Ernst & Young agora é EY.

APOIADOR OFICIAL

TM Rio 2016

# Mantenha-se à frente do crime cibernético

## Pesquisa Global da Ernst & Young sobre Segurança da Informação 2014

**Insights sobre governança, risco e compliance**

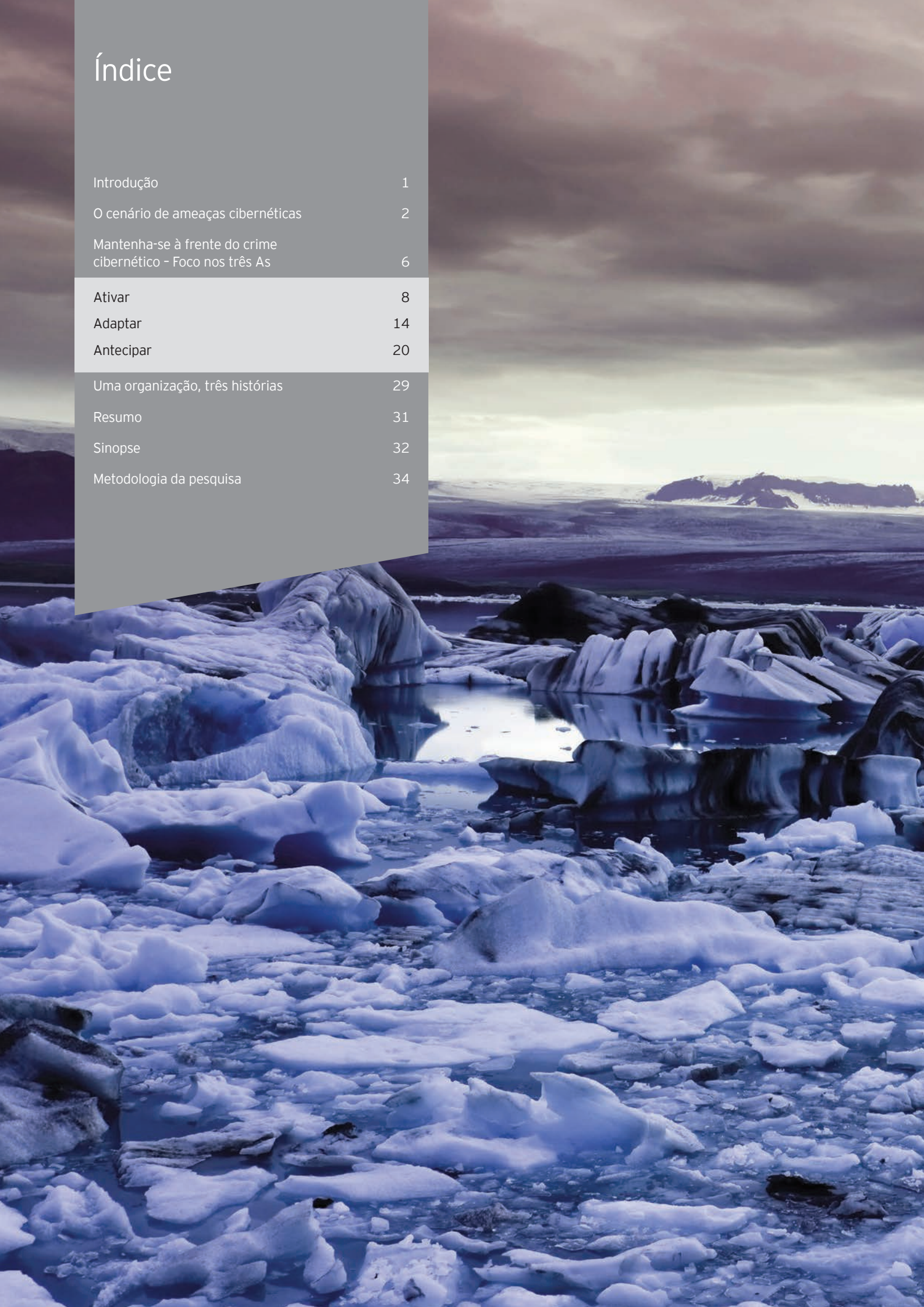
Outubro de 2014

EY

Building a better working world

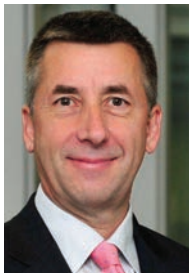
# Índice





# Introdução

Paul van Kessel
Líder global de Riscos
da Ernst & Young



Ken Allan
Líder global de
Segurança Cibernética
da Ernst & Young

## Bem-vindos ao *Mantenha-se à frente do crime cibernético*

Antecipar-se aos ataques cibernéticos é a única forma de colocar-se à frente dos criminosos cibernéticos. Essa é a nossa mensagem hoje para as empresas de todo o mundo, baseada nas respostas de 1.825 organizações à nossa 17ª Global Information Security Survey – GISS (em português, Pesquisa Global de Segurança da Informação), que neste ano foca na maneira como as organizações estão administrando as ameaças cibernéticas e o que elas precisam fazer para se manter à frente de ações criminosas.

Reportagens na mídia ilustram frequentemente que as ameaças cibernéticas estão elevando seus níveis de persistência, sofisticação e organização; e os prejuízos causados por esses ataques podem impactar fortemente os negócios. Como abordamos no relatório da GISS de 2013, mesmo não tendo ainda vivido a experiência de um ataque cibernético, você deve assumir que a sua organização será um alvo, ou até que a sua segurança já foi violada.

Na nossa pesquisa de 2014, descobrimos que as organizações estão fazendo progressos ao estabelecer os alicerces da segurança cibernética – e esse progresso é muito importante. Entretanto, a maioria dos pesquisados relatou ter apenas um nível "moderado" de amadurecimento nessa área. Ainda há muito a ser feito.

A pesquisa também mostrou que mais organizações estão olhando além do básico na sua abordagem à segurança cibernética. Essas instituições estão se adaptando à medida que mudam suas estratégias de negócios e operações (por exemplo, fusões, aquisições, introdução de novos produtos, entrada em novos mercados e implantação de novos softwares), ou de acordo com o ambiente externo dos negócios. Mas sabemos que elas também precisam mudar a sua forma de pensar para não serem apenas reativas às futuras ameaças.

Com base nos fatos acima mencionados, estruturamos o relatório da pesquisa deste ano para acompanhar a jornada de segurança cibernética:

- **Ativar**
  Essa parte do relatório aborda os fundamentos da segurança cibernética. Qual é a situação em 2014 e quais são os elementos mais importantes, que merecem mais atenção?
- **Adaptar**
  A seguir, focaremos na mudança. O que as organizações estão fazendo para adaptar suas medidas de segurança cibernética? Essas organizações continuarão a se defender de ameaças com sucesso, apesar da constante mudança e integração de tecnologias mais avançadas?
- **Antecipar**
  A última parte do relatório aborda como as organizações líderes podem atingir um estado de prontidão, tendo confiança nas suas avaliações de riscos e ameaças e na sua preparação para o que está por vir. Em outras palavras: como se antecipar e se manter à frente do crime cibernético.

Nessa jornada, as organizações deverão deixar de ser um alvo fácil para se tornarem algo muito mais respeitável. E, dessa forma, elas estarão – pela primeira vez – verdadeiramente preparadas contra os ataques cibernéticos.

Gostaríamos de acrescentar uma nota pessoal de agradecimento a todos os participantes da pesquisa. Agradecemos pelo tempo dedicado às respostas e por compartilhar suas experiências conosco. Também serão bem-vindos seus comentários sobre este relatório.

Todas as organizações estão expostas ao risco de ataques cibernéticos. Por isso, vamos continuar essas discussões juntos.

**Paul van Kessel**
Líder global de Riscos
da Ernst & Young
paul.van.kessel@nl.ey.com

**Ken Allan**
Líder global de Segurança
Cibernética da Ernst & Young
kallan@uk.ey.com

# O cenário de ameaças cibernéticas


Pesquisa Global de Segurança da Informação de 2013
Sob Ataque Cibernético
www.ey.com/giss2013


Pesquisa Global de Segurança da Informação de 2012
Lutando para reduzir o gap
www.ey.com/giss2012

## O desaparecimento do perímetro

As ameaças cibernéticas continuam a se multiplicar. O advento do mundo digital e a inerente interconectividade das pessoas, dispositivos e organizações abrem um leque totalmente novo de vulnerabilidades. Em nossas Pesquisas Globais de Segurança da Informação de 2012 (Lutando para reduzir o gap) e 2013 (Sob ataque cibernético), descrevemos essa tendência.

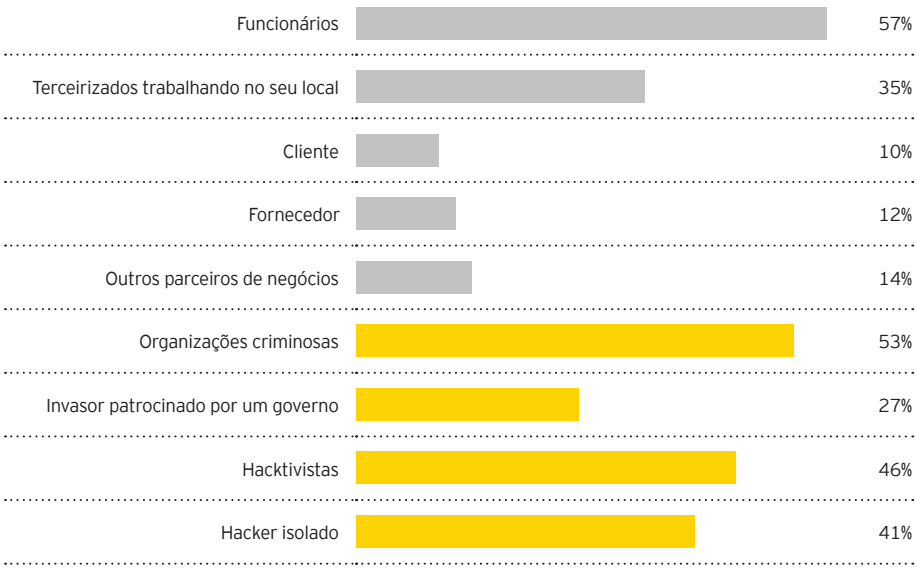
O breve resumo abaixo destaca as cinco principais razões pelas quais a segurança cibernética efetiva está cada vez mais difícil de atingir. Elas demonstram que as defesas de segurança das organizações estão sob crescente pressão, extrapolando os limites tradicionais e, assim, motivando cada vez mais os agentes das ameaças.

| | | |
|---|---|---|
| 1 | Mudança | No mundo pós-crise econômica, os negócios precisam se movimentar rapidamente. Os lançamentos de novos produtos, fusões, aquisições e a introdução de novas tecnologias estão em alta. Essas mudanças invariavelmente causam impactos complicados na solidez da segurança cibernética das organizações. |
| 2 | Mobilidade e acessibilidade | A adoção da computação móvel resultou na dissipação das fronteiras das organizações, com a área de TI aproximando-se cada vez mais dos usuários e distanciando-se, assim, das organizações. O uso da internet, smartphones e tablets, em combinação com a política de BYOD (do inglês: Bring Your Own Device, ou "Traga Seu Próprio Dispositivo") tornou os dados das organizações acessíveis em qualquer lugar. |
| 3 | Ecossistema | Vivemos e operamos num ecossistema de entidades, pessoas e dados digitalmente conectados, ampliando a possibilidade de exposição aos crimes cibernéticos, seja em casa, seja no trabalho. |
| 4 | Nuvem | Os serviços baseados em nuvem e o gerenciamento e armazenamento de dados terceirizados abrem novos canais de risco, que anteriormente não existiam. |
| 5 | Infraestrutura | Os sistemas de tecnologia de automação, anteriormente isolados, agora estão recebendo endereços IP. Por isso, as ameaças cibernéticas vêm fazendo incursões fora dos sistemas de back-office e em infraestruturas críticas, como os sistemas de geração de energia e transportes, além de outros sistemas de automação. |

## O crescente poder de ataque dos criminosos cibernéticos

O poder de ataque dos criminosos está aumentando em velocidade espantosa. Eles têm acesso a recursos significativos, tornaram-se mais pacientes e sofisticados do que antes, e estão procurando vulnerabilidades em todo o ambiente operacional – inclusive pessoas e processos.

**Quem ou o que você considera a fonte mais provável de um ataque?**




Nas nossas pesquisas anteriores, os funcionários eram considerados a fonte mais provável de ataques. Na GISS deste ano, eles ainda são vistos como um risco importante. Entretanto, pela primeira vez descobrimos que, quando diferentes tipos de criminosos externos são combinados (organizações criminosas, agressores patrocinados por um governo, hacktivistas e hackers isolados), essas ameaças passam a ser consideradas significativamente como fonte mais provável de risco. Praticamente, todos os pesquisados sofreram um ou mais ataques externos incluídos nessa classificação.

## Obstáculos enfrentados pelas organizações de hoje

Nas seções seguintes deste relatório, vamos abordar o que as organizações estão fazendo para enfrentar esses desafios. Primeiro, precisamos considerar quais obstáculos precisam ser removidos antes de uma organização ser bem-sucedida e tomar a dianteira em relação ao crime cibernético.

