A cibersegurança como um componente essencial da governança corporativa

ECOTRUST

Um chamado à ação para os conselhos de administração

Desde que a Lei Geral de Proteção de Dados (LGPD) entrou em vigor, gestores que atuam nos mais diversos segmentos têm promovido inovações em sua forma de trabalhar quando o assunto é a **cibersegurança**.

Já está muito claro que este é um tema que não pode se restringir aos setores de tecnologia da informação dentro das empresas. E é por isso que os principais frameworks de segurança da informação têm apontado a importância do envolvimento dos conselhos de administração nas ações que visam à **defesa dos negócios contra os ciberataques**.

Na verdade, a segurança da informação é um assunto relevante para a sociedade como um todo e pode envolver a atuação de diversas categorias profissionais que, de modo algum, devem estar limitadas ao setor de TI.

De acordo com o Instituto Brasileiro de Governança Corporativa (IBGC), na Europa, já é possível encontrar escritórios de advocacia que atuam junto aos conselhos administrativos das empresas para solucionar questões concernentes à proteção de dados. No Brasil, ainda que timidamente, isso também vem acontecendo.

Ao tomar as leis ligadas ao tema, como a LGPD brasileira, como uma oportunidade de **promoção da otimização do tratamento de dados e da transparência**, é possível colocar a governança corporativa em prática, melhorando também a reputação do negócio.

Porém, este avanço só é possível quando o setor de TI torna-se um aliado de outros setores, incluindo, além do operacional, os departamentos de marketing, vendas, jurídico e financeiro, só para citar alguns exemplos.

Ou seja, a obtenção de bons resultados quanto à cibersegurança depende do estabelecimento de um **diálogo multilateral** dentro da empresa e, para isso, é preciso **começar pelo envolvimento dos conselhos de administração**.

Ao ler este e-book, você vai conferir as recomendações de instituições como a Gartner e o Google no que diz respeito à participação dos conselhos de administração na construção das estratégias de promoção da cibersegurança nas empresas.

Confira os próximos tópicos.

Sumário

1

A **cibersegurança** também é responsabilidade dos conselhos de administração

Situações que envolvem incidentes cibernéticos, como sequestros de dados, ataques ransomware, entre tantas outras possibilidades já não podem ser tratadas como um problema exclusivo do departamento de TI. Até porque os prejuízos financeiros e de reputação, sem falar nas consequências previstas na LGPD, afetam a empresa como um todo.

Por isso, a cibersegurança precisa ser tratada como **um dos principais componentes da governança corporativa**, sendo acompanhada de perto pelos integrantes dos conselhos de administração.

A alta administração de uma empresa precisa não apenas estar a par do que o setor de tecnologia anda fazendo, mas também participar das decisões referentes à cibersegurança.

Essa **mudança de postura** é urgente sobretudo depois das mudanças provocadas pela pandemia da Covid-19 nas empresas. Muitas aderiram definitivamente ao trabalho remoto total ou parcialmente, o que ampliou muito a superfície de atuação dos cibercriminosos.

Mas, se o seu negócio manteve o trabalho presencial dos seus colaboradores, nem por isso você deve considerá-lo mais protegido em relação a possíveis incidentes de segurança cibernética.

O cibercrime só faz avançar e as novas tecnologias, como a computação em nuvem, cuja utilização é extremamente importante na atualidade, também ampliam as possibilidades de ataques.

Onde há tecnologia, há riscos cibernéticos

Quanto mais avançadas forem as tecnologias utilizadas em sua empresa, mais importante será contar com um setor dedicado à cibersegurança e com gestores empenhados na meta de manter o negócio protegido.

Isso significa que, mesmo sem ter formação na área de tecnologia e ocupando cargos totalmente administrativos, **os conselheiros precisam se adaptar ao novo cenário** e se familiarizar com os termos tecnológicos, com a linguagem de sistemas e com as funcionalidades de cada software que integra as rotinas da empresa.

Se isso não acontecer, não importa o quanto o seu CISO seja competente e o valor que você tenha investido em cibersegurança, sua empresa definitivamente não estará segura.

E independentemente do porte ou segmento de negócios, ela poderá ser alvo de um ataque para o qual não estará preparada. Em outros termos: ao restringir as questões de cibersegurança ao departamento de TI, a empresa coloca em risco sua própria continuidade, pois os prejuízos relacionados às finanças e à imagem do negócio causados por um ciberataque podem ser irreversíveis.

