# BOAS PRÁTICAS DE CIBERSEGURANÇA

As 10 boas práticas essenciais para o trabalhador, o cidadão e as entidades

**PME · Administração Pública Regional e Local**

*1.ª fase — conjunto base para partilha faseada no site*

Setembro de 2026

---

*"A verdadeira força da cibersegurança reside na prevenção, não na reação."*

# Introdução

A cibersegurança diz respeito a todos: compreende o conjunto de atividades necessárias para proteger, de ciberameaças, as redes e os sistemas de informação, os seus utilizadores e as demais pessoas afetadas. Uma parte importante dos incidentes tem origem em falhas comportamentais — pelo que o conhecimento e a adoção sistemática de boas práticas são, na prática, a defesa mais eficaz.

Este documento reúne as 10 boas práticas de cibersegurança consideradas mais relevantes nesta primeira fase, com aplicação transversal a três públicos: o trabalhador, o cidadão em geral e as entidades — incluindo pequenas e médias empresas (PME) e organismos da Administração Pública regional e local.

O conteúdo baseia-se em material de formação e sensibilização já desenvolvido internamente e nas orientações públicas do Centro Nacional de Cibersegurança (CNCS), disponíveis em dyn.cncs.gov.pt/pt/boaspraticas e nos restantes recursos de sensibilização do CNCS.

## Como usar este documento

Cada boa prática está organizada em página própria, com uma imagem ilustrativa dedicada — pensada para poder ser destacada e partilhada de forma autónoma (por exemplo, no site, em cartazes internos ou em publicações periódicas) — seguida de uma explicação sucinta e de um conjunto de ações concretas e verificáveis.

A indicação “Aplica-se a” no início de cada secção identifica os públicos para os quais a prática é diretamente relevante, permitindo priorizar a comunicação consoante a audiência de cada publicação.

## Próximas fases

Numa fase seguinte, poderão ser desenvolvidas boas práticas adicionais dirigidas especificamente às entidades — organizacionais (políticas, funções e responsabilidades, inventariação de ativos, gestão de riscos), técnicas (segmentação de rede, autenticação multifator generalizada, gestão de vulnerabilidades) e humanas (planos de formação e sensibilização estruturados) — decorrentes do diagnóstico realizado no âmbito da adesão a projetos de cibersegurança regionais.

# 01 Palavras-passe fortes e gestão de credenciais


**Aplica-se a:** **Trabalhador** **Cidadão** **Entidade**

As credenciais de acesso são a primeira linha de defesa de qualquer conta ou sistema. Uma password fraca ou reutilizada é, ainda hoje, a causa mais comum de comprometimento de contas pessoais e profissionais.

- **Usar passwords fortes:** mínimo 12 caracteres, combinando maiúsculas, minúsculas, algarismos e caracteres especiais (ex.: Ante$1u0ueEu).
- **Evitar passwords óbvias:** sequências, nomes próprios, datas de nascimento ou palavras comuns (admin, 123456, qwerty).
- **Nunca reutilizar:** cada serviço deve ter uma password diferente; uma fuga de dados num site não deve comprometer todos os outros.
- **Alterar por defeito:** substituir sempre as credenciais de fábrica (admin/admin, user/user) em equipamentos e aplicações.
- **Usar um gestor de passwords:** Bitwarden, KeePass ou 1Password, entre outros — evitando os gestores integrados no browser ou no telemóvel.
- **Verificar exposições:** consultar periodicamente https://haveibeenpwned.com para confirmar se as credenciais já foram comprometidas.

**Nota**

• Para entidades (PME e Administração Pública), esta prática deve ser complementada por uma política formal de gestão de credenciais e por uma periodicidade máxima de renovação (ex.: 180 dias).

## 02 Autenticação multifator (MFA)


**Aplica-se a:** **Trabalhador** **Cidadão** **Entidade**

A autenticação multifator acrescenta uma segunda barreira de proteção, exigindo mais do que a password para validar a identidade. Mesmo que uma credencial seja roubada, o acesso continua protegido.

- **Ativar o MFA sempre que disponível:** em email, redes sociais, banca online e aplicações profissionais.
- **Escolher o mecanismo mais robusto possível:** aplicações de autenticação (Google/Microsoft Authenticator), reconhecimento facial ou impressão digital são preferíveis ao SMS.
- **Usar fornecedores de autenticação credíveis:** Cartão de Cidadão, Chave Móvel Digital, ou contas Google/Microsoft, quando aplicável.
- **Nas entidades:** tornar o MFA obrigatório para acessos remotos, correio eletrónico e sistemas críticos.

# 03 Reconhecer e evitar o phishing


**Aplica-se a:** **Trabalhador** **Cidadão** **Entidade**

O phishing é a técnica mais usada por cibercriminosos para enganar vítimas e obter palavras-passe, códigos MB WAY, dados bancários ou acesso a contas, fazendo-se passar por entidades de confiança (bancos, serviços públicos, empresas, conhecidos).