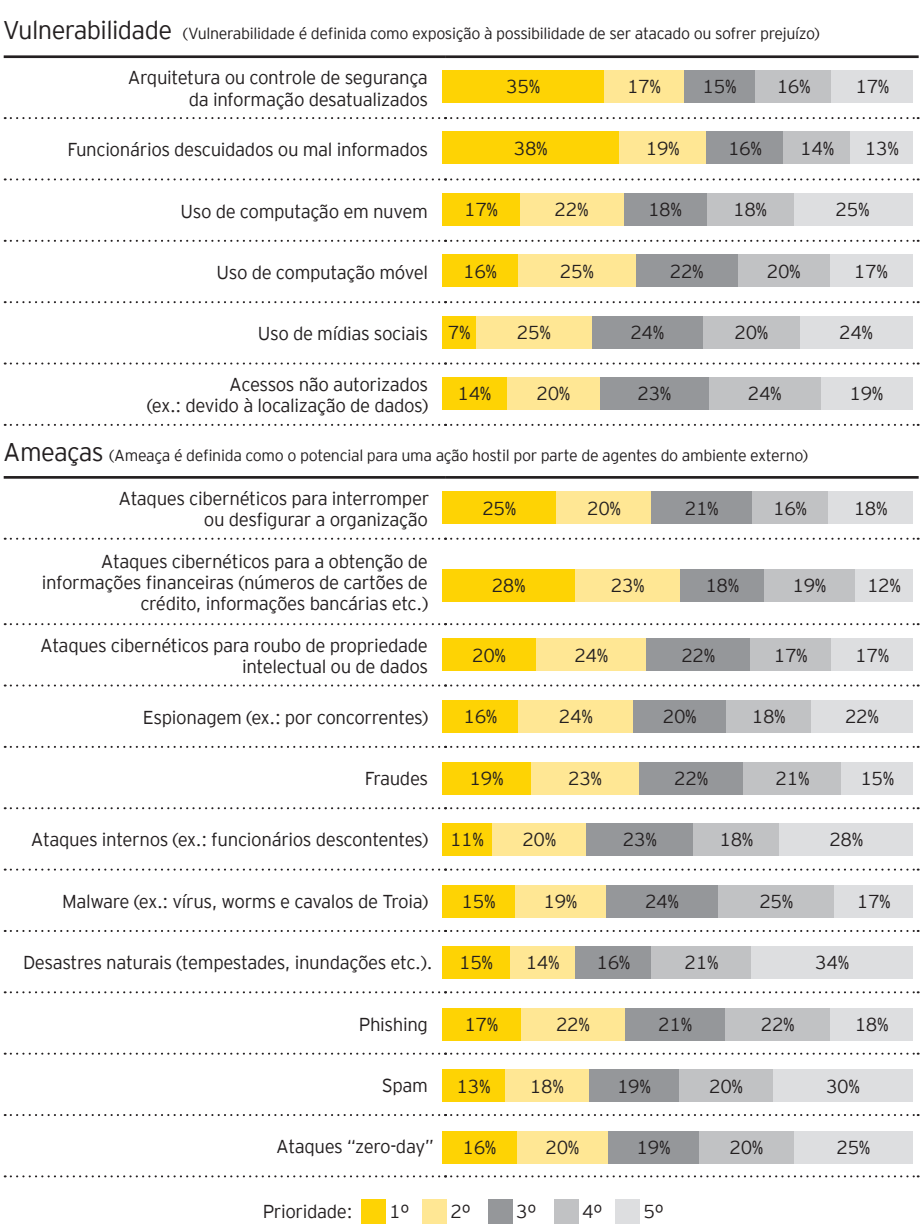
### Obstáculo 1 – Falta de agilidade

As ameaças não somente estão aumentando, como os respondentes da pesquisa também nos informam que ainda existem vulnerabilidades conhecidas nas suas defesas cibernéticas. Em outras palavras, entende-se que existe um perigo claro e presente, mas as organizações não estão se movimentando com velocidade suficiente para mitigar as vulnerabilidades conhecidas – 37% informaram não ter insights dos riscos cibernéticos em tempo real, e para outros 27% isso ocorre apenas "algumas vezes". Como resultado, as organizações estão ficando para trás na criação de seus fundamentos de segurança cibernética. *Leia a seção "Ativar" para saber mais sobre as áreas que requerem maior atenção, de acordo com a nossa pesquisa.*

## últimas notícias

A combinação de ataques externos agora é uma fonte de risco muito mais provável do que as ameaças internas

**Quais ameaças e vulnerabilidades mais aumentaram a sua exposição ao longo dos últimos 12 meses?**







**43%**

dos pesquisados apontam que os orçamentos totais de segurança da informação de suas organizações permanecerão os mesmos nos próximos 12 meses e 5% afirmaram que o orçamento atual diminuirá.

**53%**

das organizações informaram que a falta de mão de obra especializada é um dos obstáculos para a segurança da informação.

## Obstáculo 2 – Falta de orçamento

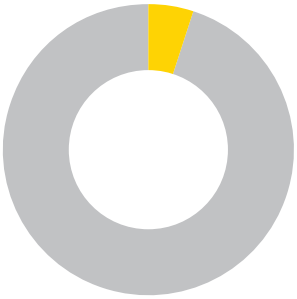
Como vimos antes, a falta de orçamento é um dos obstáculos mais desafiadores. Nos anos anteriores, estávamos relativamente certos de que os orçamentos disponíveis para a segurança cibernética dariam conta do que era necessário fazer, já que havíamos detectado um aumento ano a ano dos orçamentos para segurança cibernética. Agora, pela primeira vez, encontramos mais organizações informando que seus orçamentos permanecerão os mesmos.

Embora haja maior atenção em relação aos crimes cibernéticos entre diretores ao redor do mundo, parece que esse interesse não se traduz em recursos orçamentários adicionais. Não obstante, ainda existe a necessidade de mais dinheiro e maiores recursos para enfrentar de forma efetiva as crescentes ameaças.

### Obstáculo 3 – Falta de capacitação em segurança cibernética

O principal obstáculo é a falta de capacitação em segurança cibernética. Enquanto a necessidade de especialistas aumenta, ano após ano nossa pesquisa demonstra que cresce, também, a carência por mão de obra especializada. É necessário, ainda, desenvolver habilidades em disciplinas não técnicas a fim de integrar a segurança cibernética ao core business da empresa.

Organizações sofisticadas não apenas se defendem contra ataques cibernéticos, mas utilizam inteligência analítica para prever o que poderia ocorrer e têm confiança suficiente em seu ambiente de operações para saber que estão preparadas (*para mais informações, leia a seção "Antecipar"*). Entretanto, a nossa pesquisa aponta que é muito difícil contratar os especialistas necessários para executar a análise das ameaças, estabelecer conclusões relevantes e aplicáveis, elaborar respostas e fornecer subsídios para as decisões a serem tomadas.



5%

das organizações tem uma equipe de inteligência de ameaças com analistas dedicados e consultores externos que avaliam informações para credibilidade, relevância e exposição contra os agentes das ameaças.

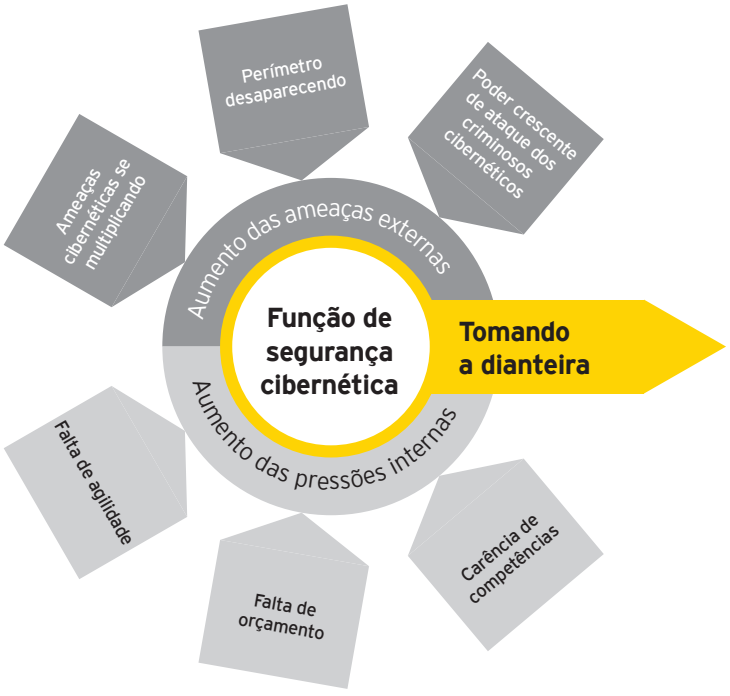
### A crescente ameaça à tecnologia de automação

A resiliência dos sistemas de tecnologia de automação (TA) – tais como como geradores de energia, sistemas de transporte, sistemas de controle de voo e sistemas de distribuição de gás – torna-se ao mesmo tempo mais importante e desafiadora. Novas tecnologias, pressão regulatória e mudanças nos requisitos dos negócios exigem maior segurança cibernética. Entretanto, a proteção dos sistemas de TA não é uma tarefa fácil, devido à complexidade dos ambientes, sistemas legados, diferentes fornecedores e diferenças culturais entre as equipes de TA e TI.

Devido à relativa facilidade de acesso por intermédio de endereços IP, os sistemas de TA tornam-se alvos frequentes de criminosos cibernéticos e poderiam ser incluídos em uma abordagem da organização para aperfeiçoar a maturidade cibernética. Exemplos de ataques incluem:

- Infecção de vírus tipo worm nos sistemas de controle de processo de uma rede ferroviária, provocando a utilização não confiável das linhas férreas;
- Acesso ao sistema de gerenciamento de uma instalação bancária e manipulação do sistema de ar-condicionado do prédio que provoque a queda dos servidores devido ao superaquecimento;
- Malware que destrua os sistemas de controle de uma usina elétrica nuclear, ou os controles de processos de exploração e produção de uma empresa de óleo e gás.

Considerando o que vimos até aqui (resumido neste diagrama), verificamos que está ocorrendo uma rápida expansão das ameaças. O poder dos criminosos cibernéticos está aumentando, e as organizações lutam contra inúmeros obstáculos. Sabemos que não é fácil manter-se à frente do crime cibernético.



# Mantenha-se à frente do crime cibernético

Nos capítulos seguintes, abordaremos os três diferentes estágios da jornada para a maturidade em segurança cibernética – Ativar, Adaptar e Antecipar (os três As) –, que devem ser seguidos à risca (e aplicados de forma consistente) para se atingir uma segurança cibernética de ponta.

Observamos que as respostas das organizações aos crimes cibernéticos consistem em três estágios distintos. O objetivo deve ser implementar medidas cada vez mais avançadas de segurança em cada um desses estágios.


## Ativar

As organizações precisam dispor de uma base sólida de segurança cibernética. Isso compreende um abrangente conjunto de medidas de segurança da informação, que proporcionarão uma defesa básica (mas não ideal) contra os ataques. Nesse estágio, as organizações estabelecem as suas bases, ou seja, "ativam" a sua segurança cibernética.

### Fundamental

Segurança cibernética **acoplada**

Foco na proteção do ambiente **atual**

Abordagem **estática**

| Onde estou? | *Leia as caixas abaixo e identifique quantas características da sua organização atendem ao perfil Ativar* |
|---|---|
| Gestão de incidentes | ☐ Nunca houve um incidente<br>☐ Terceiro libera informações publicamente ou notifica você<br>☐ Incerto sobre quem deverá responder<br>☐ Não há uma pessoa especialmente designada para divulgar publicamente as informações<br>☐ Não há um plano de resposta para incidentes |
| Discussões da liderança | ☐ Não é um tema para a diretoria<br>☐ As conversas da liderança são focadas em ferramentas e políticas<br>☐ A empresa não se engaja como uma equipe líder em segurança |
| Métricas | ☐ Número de pessoas<br>☐ Modelos de maturidade<br>☐ Orçamento<br>☐ Compliance |

# Foco nos três As

## Adaptar

As organizações mudam para sobreviver ou crescer, as ameaças também. Dessa forma, os pilares das medidas de segurança da informação também têm de se adaptar para manter o ritmo e atender às mudanças nas exigências e na dinâmica dos negócios, ou ao longo do tempo se tornarão cada vez menos efetivos. Nesse estágio, as organizações trabalham para manter a sua segurança cibernética atualizada, isto é, se "adaptam" às necessidades de mudança.