Por outro lado, quando **a cibersegurança é tomada pelo prisma do risco comercial** decorrente de um ciberataque em potencial, ela fortalece sua estrutura de defesa e ganha maior confiança junto aos clientes. Nesse caso, se um incidente acontecer, será muito mais provável que o negócio consiga lidar com ele e restabeleça suas rotinas em tempo hábil.

2

Novas **responsabilidades** dos conselheiros

Os impactos negativos de um eventual ciberataque bem sucedido podem ser imensuráveis e incluem a perda de dados confidenciais e a queda das receitas, além dos danos à reputação da empresa.

Muitas vezes a interrupção das operações é inevitável, o que causa a insatisfação dos clientes e prejudica seu relacionamento com a marca.

Por outro lado, uma boa gestão de riscos — em que os componentes do conselho de administração trabalham em conjunto com o CISO e o departamento de tecnologia de maneira proativa — pode garantir a proteção dos dados sob a responsabilidade da empresa, melhorar sua reputação e aprimorar a governança corporativa

Nesse contexto, o IBGC sugere nove ações práticas que devem ser assumidas pelos conselheiros:

- **Compreensão dos riscos cibernéticos relacionados aos negócios da organização**
- **Promoção do alinhamento entre a estratégia de negócios e a estratégia de segurança cibernética da empresa**
- **Participação na definição dos ativos críticos da empresa**
- **Confirmação do apetite de riscos da empresa em relação aos riscos cibernéticos**
- **Aprovação da política de segurança da informação corporativa e de seu efetivo modelo de governança**
- **Acompanhamento da evolução na maturidade do ambiente de segurança cibernética da empresa**
- **Supervisão da implementação de uma cultura voltada para a promoção da segurança cibernética em todos os ambientes da empresa**
- **Informação e atualização constantes sobre os planos de crise ou contingência para lidar com possíveis ataques cibernéticos, além de sua aprovação e seu monitoramento**
- **Participação em simulações periódicas sobre crises cibernéticas**

A partir da lista acima, é possível entender que, para alcançar bons resultados quanto à cibersegurança, os conselheiros precisam atuar de maneira integrada ao departamento de tecnologia da informação e, mais especificamente, à equipe responsável pela parte técnica referente à segurança cibernética.

Vamos ver em seguida quais questionamentos os conselhos de administração devem fazer para conseguirem colocar em prática, com o apoio do CISO, uma estratégia eficiente de cibersegurança.

A Cyber Security deve estar focada no valor do negócio, utilizando uma linguagem comum entre as partes interessadas e **vinculando diretamente os riscos corporativos aos controles**. Assim, ela vai ajudar a traduzir as decisões executivas sobre redução de riscos e implementação de controles. O poder da abordagem baseada em risco para otimizar a redução de risco em qualquer nível de investimento é aprimorado por sua flexibilidade, ajustando-se a uma estratégia de análise dos riscos em evolução, conforme a necessidade.

Esse tipo de abordagem implica no reconhecimento de que **soluções de segurança perfeitas não existem**, mas, por outro lado, as empresas que conseguem, a partir dessa perspectiva, equilibrar de forma estratégica a segurança, a escalabilidade, o acesso, a usabilidade e o custo, conseguem proteger-se melhor a longo prazo contra os cibercriminosos, adversários que estão sempre em evolução.

Podemos dizer que a abordagem baseada em riscos é uma estratégia de segurança que atua de dentro para fora na empresa: enquanto outras concepções se focam nas ameaças e nas regulamentações externas, a abordagem proposta aqui é **direcionada para os riscos específicos do negócio**, que ditam a melhor estratégia de segurança e o direcionamento dos investimentos.

3

Informações essenciais das quais os conselhos de administração devem estar cientes

Não há dúvida de que um conselho administrativo precisa lidar constantemente com diversos assuntos, mas esta não é uma justificativa para eximi-lo de participar e conduzir os esforços de cibersegurança da empresa.

A segurança cibernética precisa ocupar um bom espaço nas agendas dos conselheiros para que as ações expostas no tópico anterior sejam colocadas em prática.

Mas por onde os conselhos que ainda não passaram por essa mudança de perspectiva podem começar? O primeiro passo é **buscar informações**. O engajamento a qualquer causa ou propósito começa pela sua compreensão aprofundada.

Sendo assim, existem algumas informações que são essenciais para que os conselheiros passem a atuar ativamente no sentido de manter a empresa protegida dos crimes cibernéticos e preparada para lidar com incidentes.

Vamos enumerar em seguida os principais questionamentos que os conselheiros devem fazer aos setores de tecnologia para obterem as informações essenciais. Essas questões foram propostas em um recente fórum de debates promovido pelo IBGC e publicados posteriormente pela coordenadora-geral do capítulo Rio Grande do Sul da instituição, Michelle Squeff:

1. A cibersegurança está incorporada ao calendário de discussões e à agenda dos conselheiros? A alta liderança toma o tema como uma questão estratégica de negócios?

