# EFAA para PME

## Lista de Verificação de Cibersegurança

European Federation of Accountants and Auditors for SMEs –
Associação Internacional sem Fins Lucrativos

## ÍNDICE



### Nota editorial

**Documento original:** *EFAA for SMEs – Cybersecurity Checklis*t, Julho de 2026

**Versão portuguesa:** Ordem dos Contabilistas Certificados responsável pela adaptação e revisão técnica e terminológica da tradução. Reprodução autorizada pela EFAA for SMEs.

Em caso de divergência de interpretação, deve atender-se ao conteúdo do original em língua inglesa, disponível no site oficial da EFAA for SMEs.

# EFAA para PME

## Lista de Verificação de Cibersegurança

***Uma visão geral prática e proporcional à dimensão, destinada a gabinetes e sociedades de contabilidade de pequena e média dimensão e aos respetivos clientes PME***

### Por que razão isto é importante

Os gabinetes de contabilidade e consultoria tratam e conservam informação muito sensível dos seus clientes — dados fiscais, processamento de salários, demonstrações financeiras e dados de identificação —, o que os torna alvos atrativos para *ransomware* (*software* de sequestro), fraude em faturação e pagamentos e comprometimento do correio eletrónico empresarial (BEC). Um incidente pode perturbar o cumprimento de prazos declarativos, violar a confidencialidade e comprometer a confiança dos clientes. A cibersegurança é, por isso, uma questão de gestão e de responsabilidade profissional, não apenas técnica, cada vez mais relacionada com o RGPD e a Diretiva SRI 2 (NIS 2).

Esta lista de verificação ajuda a rever as principais medidas de segurança no planeamento e na execução do trabalho e a discuti-las com o titular ou os sócios, os colaboradores e os clientes. É um instrumento sintético e proporcional à dimensão do gabinete — percorra todos os pontos, sem contornar as medidas propostas.


*Os seis domínios abrangidos por esta lista de verificação*

## Modo de utilização

**Como preencher esta lista de verificação**

1. Identifique a dimensão do seu gabinete: XS, S ou M.
2. Reveja todas as medidas de segurança em cada um dos seis domínios.
3. Assinale o quadrado à esquerda de cada medida efetivamente implementada. Pode assinalar mais do que um quadrado em cada domínio.
4. Utilize as colunas XS / S / M para compreender o nível de implementação esperado em função da dimensão do gabinete (a).
5. A nota para gabinetes médios («M*») estabelece expectativas adicionais de formalização, documentação, revisão periódica e evidência da implementação.

a) O símbolo ○ remete para contexto em que é aceitável uma versão mais simples e informal — deve ser desenvolvida à medida que o gabinete cresce.
O símbolo ● constitui o nível mínimo indispensável para qualquer gabinete, independentemente da sua dimensão. Volte a aplicar esta lista de verificação, pelo menos uma vez por ano e após qualquer alteração relevante (novo sistema, mudança de instalações, entrada ou saída de um colaborador-chave).

## Adequação à dimensão do gabinete

| Dimensão do gabinete | Número típico de pessoas | O que caracteriza uma boa prática |
|---|---|---|
| **Muito pequeno (XS)** | Contabilista Certificado em prática individual, com uma equipa até cerca de 5 pessoas | Em regra, sem equipa interna de tecnologias de informação (TI). A segurança assenta sobretudo em prestadores reputados de serviços em nuvem, dispositivos atualizados, autenticação multifator (MFA) e bons hábitos. Mantenha as políticas breves e práticas. |
| **Pequeno (S)** | Cerca de 6 a 20 pessoas | Designe um responsável ou ponto de contacto para a cibersegurança e formalize por escrito as políticas essenciais, as cópias de segurança, a revisão de acessos e a resposta básica a incidentes. |
| **Médio (M)** | Cerca de 20 a 50 ou mais pessoas, eventualmente com múltiplos escritórios | Devem existir controlos e políticas documentados, revisão periódica de acessos, cópias de segurança e configurações críticas, evidência da formação e das verificações essenciais e testes, quando aplicável. Pondere o alinhamento com um referencial reconhecido, como a ISO/IEC 27001 ou um referencial nacional. |

