excelia

A cibersegurança já está na agenda do CFO

O que é a Diretiva NIS2?

A Diretiva NIS2 da União Europeia reforça a cibersegurança e a resiliência digital em setores estratégicos como energia, saúde, transporte, finanças, telecomunicações, entre outros. O seu objetivo é claro:

Prevenir ciberataques, proteger a economia e garantir a continuidade operacional das organizações.

Obrigações-chave:

- Gerir riscos de cibersegurança em toda a organização e nos seus fornecedores.
- A administração, incluindo os CFOs, deve aprovar e supervisionar as medidas implementadas.
- Notificar incidentes graves de cibersegurança no prazo máximo de 24 horas.
- Possíveis sanções económicas e penais em caso de incumprimento.

Impacto nas finanças

Os ciberincidentes não afetam apenas a tecnologia: têm um impacto direto nas finanças da empresa. Desde a tesouraria aos resultados, passando pela gestão de contratos e fornecedores, o CFO torna-se uma figura-chave que deve antecipar riscos, proteger os ativos financeiros e garantir que a organização cumpre a regulamentação.

Principais efeitos na área financeira:

- Custos diretos decorrentes de ciberincidentes: impacto na tesouraria, provisões e resultados.
- O CFO desempenha um papel essencial na gestão de contratos e fornecedores sujeitos a controlos de segurança.
- Riscos legais e reputacionais associados ao incumprimento da regulamentação.
- A cobertura de incidentes em muitas apólices de seguros já depende do cumprimento da diretiva NIS2.
- O cumprimento da regulamentação será objeto de avalição em auditorias, processos de due diligence e revisões regulatórias.

A diretiva NIS2 da União Europeia introduz um conjunto de novas exigências em matéria de cibersegurança que afetam diretamente a função financeira das organizações. Esta regulamentação não se limita a proteger setores críticos, como o financeiro, mas visa também garantir a continuidade operacional e reforçar a confiança no ecossistema digital.

Aspectos-chave para os CFOs:

- **Gestión de riesgos integral:** é fundamental implementar uma abordagem abrangente que envolva não só a organização, mas também toda a cadeia de fornecimento..

- **Continuidade do negócio:** um incidente não gerido implica interrupções, perda de receitas e possíveis litígios com clientes e/ou fornecedores.

- **Cumprimento regulamentar:** os CFOs devem garantir que a empresa está em conformidade com as novas regulamentações, uma vez que o incumprimento pode resultar em sanções económicas e danos reputacionais.

- **Colaboração interdepartamental:** promover a colaboração entre departamentos é essencial para garantir uma resposta eficaz a incidentes de cibersegurança.

- **Planeamento financeiro:** a alocação de recursos para a cibersegurança deve ser uma prioridade no planeamento financeiro, considerando tanto os custos diretos como os indiretos associados a potenciais incidentes.

O CFO, a NIS2 e a cadeia de fornecimento

A cibersegurança deixou de ser uma preocupação exclusiva da empresa: cada fornecedor e parceiro representa um ponto crítico de risco. Os CFOs devem garantir que toda a cadeia de fornecimento cumpre os requisitos da NIS2, uma vez que qualquer incumprimento pode resultar em perdas financeiras e consequências legais

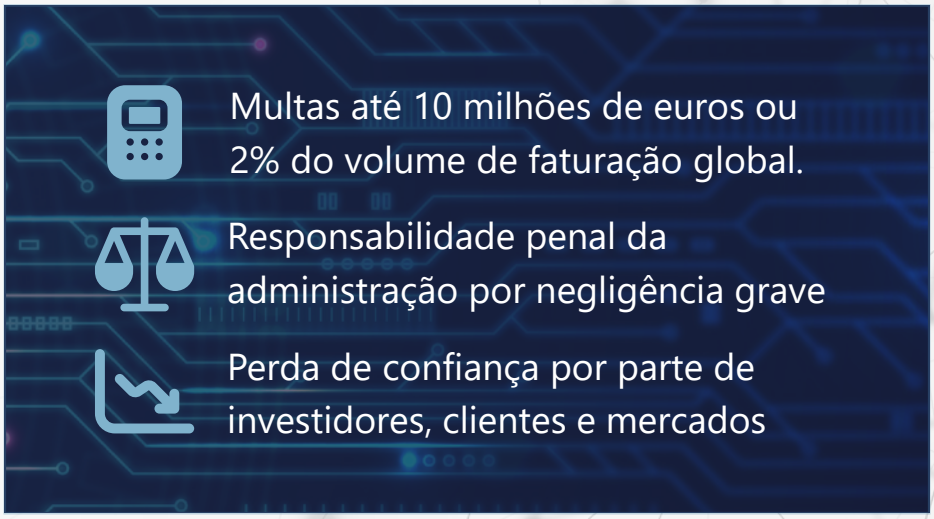
Exigências para fornecedores:

- Avaliações periódicas de riscos.
- Cláusulas de segurança nos contratos.
- Monitorização e auditorias constantes.
- PPlanos claros de notificação e resposta a incidentes.

Proteger a empresa é um processo que exige planeamento e antecipação. Os CFOs devem iniciar a implementação destas medidas antes da entrada em vigor da NIS2, garantindo assim a conformidade e evitando possíveis sanções.

Consequências do incumprimento da NIS2

A NIS2 estabelece obrigações claras e exigentes para as empresas, que passam a ser obrigadas a reportar incidentes graves num prazo máximo de 24 horas. Este requisito não é opcional: exige planeamento, supervisão contínua e adaptação de processos para proteger os ativos e assegurar a continuidade do negócio



Como a excelia apoia os CFOs

A excelia é especialista em cibersegurança, contando com uma equipa altamente experiente e certificada, dedicada a responder às necessidades e desafios específicos de cada organização, oferecendo soluções eficazes que visam proteger a operação, os ativos e a reputação da sua empresa

- Avaliações NIS2 focadas na gestão do risco económico.
- Estratégias para gestão de fornecedores e contratos.
- Planos de ação para assegurar a conformidade e mitigar riscos legais.
- Suporte contínuo para proteger a estabilidade financeira e a reputação corporativa.

A NIS2 não espera.

A cibersegurança é um processo contínuo: comece hoje e transforme-a numa vantagem competitiva.

Contacte hoje um especialista da excelia e assegure o futuro financeiro e regulatório da sua empresa.

nmartins@excelia.com · +351 926 437 847

Avenida da Liberdade, 110, 1269-046 Lisboa