2. É viável, considerando as especificidades da empresa, criar um comitê especialmente designado para lidar com as questões referentes à cibersegurança? Ou é possível abordar o tema adequadamente dentro de um comitê já existente, como o comitê de auditoria ou de riscos?

3. A empresa recentemente moveu esforços no sentido de identificar suas fragilidades e vulnerabilidades de segurança digital? Ela tem clareza sobre quais são seus ativos críticos? Ela realiza ações como os pentests coordenados pelos chamados "hackers do bem"? Com qual frequência é realizado o mapeamento de riscos?

4. A empresa conta com algum sistema de monitoramento contínuo, como um SOC (Security Operation Center), para que as eventuais invasões sejam identificadas precocemente?

5. A empresa promove reavaliações sistemáticas de seu apetite a riscos? Os investimentos necessários para melhorar os níveis de segurança cibernética são mensurados de forma recorrente?

6. A empresa conta com um plano de ação em que constam o mapeamento dos seus pontos frágeis e a explicitação dos ativos mais críticos?

7. A empresa conta com um seguro contra riscos cibernéticos?

8. A empresa conta com um plano de resposta a incidentes para colocar em prática no caso da ocorrência de um ataque cibernético? Este plano conta com a devida clareza a respeito das atribuições, por exemplo, de quem lidera, quem compõe o comitê de crise, quem negocia, quem é o porta-voz e quais são os especialistas externos envolvidos? Este plano também conta com a explicitação detalhada do passo a passo para que as ações sejam colocadas em prática em uma emergência?

9. A empresa costuma fazer benchmark com outras organizações de sua região ou de seu setor para saber quais práticas preventivas e quais ações têm sido adotadas nos casos de ciberataques?

10. A empresa promove o treinamento e a conscientização das lideranças e dos demais colaboradores sobre os riscos cibernéticos? Todos são orientados com a devida periodicidade a respeito de práticas como a troca periódica de senhas, a definição de senhas fortes, a criptografia de arquivos, o uso de drivers e a identificação de arquivos suspeitos?

4

Previsões da Gartner referentes à cibersegurança nas empresas

A Gartner divulgou recentemente suas principais previsões para os anos de 2023 e 2024 no que diz respeito à segurança cibernética nas empresas.

Vamos ver as principais delas em seguida.

• Até 2027, 50% dos CISOs devem adotar um design para os programas de cibersegurança **centrado no ser humano** para que o atrito operacional seja minimizado e as perspectivas de controle maximizadas. Esse direcionamento é uma resposta ao fato de que, conforme as próprias pesquisas da Gartner, cerca de 90% dos colaboradores das empresas colocam em prática ações inseguras mesmo sabendo que elas aumentam os riscos corridos pela organização;

• A abordagem zero trust tende a tornar-se uma prioridade, sobretudo nas grandes empresas. Até 2026, 10% delas já devem contar com um programa abrangente, mensurável e maduro, o que representa um grande avanço, já que atualmente apenas 1% das grandes corporações têm um programa de zero trust em funcionamento. O amadurecimento desta abordagem pode ser extremamente técnico e complexo, mas é importante começar por pequenos passos desenvolvendo uma **mentalidade de confiança zero** em todos os setores da empresa e ir evoluindo aos poucos;

• 10% das empresas obterão bons resultados ao utilizarem a **privacidade como diferencial competitivo**, pois contar com um programa de privacidade pode possibilitar o uso dos dados de forma mais ampla, estimulando a confiança por parte dos clientes, parceiros, fornecedores, investidores e

órgãos reguladores. A recomendação da Gartner é que os líderes em cibersegurança implementem um padrão de privacidade abrangente seguindo os princípios da LGPD para que suas empresas possam crescer sem obstáculos;

• 75% dos colaboradores serão capazes de **adquirir, modificar e criar tecnologia fora da visibilidade de TI** até 2027. A Gartner recomenda o reenquadramento dos modelos operacionais com um pensamento que vai além da tecnologia e da automação de tarefas, envolvendo mais profundamente os colaboradores, de modo que eles contem com o devido conhecimento para atuar proativamente e de maneira bem informada;

• Metade dos líderes de cibersegurança vão buscar, sem serem bem sucedidos, a orientação da tomada de decisões a partir da quantificação dos riscos cibernéticos. Para a Gartner, é importante priorizar a quantificação de temas solicitados pelos líderes e **não se concentrar em análises genéricas** para buscar o engajamento dos colaboradores quanto à cibersegurança;

