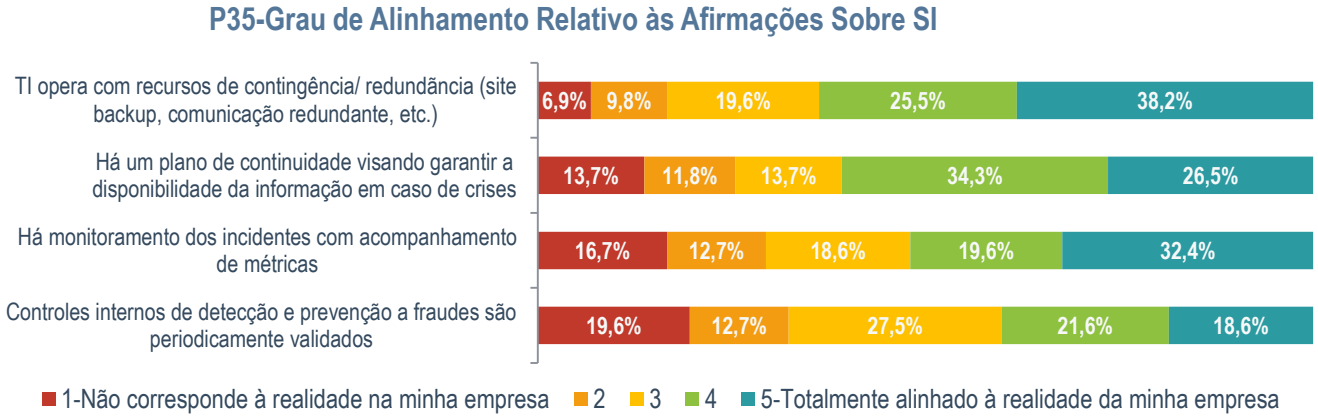
A avaliação dos respondentes ainda indicou que as empresas menores são as quem têm o maior desafio neste tema. Em adição a uma capacidade de reação limitada, vemos também que as capacidades de comunicação e a estrutura de acionamento são, em muitos casos, informais e menos documentadas.

À despeito do resultado geral desta dimensão do índice de maturidade, a acentuação dos esforços neste quesito parece também refletir a lacuna vista no quesito ferramental deste estudo. Como no dito popular, estar preparado é melhor que remediar - mas, lamentavelmente, essa máxima nem sempre é seguida quando o tema é Segurança da Informação.

Level 3 Security Index - Brasil

Prioridade em garantir a continuidade dos negócios

Os esforços para assegurar que os processos de negócios sejam preservados em caso de algum desastre foram evidenciados pelas empresas nas entrevistas para o estudo. A maioria das organizações opera com recursos de contingência (63%) e dispõe de um plano de continuidade (60%) para endereçar essas situações.



Contudo, as ações para prevenção a fraudes ainda não estão tão amadurecidas como os demais temas abordados. As organizações precisam estabelecer essas condutas que possam correlacionar eventos e identificar padrões que, em última análise, podem ser essenciais para a mitigação de um problema e o rápido reestabelecimento das operações.

Level 3 Security Index - Brasil

Estar preparado é chave para reagir de forma adequada

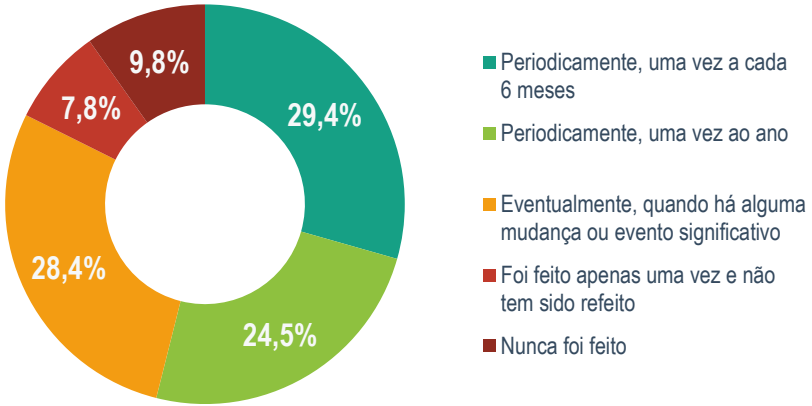
Responder a um incidente de segurança é um trabalho coletivo, que envolve não apenas a área de SI, mas todas as áreas da companhia que possam ser afetadas pelo evento adverso. Essa visão é compartilhada pela grande maioria das empresas consultadas no índice *Level 3 Security Index*, onde mais de 72% delas afirmaram dispor de uma hierarquia definida para acionar os demais envolvidos no caso de um desastre.

Estar preparado também significa garantir que os procedimentos necessários para acionamento das contingências estão atualizados e validados. O estudo mostrou que mais da metade das empresas entendem isso, com cerca de 54% das organizações que checam seus procedimentos ao menos uma vez por ano.

54,9%
Empresas que têm condutas pré-definidas para ação em momentos de ataque (P36).

72,5%
Empresas que dispõem de hierarquia de acionamento das equipes de SI e de outras áreas no caso de algum desastre (P37).