## Antecipar

As organizações precisam desenvolver táticas para detectar e diminuir potenciais ataques cibernéticos. Elas precisam saber exatamente o que deve ser protegido (as suas "joias da coroa") e ensaiar respostas apropriadas para cenários de prováveis ataques/incidentes (inclusive acidentes). Para tanto, necessitam de uma capacitação madura de inteligência para enfrentar as ameaças cibernéticas, uma metodologia sólida de avaliação de risco, um mecanismo de resposta a incidentes com experiência e uma organização bem informada. Nesse estágio, as organizações sentem-se mais confiantes em relação à sua capacidade de enfrentar as ameaças mais previsíveis e os ataques inesperados, isto é, elas "previnem" a ocorrência de ataques cibernéticos.

| **Dinâmico** | **Proativo** |
|---|---|
| Segurança cibernética incorporada **(built-in)** | Segurança cibernética incorporando o futuro **(built-beyond)** |
| Foco na **mudança** do ambiente | Foco no ambiente **futuro** |
| Abordagem **dinâmica** | Abordagem **proativa** |
| *Leia os itens abaixo e verifique quantas destas características da sua organização se enquadram no perfil Adaptar.* | *Leia os itens abaixo e verifique quantas destas características da sua organização se enquadram no perfil Antecipar.* |
| ☐ A organização identifica e reage aos seus próprios incidentes<br>☐ Notificações de participação no plano de resposta a incidentes<br>☐ Time de resposta a incidentes inclui a liderança de TI<br>☐ Relações públicas definidas<br>☐ A aceitação de que uma violação ocorrerá, ou já ocorreu | ☐ A organização se prepara para violações futuras baseada nos cenários de ameaças<br>☐ A liderança sênior da corporação faz parte da equipe de resposta<br>☐ A comunicação externa é controlada e suas posições baseiam-se em fatos defensáveis |
| ☐ Planos de recuperação de desastre<br>☐ Ambiente regulatório e impactos<br>☐ A liderança em TI e os líderes da empresa discutem a realidade da ocorrência da falha e seu impacto | ☐ Item permanente na diretoria<br>☐ A liderança de TI e os líderes da empresa discutem como a segurança pode melhorar os negócios<br>☐ Cooperação entre pares no nível de liderança |
| ☐ Ataques/incidentes<br>☐ Impacto da violação na receita<br>☐ Análise avançada de risco e pontuação | ☐ Apoio ao crescimento e proteção da receita por meio da segurança<br>☐ Alinhamento aos objetivos do negócio |

## Estabelecendo os alicerces

Cada organização necessita de uma base sólida de segurança cibernética. Concretizá-la não é uma tarefa fácil, e as especificações das necessidades vão depender de questões como o setor de atividade e a localização geográfica. Isso não é novidade: no relatório da nossa Pesquisa Global de Segurança da Informação de 2012 (*Lutando para reduzir o gap*), exploramos o gap entre as medidas de segurança cibernética realmente adotadas e os componentes fundamentais de defesa que deveriam ser agregados. Esses fundamentos proporcionam o primeiro passo na jornada de segurança cibernética.

# Ativar


As organizações que ativaram os fundamentos para a segurança cibernética, mas não foram além disso, tipicamente apresentarão as seguintes carências em sua capacitação, demonstrando por que a jornada precisa continuar.

### 1. Segurança cibernética acoplada (*bolt-on*)

A segurança cibernética da organização tem sido acrescentada aos processos de negócios e às atividades. Mas ela não foi ainda integrada no negócio, não é vista como atividade de valor agregado e, sim, como um fator de custo que deve ser limitado tanto quanto possível. Se o desenvolvimento de aplicações é apenas sobre a obtenção de certificação de segurança após a conclusão do desenvolvimento ou após pontos de decisão, a organização está estagnada aqui, com uma segurança acoplada (*bolt-on*).

### 2. O foco na proteção do ambiente atual

Esse nível de fundamento para a segurança cibernética começa com uma avaliação dos riscos que a organização já conhece, com base na sua experiência anterior. O objetivo é assegurar que estejam em vigor medidas que resolverão qualquer fraqueza.

Se as conversas forem apenas sobre as avaliações de risco, eficiência de controles e mitigação de riscos, a organização permanecerá no nível Ativar.

### 3. Abordagem estática

Esse nível de capacitação em segurança cibernética destina-se a permitir que a empresa desempenhe, de forma segura, as suas funções conhecidas e regulares do dia a dia. A organização será baseada em regras e focada em compliance, confiando em relatórios orientados por indicadores – e só poderá enfrentar ameaças em um mundo sem mudanças.

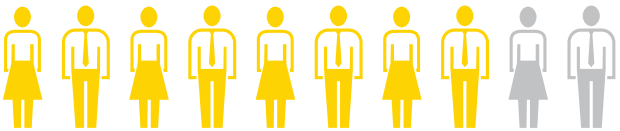
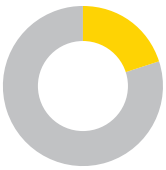
Todas as empresas, independentemente de seu estágio de desenvolvimento no assunto, precisam alcançar o domínio dos requisitos fundamentais da segurança cibernética.

Entretanto, a nossa observação baseada na pesquisa realizada este ano indica que muitas organizações ainda não dispõem de todos os componentes fundamentais de segurança cibernética ativados.

Neste relatório decidimos focar em cinco áreas críticas. Como mostrou a pesquisa deste ano e a experiência da Ernst & Young ao trabalhar com nossos clientes globais, estes são os pontos onde podem surgir os maiores problemas:

- Adesão de executivos
- Recursos
- Desempenho
- Acesso aos dados
- Custos x Valor

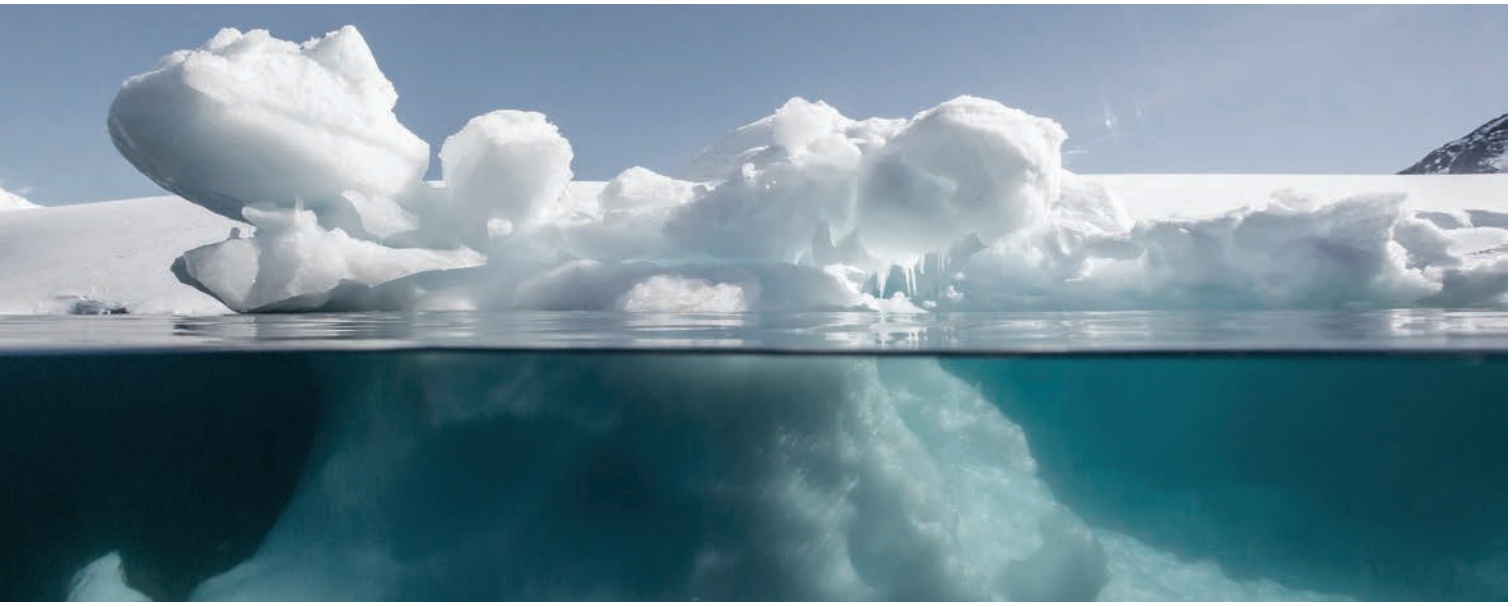
| Item | Quais são os temas? |
|---|---|
| Adesão de executivos | ▸ A liderança na estratégia, planejamento e execução da segurança cibernética vem de níveis organizacionais mais baixos ou é considerada um problema de TI.<br>▸ Não há um sistema consistente de gestão de ameaças. As ameaças não são discutidas regularmente pela alta administração. |
| Recursos | ▸ As tarefas de segurança cibernética não contam com recursos adequados e/ou não são desempenhadas por pessoal qualificado.<br>▸ As equipes de segurança cibernética não identificam nem ficam sabendo dos ataques. |
| Desempenho | ▸ Muitas organizações são amplamente superficiais: mantêm excesso de capacidades cibernéticas, mas com eficácia moderada.<br>▸ A eficácia da segurança cibernética não é medida. |
| Acesso aos dados | ▸ Os funcionários são um risco para a segurança cibernética, e o programa de gestão de suas identidades e acessos (IAM, na sigla em inglês) é fraco.<br>▸ O excesso de procedimentos manuais e a falta de regularidade nas revisões e relatórios fazem com que funcionários tenham acesso indevido aos dados.<br>▸ Pessoas que se movimentam, deixam ou chegam à empresa são uma área importante de risco cibernético. |
| Custos x Valor | ▸ Muitas organizações consideram os custos da segurança cibernética muito altos.<br>▸ As organizações não valorizam os benefícios das medidas que já adotam.<br>▸ As organizações subestimam de forma significativa os custos de um potencial ataque cibernético. |

| Resultados da Pesquisa | Implicações |
|---|---|
|  Aproximadamente 80% dos CIOs ou departamentos de TI têm a função de segurança subordinada diretamente a eles e apenas 14% se reportam diretamente ao CEO. | ▸ As organizações precisam envolver a liderança sênior na segurança cibernética.<br>▸ A falta de adesão dos executivos abre as portas para erros e criminosos cibernéticos; a segurança cibernética perderá o direcionamento e os investimentos necessários. |
|  Menos de 20% das organizações possuem insights reais sobre os riscos cibernéticos iminentes.<br>  20% compartilharam prontamente as fontes de ataques cibernéticos com seus colegas de trabalho. | ▸ As ameaças cibernéticas não são notadas ou a resposta é muito tardia.<br>▸ Os criminosos cibernéticos bem-sucedidos na utilização de *phishing* são resultado da falta de conscientização sobre segurança. |
|  De 35% a 45% dos entrevistados avaliaram que quase todo o processo de segurança cibernética "ainda precisa melhorar muito". | ▸ Os processos fundamentais de segurança cibernética não estão funcionando de forma adequada, deixando uma ampla gama de opções para aqueles que executam uma ameaça avançada persistente (APT, na sigla em inglês). |
|  Aproximadamente dois terços das organizações não têm programas de IAM bem definidos e automatizados. | ▸ Vimos que os funcionários são uma enorme ameaça para a segurança cibernética. Enquanto as organizações procuram hackers vindos do ambiente externo, as fraudes já ocorrem dentro da empresa. |
|  63% citam as limitações do orçamento como o principal obstáculo para contribuir e agregar valor.<br>  Aproximadamente 50% não preveem um aumento do orçamento de riscos nos próximos 12 meses. | ▸ As organizações precisam entender que são atacadas diariamente e que os criminosos não demonstram sinais de desistência – estão se tornando mais astutos e direcionados. A próxima brecha pode ser fatal. |

## Atividades fundamentais que todas as organizações devem "ativar"

As organizações que ainda não atingiram o nível básico em segurança cibernética devem agir rapidamente. Para ajudá-las, listamos abaixo as seis ações críticas mais frequentemente negligenciadas que precisam ser consideradas com urgência:

1. **Avaliação e roteiro de segurança**
   Avaliação das ameaças cibernéticas, do estado atual de maturidade, definição do objetivo a ser alcançado, análise do gap e programa de implementação do roteiro, alinhado com as melhores práticas, como a ISO 27001;
2. **Obter o suporte da diretoria para a transformação da segurança**
   Redefinir a governança da segurança cibernética (por exemplo, realinhando a segurança cibernética fora da função de TI) e assegurar o entendimento do processo pela alta administração;
3. **Rever e atualizar as políticas, procedimentos e padrões de suporte de segurança**
   Implantar o sistema de gestão da segurança da informação (ISMS, em inglês);
4. **Criar um Centro de Operações de Segurança (SOC, do inglês: Security Operations Center)**
   Desenvolver o monitoramento dos casos conhecidos e os procedimentos de resposta em caso de incidentes;
5. **Planejar e implantar os controles de segurança cibernética**
   Avaliar a eficácia dos processos de prevenção de perda de dados e IAM. Reforçar a segurança dos ativos de TI, como servidores e firewalls, componentes de rede e bancos de dados;
6. **Testar os planos de continuidade dos negócios e procedimentos de resposta a incidentes**
   Estimular testes regulares de invasão da rede, pontos de entrada e aplicações; identificar as fraquezas que podem ser exploradas.



