

# LISTA DE VERIFICAÇÃO DO CEO: LIDERANÇA DE CIBERSEGURANÇA

## GOVERNANÇA

- Nomear um Diretor Executivo de Segurança da informação (CISO), caso não exista.
- Estabelecer e manter uma política de cibersegurança de toda a organização que seja baseada no risco e informada de acordo com as normas e diretrizes internacionais, nacionais e da indústria.
- Definir funções e responsabilidades para todo o pessoal envolvido na cibersegurança. Trabalhar com o CISO para identificar as funções de cibersegurança adequadas e direitos de acesso para todos os níveis de pessoal.
- Estabelecer ou identificar canais de comunicação claros entre quaisquer unidades separadas ou pessoal que lide com diferentes aspetos da cibersegurança.
- Certificar-se de que o CISO tem uma linha direta e clara de comunicação para relacionar ameaças de forma atempada para si e para o Conselho.
- Manter um convite regular para o seu CISO ou outro pessoal técnico no sentido de informar a ata direção.
- Verificar se as políticas, normas e mecanismos de cibersegurança são uniformes em toda a organização.

## AVALIAÇÃO E GESTÃO DE RISCOS

- Realizar uma avaliação de risco de cibersegurança em colaboração com o seu CISO ou outro pessoal técnico, que deve incluir:
  - Descrever os ativos da sua organização e os seus vários níveis de dependência tecnológica,
  - Avaliar a maturidade da sua organização e os riscos inerentes associados às dependências tecnológicas dos seus ativos,
  - Determinar o estado desejado da maturidade da sua organização,
  - Compreender onde as ameaças de cibersegurança se encontram na lista de prioridades de risco da sua organização,
  - Identificar lacunas entre o seu estado atual de cibersegurança e o estado alvo pretendido,
  - Implementar planos para atingir e sustentar a maturidade,
  - Avaliar e reservar fundos para investir na segurança e colmatar lacunas existentes,
  - Reavaliar continuamente a maturidade, os riscos e os objetivos da segurança cibernética da sua organização, e
  - Considerar medidas de proteção como a compra de um seguro cibernético.
- Analisar e apresentar resultados aos principais intervenientes e ao Conselho.
- Planear supervisionar quaisquer medidas para aumentar a preparação cibernética e monitorizar o progresso.

## PROPÓSITO ORGANIZACIONAL

- Discuta regularmente o risco cibernético e a segurança ao nível da liderança.
- Integre uma avaliação da cibersegurança de uma organização ao considerar fusões e aquisições.
- Certifique-se de que a formação de cibersegurança faz parte de toda a integração de funcionários e que todos os funcionários assinam documentos em que concordam em cumprir as políticas de cibersegurança da organização.
- Institua uma análise anual das políticas de cibersegurança da organização.
- Institua formação de cibersegurança recorrente para todos os funcionários.
- Incentive o pessoal técnico a participar na partilha voluntária de informação sobre ameaças e incidentes de cibersegurança.
- Certifique-se de que a cibersegurança é sempre considerada quando a sua organização avalia potenciais fornecedores e partilha dados com terceiros.



[CarnegieEndowment.org](https://www.CarnegieEndowment.org)