## 1. Governação e sensibilização

| ✓ | Medida de segurança | XS | S | M* |
|---|---|---|---|---|
| ☐ | A gestão trata o risco de cibersegurança como um risco de negócio, e não apenas como uma questão de TI, e designou uma pessoa responsável pelo respetivo acompanhamento. | ● | ● | ● |
| ☐ | Os colaboradores recebem, pelo menos uma vez por ano, formação básica sobre phishing, engenharia social e utilização segura do correio eletrónico, dos serviços em nuvem e dos dispositivos móveis. | ● | ● | ● |
| ☐ | Existe uma política simples, por escrito, sobre a utilização aceitável do correio eletrónico, da Internet, dos dispositivos pessoais e dos serviços em nuvem, incluindo o armazenamento de dados de clientes. | ○ | ● | ● |
| ☐ | O gabinete identificou previamente o especialista externo de TI ou cibersegurança a contactar em caso de incidente grave. | ● | ● | ● |
| M* | **Em gabinetes médios (M), as políticas devem ser revistas periodicamente, as responsabilidades claramente atribuídas e a conclusão da formação registada.** | | | |

## 2. Acessos, identidade e palavras-passe

| ✓ | Medida de segurança | XS | S | M* |
|---|---|---|---|---|
| ☐ | São utilizadas contas individuais de utilizador em todos os sistemas com dados de clientes ou dados financeiros; evitam-se credenciais genéricas partilhadas. | ● | ● | ● |
| ☐ | São exigidas palavras-passe ou frases-passe robustas, com pelo menos 12 caracteres, não reutilizadas em diferentes sistemas; recomenda-se um gestor de palavras-passe. | ● | ● | ● |
| ☐ | A autenticação multifator (MFA) está ativada sempre que possível, nomeadamente no correio eletrónico, no software de contabilidade em nuvem, no acesso remoto e nas contas de administrador. | ● | ● | ● |
| ☐ | Os direitos de acesso seguem o princípio da «necessidade de conhecer», são revistos periodicamente e as contas e os acessos dos antigos colaboradores são desativados sem demora. | ○ | ● | ● |
| **M*** | **Em gabinetes médios (M), a revisão de acessos deve obedecer a um ciclo documentado, as contas de administrador devem ser controladas separadamente e as entradas, mudanças de funções e saídas de colaboradores documentadas.** | | | |

## 3. Dispositivos, correções e proteção *antimalware*

| ✓ | Medida de segurança | XS | S | M* |
|---|---|---|---|---|
| ☐ | Todos os portáteis, computadores de secretária e servidores usados no trabalho profissional utilizam sistemas operativos suportados pelos fornecedores e recebem atualizações automáticas de segurança. | ● | ● | ● |
| ☐ | Está instalada proteção antivírus e *antimalware* atualizada em todos os equipamentos, incluindo dispositivos móveis, sempre que viável. | ● | ● | ● |
| ☐ | As *firewalls* dos equipamentos estão ativadas, a rede Wi-Fi do escritório está protegida e são alteradas as palavras-passe predefinidas do router e das contas de administrador. | ● | ● | ● |
| ☐ | Apenas é instalado *software* licenciado e fidedigno, obtido em lojas de aplicações ou nos sítios oficiais dos fornecedores. | ● | ● | ● |
| **M*** | **Em gabinetes médios (M), mantenha um inventário básico de dispositivos e software, acompanhe as correções de segurança de maior risco e conserve evidência da aplicação das atualizações essenciais.** | | | |