# O Centro de Operações de Segurança

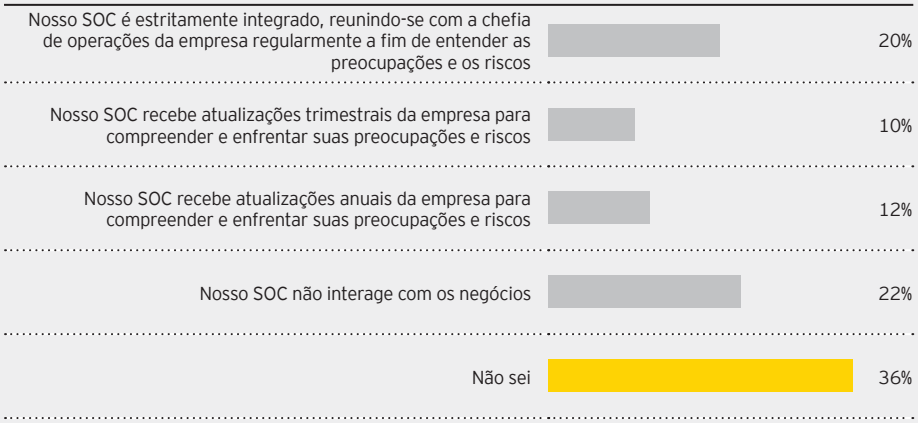
Os processos e a tecnologia que dão suporte à função de Segurança da Informação constituem parte vital e fundamental da segurança cibernética. Esses componentes são mais eficazes quando centralizados, estruturados e coordenados. Por isso, o Centro de Operações de Segurança (SOC) é um ponto de partida valioso. Embora o SOC possa ser terceirizado, é importante assegurar-se de que ele atenda às necessidades operacionais da sua empresa – estamos assistindo a uma transição clara de um "modelo genérico de SOC" para um modelo personalizado – e que o seu conhecimento das ameaças de segurança cibernética e questões correlatas seja constantemente atualizado e alinhado com a estratégia de negócios.

É preocupante saber que mais de 40% das organizações pesquisadas não possuem SOC. E, para aquelas que têm, os benefícios da centralização não são atingidos, comunicados ou compreendidos pelas organizações. Mais da metade dos pesquisados foi incapaz de responder à pergunta sobre quanto o SOC atendeu às necessidades de operações do seu negócio, ou declarou que isso era desconhecido, ou que o SOC não interagia com o negócio.

42%

das organizações não têm SOC

**Como o seu SOC garante estar de acordo com as necessidades operacionais do seu negócio?**

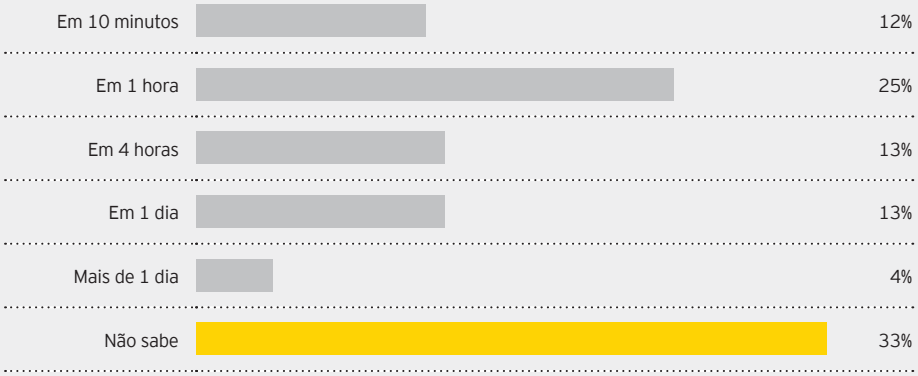



37%

afirmam que não é possível perceber o risco cibernético em tempo real

Há uma falta de conscientização sobre como o SOC se mantém atualizado em relação às ameaças mais recentes. Mais de 50% dos pesquisados ou não souberam responder à pergunta, ou não sabiam quanto tempo o SOC levaria para iniciar uma investigação sobre um incidente descoberto ou um alerta. Antes que qualquer melhoria possa ser solicitada ou determinada, as organizações precisam ter mais informações sobre o trabalho do SOC.

**Quanto tempo em média o SOC leva para iniciar uma investigação sobre um incidente descoberto ou um alerta?**

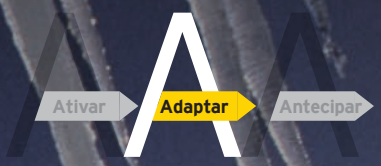



De maneira geral, a infraestrutura de tecnologia e os terminais do SOC precisam ser melhorados. Se a maioria dos benefícios do SOC fosse obtida, a capacidade de proteção das organizações, mesmo nas funções mais básicas, começaria a trazer benefícios.

## Adote uma abordagem dinâmica

As organizações que implantaram os fundamentos da segurança cibernética iniciaram a jornada, mas, para permanecer competitiva, uma empresa precisa mudar constantemente e adaptar-se ao ambiente mutável dos negócios e à consequente evolução das ameaças. Como resultado, os requisitos de segurança cibernética também devem mudar – alterando a infraestrutura de controle e a capacitação/uso da tecnologia para apoiar a melhoria da consciência dos riscos conhecidos. Se a organização não se adaptar, sua base de segurança cibernética ficará rapidamente obsoleta.

# Adaptar




O estágio Adaptar acrescenta as seguintes características ao nível Ativar:

1. **Segurança incorporada (*built-in*)**
   A segurança cibernética é considerada e envolvida em tudo o que a organização faz: seja no desenvolvimento de um novo processo de negócios, na abertura de uma nova fábrica, na aquisição ou introdução de um novo produto. Mudanças nos negócios são imediatamente avaliadas sob a perspectiva da segurança cibernética, e as necessidades de mudança da segurança cibernética estão incorporadas (*built-in*) em todos os processos da empresa. Como resultado, a segurança será atualizada continuamente.

2. **Foco no ambiente em mudança**
   Uma segurança cibernética mais madura adapta-se continuamente às mudanças nos negócios e na estrutura. Por exemplo: entrar na era digital ou utilizar os serviços em nuvem pode acarretar riscos desconhecidos pela organização até então. O aumento da conscientização da situação atual permite à avaliação de risco incorporar mudanças internas e ser capaz de reagir às mudanças esperadas no cenário de ameaças.

3. **Abordagem dinâmica**
   A segurança cibernética da organização é flexível, ágil, atualizada constantemente e adapta-se continuamente para uma melhor proteção dos negócios e da empresa.

## Ciclo de melhoria: abordagem para a adaptabilidade

As organizações estão em constante mudança. A seguir, alguns exemplos:

- A necessidade de integrar novas tecnologias (digital, mídias sociais, nuvem, big data etc.) aos processos de negócio;
- O aumento exponencial dos dispositivos móveis (BYOD) enfraquece a distinção entre o ambiente empresarial e o pessoal;
- O crescimento dos serviços gerenciados e da hospedagem remota, com maior dependência de aplicativos complexos (muitos hospedados remotamente);
- Integração do controle da infraestrutura de processos com o back-office e o ambiente externo;
- Rápidas mudanças no ambiente e nos requisitos regulatórios.

Como resultado, as organizações têm de enfrentar um ciclo interminável de novas ameaças e desafios que requer a adoção de um ciclo interminável de renovação, aperfeiçoamento e reavaliação dos recursos de segurança cibernética.

As organizações devem estabelecer um sistema que permita gerenciar esse ciclo de maneira eficiente e eficaz, para se beneficiarem ao abraçar novas/diferentes oportunidades de segurança, que, por sua vez, permitirão que a empresa habilite seus negócios e reduza seus custos.

### O ciclo de melhoria

## Usando o passado para entender o presente

Para tomar a dianteira em relação ao crime cibernético, é essencial manter as medidas de segurança 100% alinhadas ao seu negócio. Esse desafio já é prioritário na agenda há muito tempo, e melhorias têm sido feitas ano a ano. Entretanto, pela primeira vez em cinco anos, a pesquisa GISS nos mostrou que as organizações estão efetivamente olhando para trás. Elas melhoram continuamente a sua segurança cibernética, mas as mudanças no cenário das ameaças (*leia o capítulo 1 deste relatório*) viajam a velocidades ainda mais rápidas. Há dois anos, já previamos essa tendência*. Isso indica também que as organizações estão se tornando cada vez mais conscientes da realidade das ameaças – por intermédio da imprensa ou de experiências pessoais.

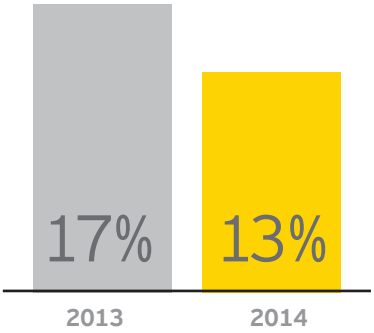
Neste ano, a nossa pesquisa GISS identificou que:

- 13% dos pesquisados relataram que a sua função de Segurança da Informação atende totalmente às necessidades das suas organizações – esse percentual caiu em relação aos 17% da pesquisa de 2013.
- No ano passado, 68% dos pesquisados sentiram que a sua função de "Segurança da Informação atendeu parcialmente às suas necessidades e que melhorias estavam a caminho". O quesito caiu para 63% neste ano.

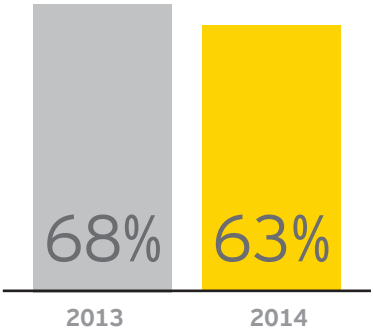
Esses resultados mostram que as organizações precisam levar mais a sério a segurança cibernética. A utilização do ciclo de melhoria aqui descrito as ajudará a retomar o caminho certo.

Nossa pesquisa também avaliou por que as medidas de segurança cibernética não estão atendendo às necessidades de tantas organizações, por exemplo, na detecção de violações:

**Que afirmação descreve melhor a maturidade do seu programa de detecção de violações?**


Ao contrário de um esperado aumento no número de organizações que informam que suas funções de Segurança da Informação atendem integralmente às suas necessidades, nossa pesquisa encontrou uma redução nesse número.




Ao contrário de um aumento no número de organizações que informam que suas funções de Segurança da Informação atendem parcialmente às suas necessidades e que melhorias estão a caminho, esse número teve um decréscimo de 5%.

## Como fazer melhorias vitais?

Então, quais são as áreas que necessitam de mais atenção específica?

O que estaria mais facilmente ao alcance das organizações para elas progredirem facilmente?

### 1. Melhorar o Centro de Operações de Segurança (SOC)

Um SOC com bom funcionamento é um ativo importante para passar à frente do crime cibernético. Se houver uma função de segurança que deva conhecer as ameaças mais recentes, é o SOC. De forma mais ampla, apenas um terço dos pesquisados sente que seu SOC está se mantendo atualizado sobre as últimas ameaças – o que significa um resultado alarmante.

Uma das principais causas é que, em muitos casos, os SOCs são excessivamente focados na tecnologia. Embora as características da tecnologia sejam importantes (e possam ser medidas e monitoradas), o ponto de partida deve ser o negócio (que deve ser medido e monitorado).

A interação com o negócio é fundamental: 22% dos pesquisados pela GISS informaram não haver interação entre o SOC e o negócio – e outros 36% não sabiam se isso ocorria. Como o SOC pode focar nos riscos certos (e em mudanças nos riscos) se o negócio não estiver regularmente conectado ao SOC?

*Leia a Pesquisa Global de Segurança da Informação da Ernst & Young, 2012 – Lutando para reduzir o gap (www.ey.com/giss2012)

55%

das organizações não incluem a segurança da informação nas avaliações de desempenho dos funcionários.

### 2. Criar uma equipe responsável pela segurança cibernética

Consolidar a abordagem e as atividades relacionadas à segurança cibernética em torno de uma equipe-base. Com isso, a organização estará apta a adaptar-se mais facilmente às novas ameaças. Essa equipe-base pode ser organizada de forma centralizada ou distribuída pelas funções/áreas, dependendo do tamanho e das necessidades da organização. A equipe responsável pode focar também em treinamento, capacitação e conscientização e tornar a segurança da informação parte do dia a dia de cada funcionário. Os membros da equipe devem agir como embaixadores, pondo em prática os seus ensinamentos.

### 3. Definir responsabilidades

Maior definição das responsabilidades e medição de desempenho são maneiras importantes de conseguir uma mudança de comportamento. Se os funcionários entenderem que a segurança do seu trabalho está ameaçada porque a segurança da empresa também está, e que a segurança cibernética é um indicador de desempenho, isso poderá levar a uma mudança permanente na conscientização e na postura. O comportamento requerido deve constar nos contratos dos funcionários – principalmente para aqueles com acesso a informações críticas – e deve ser incluído nas suas avaliações de desempenho. A violação dos protocolos de segurança da informação (mesmo sem consequências significativas) deve ser levada muito a sério.

Além de informar as ameaças cibernéticas aos funcionários, encontre formas de transformá-los nos "olhos e ouvidos" da organização e implemente um processo claro para escalar por meio do qual todos possam acompanhar caso algum funcionário note algo suspeito. Na nossa pesquisa, o apoio da computação forense e das mídias sociais possui a classificação mais baixa entre as prioridades da segurança da informação, porém essas técnicas e canais podem ser a forma inicial de detectar que a organização corre riscos de sofrer um ataque.

