CIBERSEGURANÇA PARA ORGANIZAÇÕES MAIS PEQUENAS

LISTA DE VERIFICAÇÃO DA ADMINISTRAÇÃO: LIDERANÇA DE CIBERSEGURANÇA

PRINCÍPIOS BÁSICOS DA GOVERNAÇÃO DO RISCO CIBERNÉTICO

☐ **Como um grupo, avaliamos periodicamente se o Conselho pode responder afirmativamente às seguintes questões:**

- A sua organização cumpriu os requisitos estatutários e regulamentares relevantes, por exemplo, RGPD (Regulamento Geral sobre Proteção de Dados)?
- A sua organização quantificou as suas exposições cibernéticas e testou a sua resiliência financeira?
- A sua organização tem um plano de melhoria para garantir que as exposições estão dentro da sua apetência pelo risco acordada?
- O Conselho discute regularmente informações concisas, claras e exequíveis relativamente à ciber-resiliência da organização fornecidas pela direção?
- A sua organização tem planos de resposta a incidentes que tenham sido recentemente tratados a título de ensaio, incluindo ao nível do Conselho?
- As funções dos responsáveis principais pela gestão do risco cibernético são claras e estão em concordância com as três linhas de defesa?
- Já obteve validação e garantia independentes da postura de risco cibernético da sua organização, por exemplo, por meio de teste, certificação ou seguro?

☐ **Se não conseguir responder afirmativamente a uma ou mais das questões anteriores, trabalhe com o seu CEO, CISO, pessoal da organização relevante e/ou recursos externos para corrigir o problema.**

SUPERVISÃO

☐ **Certifique-se de que o conselho está ciente do seu papel como o responsável máximo no que se refere ao risco cibernético e ciber-resiliência da sua organização.**

☐ **Delegue a supervisão a uma comissão específica do conselho, se considerado necessário.**

☐ **Designe um responsável da empresa, normalmente designado como CISO (Chief information security officer, [Diretor Executivo de Segurança da Informação]), para ser responsável por reportar a capacidade da sua organização de gerir a ciber-resiliência e o progresso na implementação dos objetivos da ciber-resiliência.**

☐ **Certificar-se de que este responsável tem acesso regular ao Conselho, autoridade suficiente, domínio do assunto, experiência e recursos para cumprir estes deveres.**

☐ **Definir anualmente a tolerância ao risco da sua organização, garantindo a consistência com a sua estratégia empresarial e apetência pelo risco.**

☐ **Certificar-se de que é realizada anualmente uma revisão de ciber-resiliência independente e formal da sua organização.**

☐ **Integre a ciber-resiliência e a avaliação de riscos na estratégia global de negócio da sua organização, gestão de risco, orçamentação e alocação de recursos.**

☐ **Analisar regularmente os riscos de terceiros.**

☐ **Supervisione a criação, implementação, teste e melhoria contínua dos planos de ciber-resiliência, assegurando conformidade em toda a sua organização e que o seu CISO ou outro responsável reporta regularmente os mesmos à administração.**

☐ **Rever periodicamente o seu desempenho relativamente ao acima e considerar aconselhamento independente para melhoria contínua.**

MANTER-SE INFORMADO

- ☐ **Certifique-se de que todos os indivíduos que participam no Conselho têm competências e conhecimentos adequados e atualizados para compreender e gerir os riscos colocados por ameaças cibernéticas.**
- ☐ **Solicite aconselhamento regular à direção sobre a exposição ao risco atual e futura da sua organização, requisitos regulamentares relevantes e referências da indústria e da sociedade quanto à apetência pelo risco. Planeie envolver-se em:**
  - Briefings regulares sobre deveres criados por novos regulamentos e legislação,
  - Planeamento conjunto da comissão executiva e do conselho executivo e visitas aos colegas e líderes da melhor prática em cibersegurança,
  - Briefings de segurança sobre o ambiente de ameaças, e
  - Trocas ao nível ao nível do Conselho no que se refere a governança e comunicação.
- ☐ **Responsabilize a direção por comunicar uma avaliação quantificada e compreensível dos riscos cibernéticos, ameaças e eventos como um elemento de ordem de trabalhos permanente durante as reuniões do Conselho.**
- ☐ **Comunique regularmente com a gestão e outro pessoal relevante sobre desenvolvimentos relacionados com desafios sistémicos contínuos, tais como vulnerabilidades da cadeia de abastecimento, dependências comuns e lacunas na partilha da informação.**

DEFINIR O TOM

- ☐ **Certifique-se de que o pessoal a todos os níveis reconhece que cada um tem responsabilidades importantes para garantir a ciber-resiliência da sua organização.**
- ☐ **Supervisione o papel da direção na promoção e manutenção da cultura de risco da sua organização. Avalie regularmente a eficácia da cultura de risco da sua organização, considerando o impacto da cultura na segurança e solidez e proceder a alterações quando necessário.**
- ☐ **Torne claro que espera que todo o pessoal atue com integridade e que remeta rapidamente a não conformidade observada dentro ou fora da sua organização.**

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE · ICBA Independent Community Bankers of America®