• Quase **metade dos líderes de segurança cibernética deve trocar de emprego** até 2025 e quase 25% desses profissionais devem ir para funções diferentes daquelas desempenhadas hoje, sobretudo por conta do estresse no ambiente de trabalho. A Gartner entende que não é possível eliminar as pressões do trabalho, mas recomenda que as empresas ofereçam apoio aos profissionais na realização de trabalhos desafiadores, promovendo mudanças culturais e também nas regras de engajamento;

• 70% dos conselhos de administração devem contar com **pelo menos um profissional com experiência significativa em cibersegurança** até 2026. Isso reflete o reconhecimento desses profissionais como parceiros de negócios a partir de uma comunicação mais efetiva com os conselheiros, demonstrando que um bom programa de cibersegurança, mais do que evitar acontecimentos desfavoráveis, melhora a capacidade do negócio de assumir riscos de forma mais eficiente. A Gartner recomenda a antecipação das mudanças para que a cibersegurança seja apoiada via conselho de administração a partir de um relacionamento próximo que melhore a confiança e o suporte;

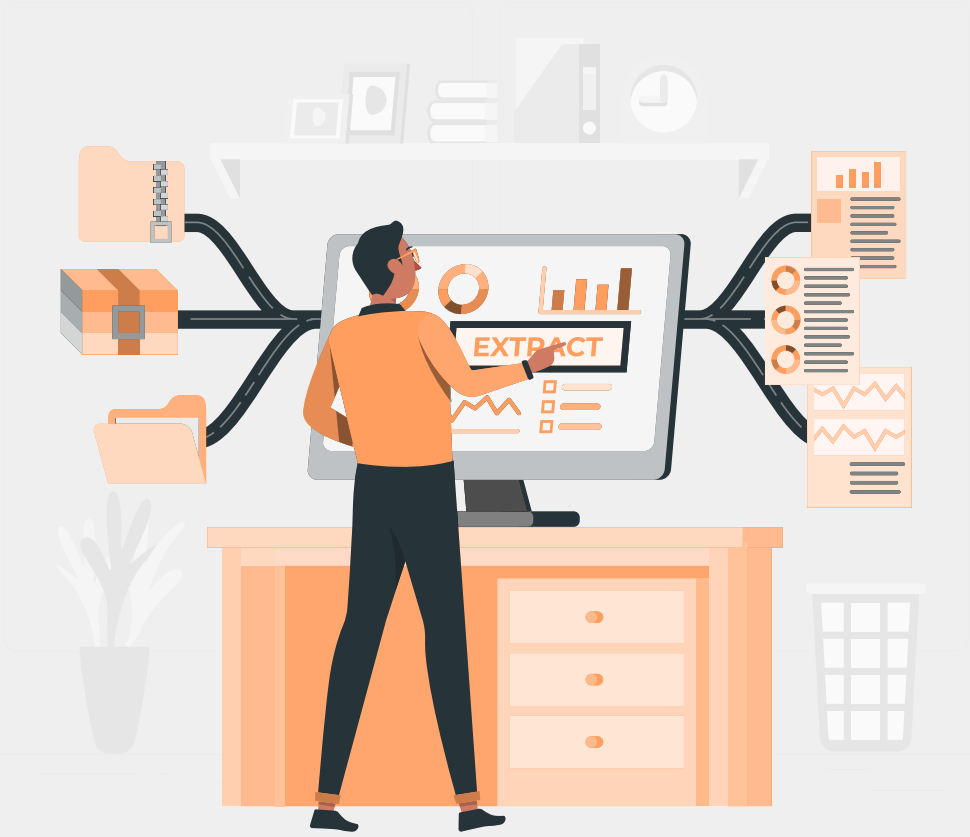
• Até 2026, **os dados de gerenciamento de exposição devem ser aproveitados** por mais de 60% dos recursos de detecção, investigação e resposta a ameaças para que os riscos detectados sejam priorizados. As superfícies de ataques organizacionais estão em constante expansão, assim como os serviços em nuvem e o uso de softwares como serviço (SaaS). Nesse contexto, as empresas precisam de uma plataforma unificada para gerenciar a detecção e a resposta aos incidentes em potencial a partir de uma visão completa dos riscos e de seus impactos.

5

Recomendações do Google para os conselhos administrativos

Em um relatório divulgado recentemente, o Google também destaca a importância do engajamento dos conselhos de administração nos assuntos ligados à cibersegurança corporativa e faz uma **série de recomendações**, a começar pelo apontamento do NIST Cybersecurity Framework como uma relevante ferramenta para o engajamento dos conselheiros.