### 4. Vá além das fronteiras

Com um ciclo de transformações estabelecido, as organizações podem começar a buscar além das suas fronteiras e a avaliar o impacto causado por ataques cibernéticos aos seus parceiros de negócios, fornecedores e prestadores de serviços – uma comunidade que pode ser descrita como o seu "ecossistema" comercial (*leia na página 19*). A sua própria transformação efetiva revelará as principais práticas, que agora poderão ser divulgadas ao ecossistema para que fornecedores e prestadores de serviços possam ser obrigados contratualmente a agir em conformidade.

## Agir para melhorar e transformar

Caso sua organização esteja entre os níveis Ativar e Adaptar, há cinco medidas que você deve considerar urgentemente:

**1. Conceber e implantar um programa de transformação**
Dar suporte a uma melhoria no desenvolvimento da segurança cibernética além do nível básico em que os projetos de segurança são concretizados separadamente, em etapas. Consiga ajuda externa para desenvolver o programa e administrá-lo.

**2. Decidir o que deve ser feito pela própria empresa e o que deve ser terceirizado**
Por exemplo, definir se é melhor manter uma equipe central no seu próprio SOC para atender a todas as necessidades da empresa, terceirizar para um provedor de serviços gerenciados de segurança (MSSP), ou então optar por um modelo misto.

**3. Definir uma matriz RACI para a segurança cibernética**

**4. Definir o ecossistema da organização**
Considerar o impacto cumulativo das violações cibernéticas sobre terceiros e adotar medidas para eliminar ou reduzir potenciais gaps de segurança na sua interação com eles.

**5. Introduzir um treinamento de conscientização sobre segurança para os funcionários**
Fazer uma avaliação do amadurecimento, definir se a meta foi atingida e analisar o gap. Desenvolver e implantar um plano de treinamento para funcionários (inclusive os terceirizados).

# Olhando além das fronteiras: o ecossistema do negócio

Nossa pesquisa mostra que, na luta contra o crime cibernético, muitas empresas gastam a maior parte do seu tempo e recursos construindo barreiras internas – incluindo seus dados, sistemas e pessoas. Esse é um ponto de partida, mas esse perímetro não é mais estável e essa barreira deixou de ser eficaz.

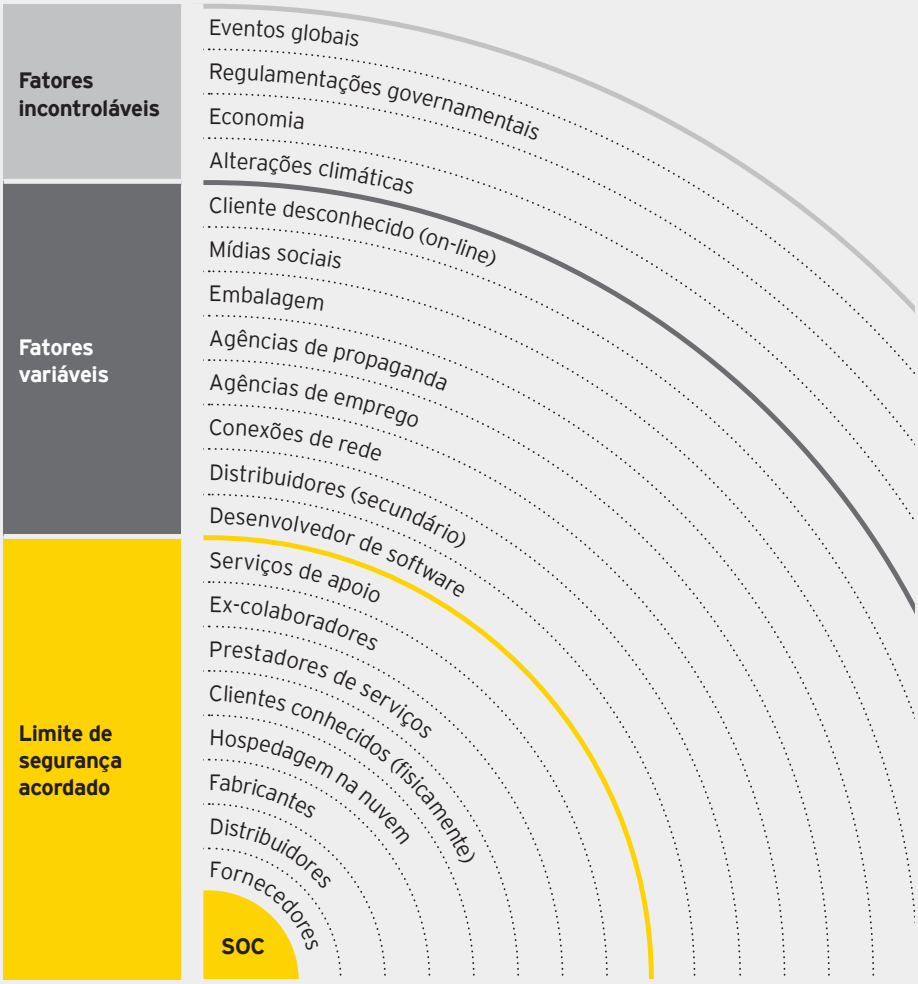
A maioria dos negócios atuais é conduzida além desse limite. Sendo assim, para que as organizações sejam capazes de se comunicar com seus parceiros de negócio, criam-se "brechas" na barreira. Consequentemente, o sistema de segurança cibernética deverá também incluir a rede mais ampla: clientes, fornecedores, parceiros de negócios e até ex-colaboradores – que, juntos, formam o chamado "ecossistema do negócio".

Para uma organização ser capaz de gerenciar efetivamente os riscos do seu ecossistema, ela precisa definir com clareza os limites desse ecossistema. E deve também decidir o que está disposta a gerenciar dentro desses limites. São apenas os riscos enfrentados pelos grupos que estão a um passo da organização (por exemplo, fornecedores) ou a organização deverá também influenciar a mitigação dos riscos enfrentados pelos grupos que estão a dois passos do centro (por exemplo, os fornecedores dos fornecedores)?

As organizações devem questionar:

- Qual é o nosso "limite de segurança"? Em outras palavras: com quantos parceiros deveremos trabalhar para aprimorar a segurança cibernética geral?
- Quanto podemos fazer para gerenciar o risco no ecossistema de negócios?
- Estamos preparados para aceitar certo nível de risco proveniente do ecossistema dos negócios?

O seu ecossistema de negócios



## Coloque-se em estado proativo

Há muita coisa que uma organização pode fazer para responder às ameaças que já surgiram. Mas uma organização que apenas reage às novas ameaças quando elas já se tornaram ativas pode descobrir que reagiu tarde demais.

A única maneira de manter-se à frente nesse ambiente complexo e dinâmico é encarar os desafios de cabeça erguida – considerar a segurança cibernética como um aspecto central do negócio e como um conhecimento essencial para sobreviver e prosperar. Tornar-se e permanecer bem-sucedido é uma jornada que nunca termina, e desenvolver e manter a capacitação em segurança cibernética faz parte dessa jornada.

A ambição deve avançar para um estágio de prontidão – para ser capaz de prever o que provavelmente acontecerá além de preparar-se, agir e reagir apropriadamente. Para fazer isso, é necessário acabar com a mentalidade de "vítima" e o modo de operar em perpétuo estado de incerteza (e ansiedade) sobre as ameaças cibernéticas desconhecidas, deixando a organização vulnerável a surpresas desagradáveis e prejudiciais.

Isso significa estabelecer uma conscientização e capacitação avançadas, desenvolvendo uma estratégia envolvente e instalando componentes de segurança cibernética em toda a empresa: significa promover a confiança na capacidade da organização de enfrentar esse tipo de ameaça.

# Antecipar


Para atingir o estágio da Antecipação, devem ser acrescentadas as seguintes características :

## 1. Segurança cibernética incorporando o futuro (built-beyond)

- **Permaneça alerta, pronto para agir e responder rapidamente de maneira equilibrada.** A liderança admite ameaças/riscos como um tema central do negócio, e a capacitação em segurança cibernética faz parte de um processo de decisão dinâmico. Isso possibilita a ação preventiva e auxilia os mecanismos de resposta a operarem rapidamente e sem problemas.
- **Conheça as suas "joias da coroa".** A organização não estará pronta para enfrentar ataques se não conhecer os ativos mais valiosos da empresa. Ela deve ser capaz de priorizar esses ativos e entender o impacto caso sejam violados, comprometidos ou anulados de alguma maneira e, em seguida, conectar tudo isso ao processo de avaliação de ameaças.

## 2. Foco no ambiente futuro

- **Conheça o seu ambiente, dentro e fora.** Um conhecimento abrangente – embora focado – da situação é fundamental para a compreensão do cenário mais amplo de ameaças e de como tal cenário está relacionado com a organização. Informações sobre ameaças cibernéticas podem trazer esse conhecimento – incorporando as fontes de risco internas e externas e abrangendo o presente e o futuro, mas sempre aprendendo com o passado.
- **Aprendizagem e evolução contínuas.** Nada é estático – nem os criminosos, nem a organização, nem qualquer parte do seu ambiente operacional – portanto, o ciclo de melhorias contínuas permanece. Tornar-se uma organização informada: estudar os dados (inclusive a computação forense); manter e desenvolver novos relacionamentos colaborativos; renovar regularmente a estratégia e aumentar a capacitação em segurança cibernética.

## 3. Abordagem proativa

- **Ter confiança nos seus mecanismos de resposta a incidentes e crises.** As organizações que atingiram o estágio de antecipação ensaiam regularmente sua capacidade de resposta a incidentes. Isso inclui "jogos de guerra" e outros exercícios, assim como simulações de incidentes complexos que realmente testam a capacidade da organização.

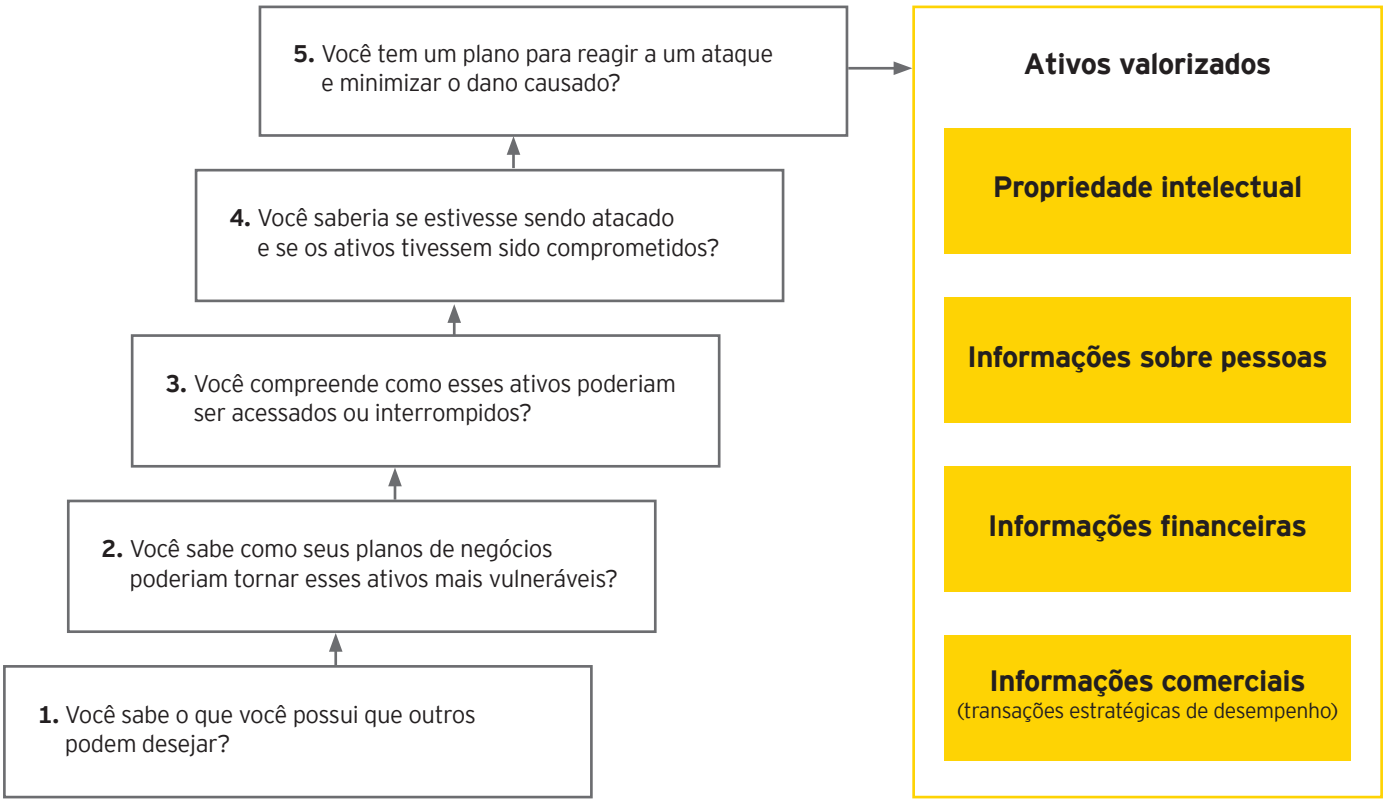
## Prepare-se para antecipar

Uma organização em estado de prontidão tem uma mentalidade totalmente diferente, enxerga o mundo de outra forma e reage de um modo que os criminosos cibernéticos não esperam. Para tanto, é necessário um comportamento cuidadoso, ponderado e colaborativo. Ela aprende, prepara e ensaia. Nenhuma organização ou governo conseguem prever todos os ataques, nem mesmo a maioria; mas é possível reduzir a sua atratividade como alvo, aumentar a resiliência e limitar os danos causados por um determinado ataque.