## 4. Proteção de dados, nuvem e cópias de segurança

| ✓ | Medida de segurança | XS | S | M* |
|---|---|---|---|---|
| ☐ | O gabinete mantém um registo dos principais ativos de informação, incluindo ficheiros de clientes, papéis de trabalho, processamento de salários, ficheiros fiscais e arquivos de correio eletrónico. | ● | ● | ● |
| ☐ | Os dados confidenciais dos clientes são cifrados; os portáteis e os suportes amovíveis estão protegidos por cifragem integral do disco. | ● | ● | ● |
| ☐ | A utilização de serviços em nuvem está documentada, com identificação clara das responsabilidades do gabinete e do prestador pelas configurações de segurança. | ○ | ● | ● |
| **M*** | **Em gabinetes médios (M), os contratos ou acordos com prestadores de serviços em nuvem devem ser documentados e revistos, as responsabilidades pela retenção dos dados claramente definidas e os testes de restauro estruturados e registados.** | | | |

## 5. Correio eletrónico, phishing e trabalho remoto

| ✓ | Medida de segurança | XS | S | M* |
|---|---|---|---|---|
| ☐ | Os colaboradores sabem detetar e comunicar mensagens, anexos, ligações e pedidos suspeitos de alteração de dados ou de instruções de pagamento. | ● | ● | ● |
| ☐ | Estão implementados controlos básicos de segurança do correio eletrónico, incluindo filtragem de spam, análise de anexos e bloqueio de tipos de ficheiro perigosos. | ● | ● | ● |
| ☐ | O acesso remoto, incluindo rede privada virtual (VPN), ambiente de trabalho remoto e portais em nuvem, utiliza MFA e está restrito a dispositivos autorizados. | ● | ● | ● |
| ☐ | Existem regras para a utilização de dispositivos pessoais para fins profissionais (BYOD), incluindo configurações mínimas de segurança e locais autorizados para armazenar dados de clientes. | ○ | ● | ● |
| M* | **Em gabinetes médios (M), as regras de acesso remoto devem ser formalizadas, a utilização de dispositivos pessoais para fins profissionais (BYOD) limitada ou sujeita a condições e os acessos de maior risco revistos sempre que viável.** | | | |

## 6. Resposta a incidentes e continuidade

| ✓ | Medida de segurança | XS | S | M* |
|---|---|---|---|---|
| ☐ | Existe um procedimento simples e escrito de resposta a incidentes, que define quem contactar, como isolar os sistemas e quando notificar clientes e autoridades. | ○ | ● | ● |
| ☐ | Estão identificados os processos críticos, como processamento de salários, declarações de IVA, obrigações legais de relato e trabalho de campo de auditoria, com um plano básico de continuidade. | ○ | ● | ● |
| ☐ | Os contactos essenciais, incluindo decisores, apoio de TI, consultores e seguradoras, estão também disponíveis offline e mantidos atualizados. | ● | ● | ● |
| ☐ | Os incidentes significativos são analisados posteriormente e dão origem a medidas concretas de melhoria, como formação adicional ou melhorias nos processos e controlos. | ○ | ● | ● |
| M* | **Em gabinetes médios (M), mantenha um registo de incidentes, documente as medidas de seguimento, atribua responsabilidades e realize ocasionalmente uma revisão do procedimento ou uma simulação de resposta.** | | | |

**Autoavaliação rápida**

- Todos os requisitos essenciais e a maioria dos restantes estão assinalados — existe uma base sólida; mantenha as medidas atualizadas e testadas.
- A maioria dos requisitos essenciais está implementada, mas há lacunas — dê prioridade aos que ainda não estão assinalados.
- Faltam vários requisitos essenciais — trate o assunto como prioritário, começando pela autenticação multifator (MFA), pelas cópias de segurança, pelas atualizações e pela formação.

**Nota:** Esta lista de verificação é uma orientação geral e não substitui orientações específicas sobre a Diretiva SRI 2 (NIS 2), o RGPD ou os referenciais nacionais de cibersegurança. Adapte-a ao seu gabinete e aos seus clientes.