P33-Frequência de Teste/Revisão dos Procedimentos de Contingência

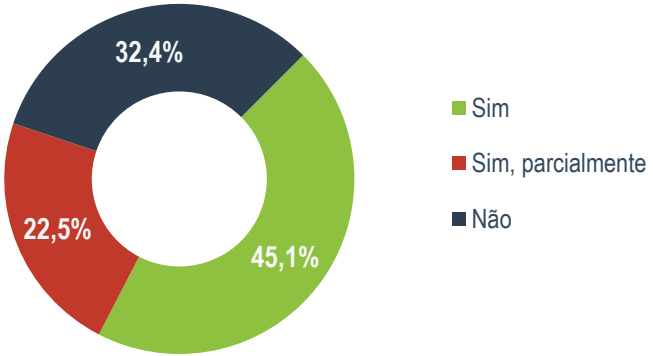


Level 3 Security Index - Brasil

Comunicar adequadamente traz agilidade e transparência

Quando um evento adverso ocorre é comum surgirem dúvidas sobre o que deve ser endereçado prioritariamente e quem precisa ser comunicado sobre os possíveis impactos. Por isso, dispor de uma classificação dos ativos de informação da empresa é importante para assegurar que as ações de reparação sejam executadas de maneira ágil e eficaz.

P34-Existência de Hierarquia Definida Sobre a Importância das Informações



Desastres de segurança, por vezes, trazem incertezas para todos dentro da organização, e, em especial, para aquelas áreas que não estão diretamente envolvidas nessas ocorrências. É nesse momento que um plano de comunicação ajuda a minimizar essas preocupações e faz com que a empresa tenha uma resposta alinhada e única para seus colaboradores e parceiros de negócio.

As pessoas têm um papel de grande importância nas questões de Segurança da Informação; trata-las com clareza e transparência garante que o entendimento da necessidade de SI e de seu valor para os negócios.

60,8%

Empresas que contam com um plano de comunicação para informar as áreas da empresa no evento de um desastre de grandes proporções (P38).

IDC Analyze the Future

Preparado para Level (3) COMMUNICATIONS

BR: 64,9 **AL**: 60-68* **Maduros**: 76-83*

* Pontuação estimada; não houve pesquisa primária.

Level 3 Security Index pelo Mundo

A IDC estimou qual seria a pontuação do índice na América Latina e em países maduros. Trata-se de apenas de uma estimativa, visto que não foram entrevistadas empresas em outros países para determinar o seu atual grau de maturidade.

IDC Analyze the Future

Level 3 Security Index:
O que fazer para superar 64,9 pontos?

O índice de maturidade de segurança na infraestrutura corporativa de TI - *Level 3 Security Index* - avalia o grau de maturidade de Segurança da Informação nas empresas do Brasil. Com base na pontuação obtida e na sua distribuição pelas dimensões do índice, alguns pontos se destacam como ações para avançar em maturidade.

✓ **Considere a contratação de serviços terceirizados e gerenciados.**

Contar com uma equipe especializada e dedicada para lidar com Segurança da Informação pode trazer benefícios em diversos aspectos da gestão desse tema. Como exemplos podemos citar a melhora no acompanhamento e visibilidade de incidentes, o estabelecimento e a gestão de métricas de segurança e a aplicação de um melhor nível de gerenciamento e manutenção dos controles de segurança (sejam eles técnicos ou formais). Adicionalmente, uma equipe terceirizada pode compensar lacunas de capacitação da equipe interna, que poderá até mesmo tirar proveito dessa vivência para aprimorar seus conhecimentos.

✓ **Invista em ferramental que possa viabilizar melhor controle, maior visibilidade e automação.**

Atuar de forma preventiva e preditiva requer um conjunto de ferramentas trabalhando de maneira integrada, que possam analisar os ambientes detalhadamente gerando informações sobre cada evento e cada incidente, e tomando ações corretivas de maneira automatizada sempre que possível. Em última análise, um ferramental bem colocado e dimensionado pode melhorar consideravelmente a eficiência da equipe de SI, gerando oportunidades para que esses profissionais invistam mais tempo em outras frentes e estejam mais próximos das demais áreas da companhia.

Level 3 Security Index:
O que fazer para superar 64,9 pontos?

(continuação)

✓ **Priorize seus investimentos de acordo com a prioridade de cada ambiente, sua classificação de riscos e impactos.**

Adequar a infraestrutura de TI de uma organização às boas práticas de Segurança da Informação pode exigir grandes aportes de recursos, o que nem sempre é viável. A despeito do otimismo em relação aos orçamentos de TI e de SI para 2017, os gestores e C-Level têm o desafio de equilibrar o "wallet share". Assim sendo, o caminho é avaliar seus ambientes e ativos de informação, planejando seus investimentos prioritários naqueles de maior criticidade e que representam maior risco para sua empresa.

✓ **Tangibilize os benefícios da Segurança da Informação por meio de indicadores bem definidos.**

Demonstrar o retorno do investimento em Segurança da Informação é uma tarefa árdua, mas não impossível. Defina e acompanhe indicadores de SI que possam mostrar como essas iniciativas evitaram indisponibilidade, vazamento de informações, prejuízo à marca da companhia, entre outros. De posse dessas métricas, divulgue-as nas campanhas de conscientização em alinhamento com a alta direção da empresa, e faça com que todos os colaboradores as entendam e sintam-se corresponsáveis pelos resultados atingidos.

✓ **Faça testes de segurança com maior frequência e abrangência.**

Os testes de segurança são um dos principais aliados do gestor de SI, pois eles apontam com clareza e transparência onde estão as vulnerabilidades e como combate-las. Muitos fornecedores chegam a oferecer esse serviço gratuitamente, o que pode ser especialmente importante no momento em que se necessita um motivador adicional para validar e aprovar um projeto.

Obrigado!

Contato:

Luciano Ramos
Software Research Coordinator
lramos@idc.com
55 11 5508-3405