Aprender a manter-se à frente é desafiador e leva tempo, mas os benefícios para a organização são consideráveis. A organização será capaz de explorar as oportunidades oferecidas pelo mundo digital enquanto minimiza a sua exposição aos riscos e os custos de enfrentá-los.

Para começar, a organização e sua liderança devem conhecer as respostas a todas essas perguntas, e sentir confiança nelas. Se uma das respostas for "não", é aí que ela deverá se concentrar e onde existe a necessidade de mudanças.

Sofrer um ataque é inevitável – você está preparado? Você consegue dizer "sim" a estas cinco perguntas fundamentais?




As seções seguintes descrevem o que uma organização pode fazer para manter-se à frente, tornar-se apta a responder "sim" aos itens acima e ir além.

## Compreender o seu ambiente de ameaças e estabelecer uma detecção precoce

Não basta apenas saber que existem ameaças. A organização precisa compreender a natureza delas, como (e onde) se manifestarão e avaliar o impacto que podem causar. O alerta e a detecção precoce das violações são fundamentais para o estado de prontidão. Entretanto, a maioria das organizações consegue detectar apenas ataques relativamente simples. Isso significa que elas talvez não saibam que já foram violadas por ataques mais sofisticados e, além disso, não serão capazes de detectar ataques futuros dessa natureza.

Incorporar ou estabelecer uma inteligência capacitada em ameaças cibernéticas pode ajudar a colocar a organização à frente do problema. No nível tático, essa capacitação se concentrará no SOC, mas o alcance da função se estenderá à camada estratégica e à alta administração (C-level), se for bem-feito.

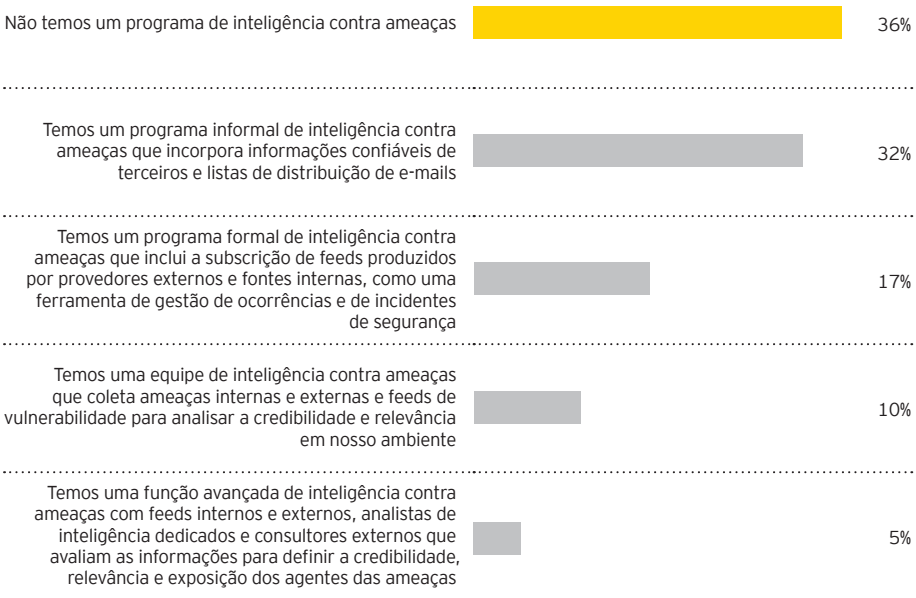
- O que está acontecendo lá fora que a organização pode aprender?
- Como a organização pode se proteger contra ameaças? Isso é necessário?
- Como as outras organizações enfrentam ameaças e ataques específicos?
- Como a organização pode ajudar outras a enfrentar essas ameaças e ataques?
- A organização compreende a diferença entre um ataque dirigido e um ataque "aleatório"?
- Quais agentes de ameaças são relevantes?

Todas as questões acima podem ser respondidas pelo sistema de inteligência sobre ameaças cibernéticas, mas a nossa pesquisa mostra que poucas organizações entendem claramente o que é esse sistema e o que ele pode oferecer:

56%

das organizações informam que é improvável ou pouco provável que sejam capazes de detectar um ataque sofisticado.

**Qual afirmação abaixo melhor descreve a maturidade do seu programa de inteligência contra ameaças?**



36%

dos respondentes não contam com um programa de inteligência contra ameaças.

Inteligência é muito mais do que a simples coleta de informações. O ciclo de inteligência compreende a seguinte sequência de atividades:

### 1. Determinar os requisitos de inteligência

Do que as organizações devem ter consciência? Existem lacunas no seu conhecimento?

### 2. Reunir informações

Vários feeds de código aberto estão disponíveis para informações externas, e também muitos feeds com dados originados dos sistemas internos.

### 3. Analisar e avaliar as informações reunidas para elaborar um relatório de inteligência

Isso pode ser obtido externamente ou conduzido internamente. O entendimento da atividade principal da empresa é crucial para que a avaliação seja significativa.

### 4. Distribuir e divulgar o relatório

### 5. Adotar as medidas apropriadas

Para que a inteligência contra ameaças cibernéticas se torne efetiva, esse ciclo precisará ser cumprido rapidamente. Algumas atividades podem ser automatizadas e, para isso, existem técnicas, ferramentas e serviços disponíveis. Outros elementos não podem ser automatizados e necessitam de envolvimento e intervenção humana. Existe uma grande variedade de serviços de inteligência contra ameaças cibernéticas disponíveis, que precisam ser avaliados especificamente para verificar se atendem aos requisitos, características e maturidade da organização. Entretanto, o defeito de muitos desses serviços é inundar a organização com informações não relevantes ou aplicáveis, que muitas vezes são ignoradas.

A inteligência contra ameaças cibernéticas pode também provar ser muito útil ao criar mais valor na gestão de risco indicando as falhas na rede atual e no seu ecossistema, o que poderia resultar em mudanças nos processos para tornar toda a organização mais ágil. Decisões seriam tomadas mais depressa, os dados seriam protegidos e as brechas seriam descobertas, priorizadas e mitigadas. Um programa sólido de inteligência contra ameaças pode também ser alavancado por um bom programa de análise de indicadores e dados, frequentemente conectado ao programa de Big Data da empresa.

23%

dos pesquisados afirmam que a sua estratégia de segurança da informação esboça o estado futuro da segurança da informação três a cinco anos à frente.

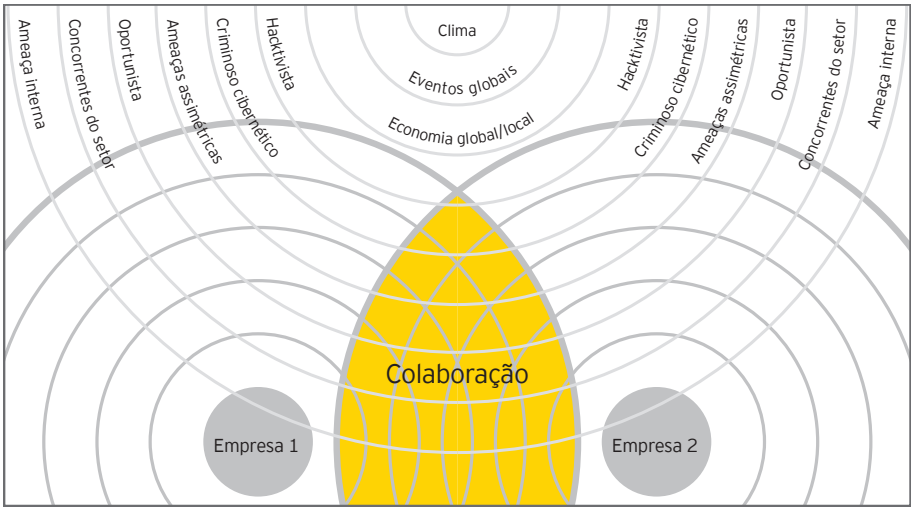
## Pense no passado, presente e futuro

A ambição da organização precisa abranger esforços para olhar em direção ao futuro, aprender com o passado e preparar-se para o agora. As empresas precisam se manter informadas sobre as novas tendências e os diferentes tipos e métodos de ataque, bem como as ferramentas e técnicas para enfrentá-los. É vital manter-se informado sobre as tecnologias emergentes e continuar a explorar as oportunidades da organização de explorá-las, mantendo sempre um olhar firme nos novos riscos e fragilidades que podem introduzir. Nossa pesquisa de 2014, entretanto, mostra que a maioria das organizações ainda está preocupada com a situação atual e não está olhando para o futuro.

**Em comparação com o ano anterior, a sua organização planeja gastar mais, menos ou relativamente o mesmo valor ao longo do próximo ano com as seguintes atividades?**

## Envolva-se e colabore

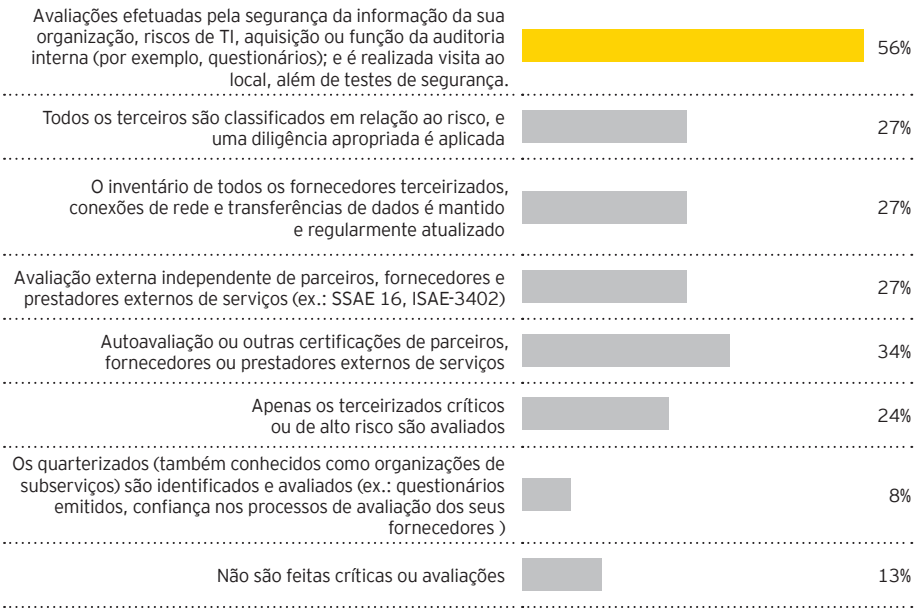
A colaboração é necessária no nível de Antecipação. Todas as organizações (e também as pessoas) enfrentam esses desafios e, quando a capacitação amadurece, aprendem que a colaboração traz frutos, especialmente se conduzida de forma objetiva. O compartilhamento de informações pelo ecossistema de negócios num grupo mais amplo (seja um ambiente ad hoc, semiformal ou moderadamente formal) é o ingrediente secreto para as organizações mais bem-sucedidas na compreensão, planejamento e mitigação de intrusões nas suas redes.




Esse importante componente colaborativo também é verdadeiro no caso da inteligência contra ameaças cibernéticas. O compartilhamento de plataformas entre informações e inteligência existe de várias formas: específico de cada setor ou entre setores, entidades governamentais, ligadas ao CERT nacional, ou entidades autônomas com envolvimento de governo etc. Os governos e as grandes organizações assumiram um papel de liderança no estabelecimento das estruturas políticas e práticas que dão suporte ao desenvolvimento de ecossistemas cibernéticos resilientes. Por exemplo, o US-CERT como o Cyber Resilience Review (CRR) e a iniciativa de Parceria do Fórum Econômico Mundial para a Resiliência Cibernética (PCR, em inglês). Esses fóruns fornecerão informações críticas para divulgação imediata entre as organizações e também proporcionarão acesso a insights estratégicos sobre agentes das ameaças e cenários futuros, técnicas de mitigação, contexto do setor e ações governamentais.

A colaboração também proporciona às organizações uma maior conscientização sobre os seus parceiros e a sua cadeia de fornecimento, e a capacidade de influenciar e aprender com todo o ecossistema. As maiores organizações precisam compreender que a sua capacitação muitas vezes é mais madura do que a de alguns dos seus fornecedores, por isso o conhecimento compartilhado sobre a segurança cibernética – ou a coordenação das atividades de segurança cibernética com os fornecedores – pode ser muito mais efetivo do que uma caminhada solitária. Uma solução compartilhada fortalece as camadas de proteção dentro e ao redor do seu ecossistema. Entretanto, isso pode requerer que a organização desenvolva um "modelo de confiança" baseado em autenticação, acordos de segurança etc. Os exercícios de resposta a incidentes devem incluir terceiros e outros players no seu ecossistema mais amplo.

**Como você assegura que os seus parceiros externos, fornecedores ou prestadores de serviço terceirizados estão protegendo as informações da sua organização?**




## Economia cibernética

As organizações utilizam as quatro perguntas abaixo para avaliar o impacto de um ataque cibernético em termos reais, como forma de entender o impacto nos seus resultados financeiros, na marca e na reputação.

