

GUIA DO NÍVEL DO CONSELHO: LIDERANÇA DE CIBERSEGURANÇA

SUPERVISÃO

Como o nível mais alto da liderança da sua organização, o Conselho assume a máxima responsabilidade por controlar o risco cibernético e, por conseguinte, deve supervisionar a estratégia, políticas e atividades da organização nesta área. Especificamente, o Conselho deve:

- Assumir a responsabilidade final pela supervisão do risco cibernético e da resiliência, seja como Conselho no seu todo ou através da delegação de supervisão numa Comissão de Conselho específica.
- Designar um responsável da empresa, normalmente o 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; garantir 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.
- Supervisionar 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.
- Integrar a ciber-resiliência e a avaliação de riscos na estratégia global de negócio da sua organização, gestão de risco, orçamentação e alocação de recursos, com o objetivo de integrar totalmente o risco cibernético em risco operacional global. Analisar regularmente os riscos de terceiros.
- Rever periodicamente o seu desempenho relativamente ao acima e considerar aconselhamento independente para melhoria contínua.

MANTER-SE INFORMADO

A supervisão eficaz do risco cibernético do Conselho depende do domínio dos membros sobre o tema e da informação atualizada.

- 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. Além disso, envolva-se em briefings regulares sobre os últimos desenvolvimentos em relação ao cenário de ameaças e ambiente regulamentar, planeamento conjunto e visitas aos pares de melhores práticas e líderes em cibersegurança e trocas ao nível da 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.
- Mantenha a consciencialização de desafios sistémicos contínuos, tais como vulnerabilidades da cadeia de fornecimento, dependências comuns e lacunas na partilha de informação.

DEFINIR O TOM

Juntamente com a direção sénior, o Conselho deve definir e exemplificar os valores fundamentais, a cultura de risco e as expetativas da sua organização relativamente à ciber-resiliência.

- Promova uma cultura em que o pessoal a todos os níveis reconheça as suas responsabilidades importantes em garantir a ciber-resiliência da sua organização. Liderar dando o exemplo.
- Supervisione o papel da direção na promoção e manutenção da cultura de risco da sua organização. Promova, monitorize e avalie a cultura de risco, 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.

Princípios Básicos da Governação do Risco Cibernético

Confirme que pode responder afirmativamente às seguintes perguntas:

- A sua organização cumpriu os requisitos estatutários e regulamentares relevantes?
- 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?