A partir da compreensão e da promoção de esforços no sentido de colocar em prática os cinco pilares do NIST CSF (identificar, proteger, detectar, responder e recuperar), os conselhos de administração podem obter uma postura mais proativa quando o assunto é a cibersegurança.



O relatório do Google também aborda três princípios a serem seguidos para a supervisão eficaz dos riscos cibernéticos:

Buscar instrução

Os conselheiros precisam aprender sobre cibersegurança, se familiarizar com os termos técnicos e ficar a par das vulnerabilidades e riscos cibernéticos corridos pela empresa para que as decisões relacionadas ao assunto sejam mais assertivas;

Ser comprometido

O conselheiros precisam manter uma comunicação efetiva e um trabalho conjunto com os CISOs para que as lacunas mais críticas e as necessidades de recursos sejam devidamente compreendidas;

Manter-se atualizado

a área de tecnologia passa por mudanças e evoluções constantes e o cibercrime avança a cada dia com maior velocidade. Assim, para manter o engajamento e obter bons resultados quanto à estratégia de cibersegurança, os conselheiros precisam fazer perguntas, manter-se a par dos relatórios em andamento e agir de maneira proativa em relação ao trabalho do CISO.

Entre os principais questionamentos a serem feitos aos CISOs estão os seguintes:

- **Quão bons somos em segurança cibernética?**
- **Quão resilientes somos?**
- **Qual é o nosso risco?**

Como a estratégia de cibersegurança precisa ser extremamente dinâmica, essas perguntas devem ser refeitas e as respostas reavaliadas com a periodicidade adequada.

O Google também destaca a importância de estabelecer uma **conexão entre a inteligência de ameaças e a mitigação de riscos** e de promover o engajamento dos conselheiros também em relação à utilização de tecnologias de inteligência artificial.

Para que os benefícios dessas tecnologias sejam maximizados, o Google recomenda a adoção de uma abordagem que engloba três frentes em um trabalho conjunto dos conselheiros com os CISOs:

- **Proteger:** os conselheiros devem se familiarizar com a forma como o CISO planeja implementar sistemas seguros de inteligência artificial e proteger os dados e controles de acesso;
- **Dimensionar:** o trabalho conjunto entre os conselheiros e o CISO deve promover a identificação da melhor maneira de aproveitar o poder da IA para alcançar melhores resultados de cibersegurança;
- **Evoluir:** devem ser organizados briefings regulares para detectar tendências emergentes de IA e novos riscos de segurança. Além disso, é importante a avaliação de possíveis parcerias para desenvolver melhores práticas, ferramentas e modelos de ameaças que abordem interações e riscos típicos de IA.

6

Conclusão

Se você chegou até aqui, agora já está a par dos principais direcionamentos a serem colocados em prática para que o seu conselho de administração adote um **posicionamento proativo** quanto às ações organizacionais relacionadas à cibersegurança.

Agora é hora de colocar tudo o que mencionamos acima em prática e, para esta missão, você pode contar com o EcoTrust, uma plataforma de inteligência em riscos cibernéticos que ajuda as empresas a priorizar riscos cibernéticos que podem impactar o negócio.

Acesse o site e saiba mais sobre esta tecnologia.

Eco Trust

Adotar métodos corretos e eficientes e aplicá-los com regularidade pode resultar na **economia de custos e aumento da competitividade** de negócios que dependem de tecnologia. As vantagens da segurança da informação e da proteção de dados para o presente e o futuro são diversas e podem evitar prejuízos muito severos.

É importante entender que processos relacionados a gestão de vulnerabilidades são os verdadeiros **investimentos em prevenção** e cuidados mais do que necessários. É hora de começar a agir de forma eficiente o mais rápido possível em favor da continuidade do negócio. Veja como a Eco IT pode te ajudar.

A **EcoTrust**, nossa **plataforma de *Inteligência em Riscos Cibernéticos***, possibilita que os líderes de Segurança e TI possam tomar decisões importantes de forma mais assertiva quando o assunto for segurança cibernética. Através da descoberta e gerenciamento de vulnerabilidades e riscos cibernéticos, de forma orquestrada, simplificada e com abordagem orientada aos riscos de negócio, a plataforma traz uma visão estratégica (negócio) com embasamento em indicadores técnicos (táticos e operacionais).

E para comprovar todas essas vantagens, você pode experimentar a plataforma gratuitamente. Basta clicar no botão abaixo.

Conhecer a solução

Entre em contato

site

www.ecotrust.io

ECOTRUST