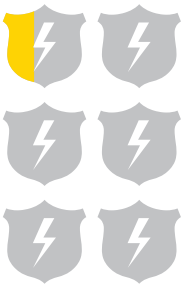
- Como os valores das ações seriam afetados?
- Os clientes seriam prejudicados?
- Isso provocaria uma redução nas receitas?
- Quais seriam os custos de reparar os danos em todos os sistemas internos e/ou substituir o hardware porque a organização não estava preparada para um ataque?

Técnicas de economia cibernética estão sendo desenvolvidas para ajudar as organizações a converter esses aspectos em cifras tangíveis.

## Conduzir exercícios de incidentes cibernéticos

A organização está confiante de que todos saberão o que fazer caso ocorra um ataque? Em caso negativo, os danos causados pelo ataque serão maiores do que o esperado.

A condução inadequada de incidentes cibernéticos já causou impactos severos em muitas empresas. Uma vez constatada a violação, ter conhecimento profundo de seus ativos críticos e ramificações associadas permitirá que a organização ponha em prática os mecanismos de resposta adequados. Os stakeholders, clientes, funcionários, recursos humanos, agentes reguladores – todos esses grupos desempenham um papel que resultará em quão bem a sua organização resiste a um ataque.



6%

das organizações afirmam ter um programa robusto de resposta a incidentes, que inclui terceiros e aplicação da lei e que é integrado com uma abrangente função de gerenciamento de ameaças e vulnerabilidades.

58%

das organizações não têm uma área ou departamento focado em novas tecnologias e em seu impacto na segurança da informação.

Estar em prontidão requer que a organização já tenha ensaiado vários cenários de ataque. Pelo menos uma vez ao ano, a organização deve ensaiar seus mecanismos de resposta à crise, por meio de cenários complexos de ataque cibernético. Diferentes serviços estão disponíveis para ajudar a organização, de forma segura e realista, a executar esses exercícios. Isso será difícil, mas as lições aprendidas se mostrarão de grande valor. Em algumas áreas, as agências reguladoras estão agora exigindo que os cenários cibernéticos sejam conduzidos e seus resultados relatados.

As equipes de atendimento ao cliente da Ernst & Young vêm trabalhando com a alta administração de várias das principais empresas que estão empreendendo simulações de segurança cibernética e "jogos de guerra" para encorajar o nível dos altos executivos (C-level) a considerar de uma forma mais ampla e séria os aspectos de ameaças e oportunidades, e os auxiliando a caminhar na direção certa para "Antecipar".

## Aja e assuma a dianteira

Se a sua organização estiver pronta para atingir o nível "Antecipar", sugerimos a seguir cinco ações que você deveria tomar:

**1. Planejar e implantar uma estratégia de inteligência contra ameaça cibernética**
A função de Segurança da Informação deve atuar com o apoio da administração para ajudá-la a compreender como poderia usar a inteligência contra ameaças a fim de subsidiar as decisões da empresa e alavancar o valor da segurança cibernética.

**2. Definir e envolver o ecossistema ampliado da organização**
Trabalhar em parceria com outros membros do ecossistema ampliado para definir a matriz RACI e modelos confiáveis, implementar a cooperação e compartilhar os recursos onde for vantajoso.

**3. Adotar uma abordagem econômica dos temas cibernéticos**
Entender quais são os ativos cibernéticos vitais e seus respectivos valores para os criminosos cibernéticos; então, reavaliar os planos para investir na sua segurança.

**4. Usar análise de dados da computação forense e inteligência contra ameaças**
Valer-se das mais recentes ferramentas técnicas para analisar onde e quando podem surgir as ameaças mais prováveis, aumentando o seu poder de combatê-las.

**5. Assegurar que todos compreendam o que está ocorrendo**
Governança forte, controle dos usuários e comunicações regulares atualizarão os funcionários e os manterão atuando como os "olhos e ouvidos" de toda a organização.


# Uma organização, três histórias

Relatamos abaixo uma história familiar, contada de três maneiras diferentes. Ainda que seja um exemplo fictício, as reações, os impactos e os acontecimentos são baseados no tempo de experiência que tivemos com nossos clientes e nos eventos que foram descobertos ao longo deste período. Empresas em diferentes fases de Ativar, Adaptar ou Antecipar irão identificar, reagir, responder e se recuperar desses incidentes de maneiras muito diferentes. Iremos avaliar os impactos que cada empresa sofreu:

**1. Financeiramente | 2. Operacionalmente | 3. Pessoalmente**

Nosso estudo de caso envolve três versões (Ativar, Adaptar e Antecipar) de uma grande empresa operadora de telecomunicações (com um faturamento maior que US$ 12 bilhões) com operações de varejo significativas (mais de 400 centros de atendimento) e interação direta com seus clientes, tanto pessoalmente como on-line. Essa empresa sofrerá uma violação dos dados dos seus clientes e examinaremos as diferentes reações a eventos similares.

## Ativar

**O cenário:** essa empresa sofreu uma violação importante dos dados dos clientes. O anúncio público foi feito pela primeira vez por uma fonte externa e, depois, pela empresa. A empresa respondeu muito rapidamente, confirmando a ocorrência da violação e informando ao público que o problema foi identificado e resolvido com um impacto mínimo.

Entretanto, uma semana depois, a mesma fonte externa afirmou que os danos eram significativos e os dados detalhados de milhões cartões de crédito haviam sido roubados. A empresa reconheceu que isso era verdadeiro. A fonte fez mais descobertas e o vaivém continuou na mídia ao longo de várias semanas, até que foi descoberto que o número dos cartões que tiveram seus dados roubados era dez vezes maior que o originalmente mencionado – e que as evidências indicavam que a violação ainda estava ativa e não havia sido resolvida.

**Financeiramente:** a história foi divulgada pela mídia ao longo de mais de dois meses, exatamente antes do período mais movimentado do ano. Além da perda de muitos clientes, o custo percentual final foi acima de dois dígitos, tanto no preço das ações como nas receitas. Após um ano, a empresa ainda não tinha visto a volta dos números do período anterior à violação. No fim das contas, o custo total da violação ultrapassou 5% do faturamento anual.

**Operacionalmente:** a empresa gastou muitos meses de esforço concentrando-se nesse problema e, em vez de resolvê-lo, seus esforços foram no sentido de responder e gerenciar a crise na mídia. A empresa teve de identificar e fornecer serviços de monitoramento de crédito, trabalhar com os bancos e clientes para dissipar suas preocupações e poder finalmente tentar restabelecer a confiança dos clientes.

**Pessoalmente:** essa situação conduziu à exoneração de muitos executivos e líderes da organização, inclusive o CEO e o CIO.

## Adaptar

**O cenário:** essa empresa sofreu uma violação significativa dos dados de seus clientes. O anúncio público foi inicialmente veiculado por uma fonte externa e posteriormente confirmado pela empresa, que não comentou o assunto durante quase uma semana. Ela ofereceu uma resposta muito comedida, confirmando a violação e informando ter conhecimento sobre onde a violação teria ocorrido. Afirmou também estar confiante em ter remediado o problema e que permanecia aguardando o término de uma investigação para confirmar a extensão do problema. Duas semanas mais tarde, a empresa confirmou a perda total e informou ter identificado a fonte da violação. Disse ainda que havia adotado os controles de mitigação necessários e que estava trabalhando na solução permanente do problema.

Desde então, não houve mais relatórios contraditórios.

**Financeiramente:** esse incidente gerou três novas histórias, mas entrou e saiu da mídia rapidamente. Embora a violação tivesse sido significativa, a empresa não sofreu uma grande perda de clientes. Ela proporcionou monitoramento de crédito e ofertas especiais para trazer de volta os clientes, com algum custo. Em três meses, a receita, os preços das ações e as operações retornaram aos níveis anteriores à violação.

**Operacionalmente:** essa história saiu do foco da mídia em um mês. A empresa investiu mais tempo na solução do problema do que em responder à pressão da mídia, tendo trabalhado também com os bancos, marcas e clientes. Seus esforços se concentraram em serviços agregados e no apoio aos negócios.

**Pessoalmente:** ao longo desse período desafiador, a empresa demonstrou uma liderança sólida na crise e manteve a confiança de seus clientes, acionistas e da diretoria.

## Antecipar

**O cenário:** essa empresa sofreu uma violação importante dos dados de seus clientes. Nos meses que antecederam o ataque, a empresa havia trabalhado com organizações semelhantes, equipes internas de inteligência e de aplicação da lei, para coletar informações relevantes das atividades de agressores potenciais, e também procurou identificar os riscos aos quais estava sujeita. Também se informou sobre outras violações em seu setor. Como resultado, foram capazes de desenvolver controles de segregação e proteção e criar cenários para exercícios de ataque e resposta. Em última análise, não foram capazes de conter o ataque, mas evitaram a perda de detalhes de pagamentos e informações pessoais sensíveis, que já haviam sido armazenadas separadamente e protegidas por controles diferentes.

Devido ao monitoramento adicional, a violação foi descoberta em primeiro lugar no âmbito interno da empresa. Logo após o incidente, a empresa emitiu um comunicado público sobre o que havia ocorrido e como isso havia sido resolvido.

**Financeiramente:** apesar de o custo da recuperação da violação ter sido significativo, o impacto no preço das ações, a perda da base de clientes e a exposição na mídia foram mínimos ou quase nulos. O custo ficou confinado às atividades de investigação e mitigação. A empresa foi capaz de controlar a atenção da mídia com suficiente confiança, e não foi necessário oferecer o serviço de monitoramento de crédito, que é normalmente a resposta usual para a violação de dados dos clientes. Apenas esse aspecto economizou pelo menos US$ 350 milhões de custo potencial de resposta e, possivelmente, fortaleceu a confiança dos clientes e dos órgãos regulatórios.

**Operacionalmente:** não houve praticamente nenhuma cobertura da mídia além do comunicado emitido pela própria empresa, e dessa forma ela pôde concentrar seus esforços em retomar os negócios como de costume. O custo da investigação e da mitigação tornou-se um custo operacional. Assim, a investigação da violação não causou impacto negativo nos processos BAU (do inglês, "Business As Usual"), nem enfraqueceu suas defesas – um erro frequente que cria um efeito que pode causar novas violações posteriores.

**Pessoalmente:** não houve demissões nem renúncias. A confiança nos executivos foi renovada.

# Resumo

## Onde as organizações se situam agora

Os riscos cibernéticos estão aumentando e mudando rapidamente. A cada dia, os criminosos estão desenvolvendo novas técnicas para se infiltrar na segurança das organizações, inclusive da sua. Agem dessa forma para causar danos, ter acesso a informações sensíveis e roubar propriedade intelectual. A cada dia, seus ataques se tornam mais sofisticados e mais difíceis de serem derrotados.

Devido a esse contínuo desenvolvimento, não podemos dizer exatamente quais tipos de ameaças surgirão daqui a um, cinco ou dez anos. Podemos afirmar, apenas, que essas ameaças se tornarão cada vez mais perigosas do que já são atualmente. Podemos também estar certos de que as antigas fontes de ameaças cibernéticas se enfraquecerão e novas fontes surgirão para substituí-las.

Apesar dessa incerteza – e de fato, devido a ela –, você precisa avaliar com clareza qual o tipo de segurança cibernética de que necessita.

## O que as organizações necessitam fazer

Para compreender bem a segurança cibernética, o primeiro passo é compreender os fundamentos corretamente. Devido à atenção que os recentes ataques têm recebido, ninguém pode afirmar que desconhece os perigos, portanto, não há desculpa para as organizações que ainda não implantaram sistemas básicos de segurança cibernética.

Uma vez dominados os fundamentos, o estágio seguinte será tornar a sua segurança cibernética mais dinâmica e mais bem alinhada e integrada com os principais processos da empresa. Sem dar esse passo crucial, as organizações permanecerão vulneráveis – particularmente quando as próprias empresas, seu ambiente e as ameaças cibernéticas que elas enfrentam estão mudando.

E então surge a oportunidade real: colocar-se à frente do crime cibernético. Ao focar a sua segurança cibernética em algo desconhecido – o futuro e o seu amplo ecossistema dos negócios –, você poderá começar a desenvolver a capacitação da sua empresa antes que ela se torne necessária e se preparar desde já para as ameaças que surgirão.

| O que é | Os elementos da implementação da segurança cibernética | Status |
|---|---|---|
| **Antecipar** é olhar para o desconhecido. Baseado na inteligência contra as ameaças cibernéticas, hackers potenciais são identificados. São tomadas medidas antes que algum dano seja causado. | **Antecipar** | **Antecipar** é um nível emergente. Cada vez mais organizações estão usando a inteligência contra as ameaças para tomar a dianteira em relação ao crime cibernético. É um acréscimo em relação ao estágio abaixo. |
| **Adaptar** tem a ver com mudança. O sistema de segurança cibernética muda quando o ambiente também se altera. O foco é proteger a empresa do futuro. | **Adaptar** | **Adaptar** ainda não foi amplamente adotado. Não é uma prática comum avaliar as implicações da segurança cibernética todas as vezes que a organização faz mudanças no negócio. |
| **Ativar** é preparar o cenário. Envolve um complexo conjunto de medidas de segurança cibernética focado na proteção da empresa como ela está hoje. | **Ativar** | **Ativar** é parte do sistema de segurança cibernética de todas as organizações. Nem todas as medidas necessárias já foram tomadas; ainda há muito a fazer. |

## Onde gostaríamos que as organizações chegassem

As organizações precisam olhar à frente e enxergar além dos negócios – novos desafios estão sendo criados hoje, e é preciso assumir a liderança do jogo. Gostaríamos que uma inteligência proativa contra ameaças de segurança cibernética se tornasse norma para todas as organizações, embora a pesquisa deste ano não sugira que elas chegarão a esse nível no futuro próximo.

Não desejamos que o foco permaneça restrito aos ataques destruidores de empresas ou desastres de relações públicas: queremos que o foco seja centrado no aperfeiçoamento das organizações, para que dominem os fundamentos da segurança cibernética, pratiquem abordagens inovadoras e utilizem novas ferramentas poderosas que as tornem mais fortes e seguras do que nunca. Queremos que as empresas tomem a iniciativa e tornem os crimes cibernéticos menos lucrativos, gastando bem menos tempo e recursos do que ocorre atualmente. Em outras palavras, tirar o poder dos hackers e tomar a dianteira em relação aos crimes cibernéticos.

# Sinopse

## Como a Ernst & Young pode ajudar

Na Ernst & Young, temos uma perspectiva integrada de todos os aspectos do risco organizacional, e a segurança cibernética é uma importante área de foco em que a Ernst & Young é líder reconhecida, inclusive no atual cenário de tecnologia móvel, mídias sociais e computação em nuvem.

Nossos profissionais enfrentam o desafio de administrar as informações e os riscos de segurança cibernética nas operações comerciais. Contamos com o conhecimento profundo em gestão de riscos relacionados a TI da nossa organização global e somos líderes no setor. Prestamos serviços de controle de TI focados na concepção, implementação e racionalização de controles que reduzem potencialmente os riscos nas aplicações, infraestrutura e dados dos nossos clientes.

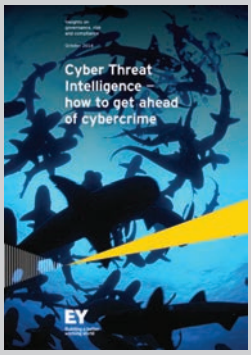
A segurança cibernética é regularmente discutida nas reuniões de diretoria. Conhecemos o impacto nos negócios e os detalhes técnicos, como também sabemos como apresentá-los à camada estratégica e à alta administração (C-level), resultando em maiores insights dos riscos e em conversas mais detalhadas entre os executivos. Nosso objetivo é sermos consultores de confiança para os nossos clientes, enquanto eles enfrentam o desafio de proteger e assegurar seus ativos, como, por exemplo, ajudamos os nossos clientes a:

- Alinhar as suas estratégias relacionadas à segurança da informação às necessidades comerciais;
- Investigar as violações cibernéticas complexas, além de auxiliar na detecção e resposta às abordagens;
- Otimizar os gastos relacionados à segurança da informação e tornar a sua Gestão do Programa Cibernético mais sustentável e proveitosa;
- Aprimorar a capacitação do SOC – Centro de Operações de Segurança;
- Ajudar a monitorar, manter e auxiliar o cumprimento da conformidade com as políticas de gestão de acesso, bem como lidar com questões legais e regulatórias;
- Avaliar a adequação dos recursos e habilidades para a implementação de tecnologias e processos.

Nossos serviços de segurança cibernética incluem importantes aspectos das fases **Ativar, Adaptar** e **Antecipar,** mencionadas neste relatório, para ajudá-lo a permanecer à frente dos ataques criminosos.

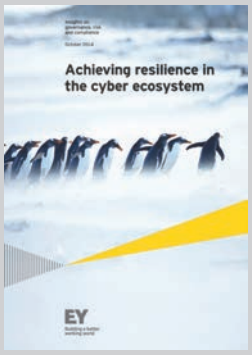
## Você deseja aprender mais?

**Insights sobre governança, risco e compliance** é uma série contínua de estudos focados em TI e outros riscos comerciais, e nas diversas oportunidades e desafios relacionados. Estas publicações oportunas e dinâmicas são concebidas para ajudá-lo a entender os problemas e fornecer insights valiosos sobre a nossa perspectiva. Para saber mais, acesse a nossa série Insights sobre governança, risco e compliance, em www.ey.com/GRCinsights.




*Inteligência Relacionada a Ameaças Cibernéticas – Como manter-se à frente dos crimes cibernéticos*

www.ey.com/CTI




*Conquistando a resiliência no ecossistema cibernético*

www.ey.com/cyberecosystem


*Gestão de Programas Cibernéticos: identificando formas de permanecer à frente dos crimes cibernéticos*

www.ey.com/CPM


*Centros de Operações de Segurança – Ajudando você a manter-se à frente dos crimes cibernéticos*

www.ey.com/SOC


*Tendências de privacidade para 2014: proteção da privacidade na era da tecnologia*

www.ey.com/privacy2014


*Maximizando o valor do programa de proteção de dados*

www.ey.com/dataprotect


*Aumentando a confiança na nuvem*

www.ey.com/cloudtrust


*Identificação e administração de acessos: além do compliance*

www.ey.com/IAM


*Big data: mudando a forma de operar das empresas*

www.ey.com/bigdatachange

# Metodologia da pesquisa

A Pesquisa Global de Segurança da Informação da Ernst & Young foi realizada entre junho e agosto de 2014. Participaram mais de 1.800 respondentes, de todos os principais setores, em 60 países.

Para participar da nossa pesquisa, convidamos CIOs, CISOs, CFOs, CEOs e outros executivos da área de segurança da informação. Distribuímos um questionário a profissionais selecionados da Ernst & Young em cada país, juntamente com instruções para a administração consistente do processo de pesquisa.

A maioria das respostas da pesquisa foi coletada em entrevistas personalizadas. Quando não foi possível, o questionário foi respondido on-line.

Caso você deseje participar de futuras Pesquisas Globais de Segurança da Informação da Ernst & Young, entre em contato com o seu representante da Ernst & Young ou com o escritório local, ou acesse www.ey.com/giss e preencha um formulário de solicitação.

**Respondentes por área (1.825 respondentes)**

| | |
|---|---|
| EMEIA | 39% |
| Américas | 26% |
| Ásia-Pacífico | 22% |
| Japão | 13% |

**Respondentes por receita anual total da empresa**

| | |
|---|---|
| US$ 10 bilhões – US$ 50 bilhões | 167 |
| US$ 1 bilhão – US$ 10 bilhões | 441 |
| US$ 100 milhões – US$ 1 bilhão | 479 |
| US$ 10 milhões – US$ 100 milhões | 314 |
| Menos de US$ 10 milhões | 209 |
| Governo, sem fins lucrativos | 119 |
| Não se aplica | 215 |

## Respondentes por setor

| | |
|---|---|
| Aeroespacial e defesa | 63 |
| Gestão de ativos | 60 |
| Automotiva | 62 |
| Bancos e mercados de capitais | 308 |
| Tecnologia limpa | 2 |
| Bens de consumo | 132 |
| Produtos industriais diversos e químicos | 146 |
| Setor público e governo | 119 |
| Assistência médica e provedoras | 70 |
| Seguros | 138 |
| Ciências da vida | 40 |
| Mídia e entretenimento | 44 |
| Mineração e metais | 43 |
| Petróleo e gás | 55 |
| Energia e concessionárias | 68 |
| Private equity | 1 |
| Firmas e serviços profissionais | 68 |
| Real Estate | 56 |
| Atacado e varejo | 100 |
| Tecnologia | 117 |
| Telecomunicações | 62 |
| Transportes | 71 |

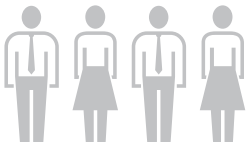
## Respondentes por número de funcionários

| | |
|---|---|
| Menos de 1.000 | 664 |
| De 1.000 a 5.000 | 557 |
| De 5.000 a 15.000 | 283 |
| De 15.000 a 50.000 | 194 |
| Acima de 50.000 | 127 |

## Respondentes por cargos/posições

| | |
|---|---|
| Chief Information Officer | 208 |
| Chief Information Security Officer | 283 |
| Chief Security Officer | 54 |
| Chief Technology Officer | 41 |
| Information Security Executive | 233 |
| Information Technology Executive | 346 |
| Auditoria interna Diretor/gerente | 72 |
| Administrador de redes e sistemas | 38 |
| Outros C-level, executivos, vice-presidentes | 60 |
| Outros | 490 |

## Perfil dos participantes



1.825
respondentes

60
países

25
setores

## Contate-nos

Possuímos uma perspectiva integrada de todos os aspectos do risco organizacional. Somos líderes de mercado em auditorias internas, riscos financeiros e controladoria, e continuamos expandindo as nossas habilidades em outras áreas de risco, inclusive governança, risco e compliance, bem como gestão de riscos empresariais.

Inovamos em áreas como consultoria de riscos, análise de riscos e tecnologias de risco para permanecermos à frente dos nossos concorrentes. Contamos com um conhecimento profundo da gestão de riscos técnicos e relacionados ao ambiente de TI e somos líderes no setor. Prestamos serviços de controle de TI focados na concepção, implementação e racionalização dos controles que reduzem potencialmente os riscos nas aplicações, infraestrutura e dados dos nossos clientes. Segurança da informação é uma importante área de foco em que a Ernst & Young é líder reconhecida no atual panorama de tecnologia de dispositivos móveis, mídias sociais e computação em nuvem.

Nossos líderes na área de Riscos são:

| **Líder global de Riscos** | | |
|---|---|---|
| **Paul van Kessel** | +31 88 40 71271 | paul.van.kessel@nl.ey.com |
| **Líderes de Riscos por área** | | |
| Américas | | |
| **Amy Brachio** | +1 612 371 8537 | amy.brachio@ey.com |
| EMEIA | | |
| **Jonathan Blackmore** | +971 4 312 9921 | jonathan.blackmore@ae.ey.com |
| Ásia-Pacífico | | |
| **Iain Burnet** | +61 8 9429 2486 | iain.burnet@au.ey.com |
| Japão | | |
| **Yoshihiro Azuma** | +81 3 3503 1100 | azuma-yshhr@shinnihon.or.jp |

Nossos líderes em Segurança da Informação são:

| **Líder global de Segurança da Informação** | | |
|---|---|---|
| **Ken Allan** | +44 20 795 15769 | kallan@uk.ey.com |
| **Líderes das áreas de Segurança da Informação** | | |
| Américas | | |
| **Bob Sydow** | +1 513 612 1591 | bob.sydow@ey.com |
| EMEIA | | |
| **Ken Allan** | +44 20 795 15769 | kallan@uk.ey.com |
| Ásia-Pacífico | | |
| **Paul O'Rourke** | +65 6309 8890 | paul.o'rourke@sg.ey.com |
| Japão | | |
| **Shinichiro Nagao** | +81 3 3503 1100 | nagao-shnchr@shinnihon.or.jp |

Nossos contatos de Segurança da Informação no Brasil são:

| **Sócio de Segurança da Informação** | | |
|---|---|---|
| **Sergio Kogan** | +55 11 2573 3395 | sergio.kogan@br.ey.com |
| **Diretor de Segurança da Informação** | | |
| **Demetrio Carrión** | + 55 21 3263 7038 | demetrio.carrion@br.ey.com |

**EY**

Auditoria | Impostos | Transações Corporativas | Consultoria

## Sobre a Ernst & Young

A Ernst & Young é líder global em serviços de Auditoria, Impostos, Transações Corporativas e Consultoria. Nossos insights e os serviços de qualidade que prestamos ajudam a criar confiança nos mercados de capitais e nas economias ao redor do mundo. Desenvolvemos líderes excepcionais que trabalham em equipe para cumprir nossos compromissos perante todas as partes interessadas. Com isso, desempenhamos papel fundamental na construção de um mundo de negócios melhor para nossas pessoas, nossos clientes e nossas comunidades.

No Brasil, a Ernst & Young é a mais completa empresa de Auditoria, Impostos, Transações Corporativas e Consultoria, com 5.000 profissionais que dão suporte e atendimento a mais de 3.400 clientes de pequeno, médio e grande portes.

A Ernst & Young Brasil é Apoiadora Oficial dos Jogos Olímpicos e Paralímpicos Rio 2016 e fornecedora exclusiva de serviços de Consultoria para o Comitê Organizador. O alinhamento dos valores do Movimento Olímpico e da EY foi decisivo nessa iniciativa.

Ernst & Young refere-se à organização global e pode referir-se também a uma ou mais firmas-membro da Ernst & Young Global Limited (EYG), cada uma das quais é uma entidade legal independente. A Ernst & Young Global Limited, companhia privada constituída no Reino Unido e limitada por garantia, não presta serviços a clientes.



**ey.com.br**

facebook | **EYBrasil**
twitter | **EY_Brasil**
linkedin | **ernstandyoung**
app | **ey.com.br/eyinsights**

APOIADOR OFICIAL

Baixe o app **EY Insights** gratuitamente na Apple Store ou no Google Play e conheça nossos estudos e publicações.