- **Email (phishing):** tentativas de roubo de credenciais e dados pessoais através de mensagens de correio eletrónico falsas.
- **SMS (smishing):** ex. falsos avisos de pagamento (EEM) ou de levantamento de encomendas nos CTT.
- **Voz (vishing):** chamadas fraudulentas, incluindo vozes clonadas por IA ("olá pai", "olá mãe") e engenharia social por telefone.
- **QR code (quishing):** códigos QR falsos, associados por exemplo a eventos, que redirecionam para sites maliciosos.

**Nota**

• Como se proteger: confirmar sempre o remetente antes de abrir links ou anexos; verificar o link antes de clicar; desconfiar de pedidos de dados pessoais ou financeiros — nenhuma instituição legítima os solicita por email ou SMS; desconfiar de mensagens urgentes ou "boas demais para ser verdade"; manter antivírus, anti-malware e firewall ativos. Exercício prático de treino: https://phishingquiz.withgoogle.com

## 04 Atualizações e antivírus sempre ativos


Aplica-se a: **Trabalhador** **Cidadão** **Entidade**

Grande parte dos ataques explora vulnerabilidades já conhecidas e corrigidas pelos fabricantes. Manter os sistemas atualizados fecha essas portas de entrada antes que sejam exploradas.

- **Atualizar sistema operativo e aplicações:** ativar atualizações automáticas sempre que possível, em computadores, telemóveis e outros dispositivos.
- **Manter antivírus e firewall ativos e atualizados:** tanto em equipamento pessoal como profissional.
- **Aplicar patches de segurança de imediato:** reduzindo a janela de tempo em que uma vulnerabilidade pode ser explorada.
- **Nas entidades:** definir um processo formal de gestão de atualizações e vulnerabilidades para servidores, postos de trabalho e equipamento de rede.

# 05 Cópias de segurança regulares — regra 3-2-1-1


Aplica-se a: **Trabalhador** **Cidadão** **Entidade**

Os dados vão falhar e as pessoas podem errar — o backup não é opcional, é essencial para a continuidade pessoal e do negócio. A referência internacional é a regra 3-2-1-1: 3 cópias dos dados, em 2 suportes diferentes, com 1 cópia fora do local (offsite) e 1 cópia imutável.

- **Centralizar:** guardar documentos importantes em repositórios seguros (ex.: OneDrive/SharePoint).
- **Regularidade:** fazer cópias de segurança com frequência definida (diária, semanal ou mensal, consoante a tolerância a perda de dados).
- **Diversificar suportes:** usar discos externos e USB apenas quando necessário, sempre encriptados, sem depender exclusivamente do armazenamento local.
- **Testar a recuperação:** verificar regularmente que os backups funcionam e podem ser restaurados.
- **Limitar o acesso:** restringir os backups a pessoal autorizado e definir uma política de retenção.

**Nota**

• Nas entidades, esta prática deve incluir um plano de continuidade de negócio para falhas técnicas e automatizar o processo com ferramentas dedicadas.

# 06 Proteção dos dispositivos


**Aplica-se a:** **Trabalhador** **Cidadão** **Entidade**

Computadores, telemóveis e tablets concentram grande parte da nossa vida digital e profissional. Protegê-los fisicamente é tão importante como protegê-los digitalmente.

- **Bloquear sempre:** ativar bloqueio automático e nunca deixar dispositivos desbloqueados sem vigilância.
- **Usar autenticação robusta:** PIN, password, impressão digital ou reconhecimento facial, com limite de tentativas falhadas.
- **Cobrir câmaras e desativar microfones:** sobretudo em portáteis e computadores fixos, quando não estão a ser usados.
- **Evitar olhares indiscretos:** usar filtros de privacidade em locais públicos e vigiar os dispositivos em viagem.
- **Controlar permissões:** não permitir que terceiros instalem aplicações ou acedam a contactos, câmara, microfone, armazenamento ou localização sem necessidade.

# 07 Redes seguras e uso de VPN


**Aplica-se a:** **Trabalhador** **Cidadão** **Entidade**

A rede é o caminho por onde circula toda a informação. Uma rede mal protegida expõe dados a interceção, mesmo que os restantes cuidados estejam a ser seguidos.

- **Evitar redes Wi-Fi públicas:** não aceder a informação sensível em redes abertas (cafés, aeroportos, espaços públicos).
- **Usar VPN:** ligar sempre através da VPN da organização quando disponível, sobretudo em teletrabalho ou deslocação.
- **Proteger a rede doméstica:** password forte e alterada com regularidade, cifra máxima (WPA2/WPA3) e nome de rede que não identifique o titular.
- **Navegar em sites seguros:** confirmar que o endereço usa HTTPS antes de introduzir dados.

**Nota**

• Nas entidades, a rede interna deve estar segmentada, isolando sistemas críticos do restante tráfego, com recurso a firewalls.

# 08 Encriptação de dados sensíveis


**Aplica-se a:** **Trabalhador** **Entidade**

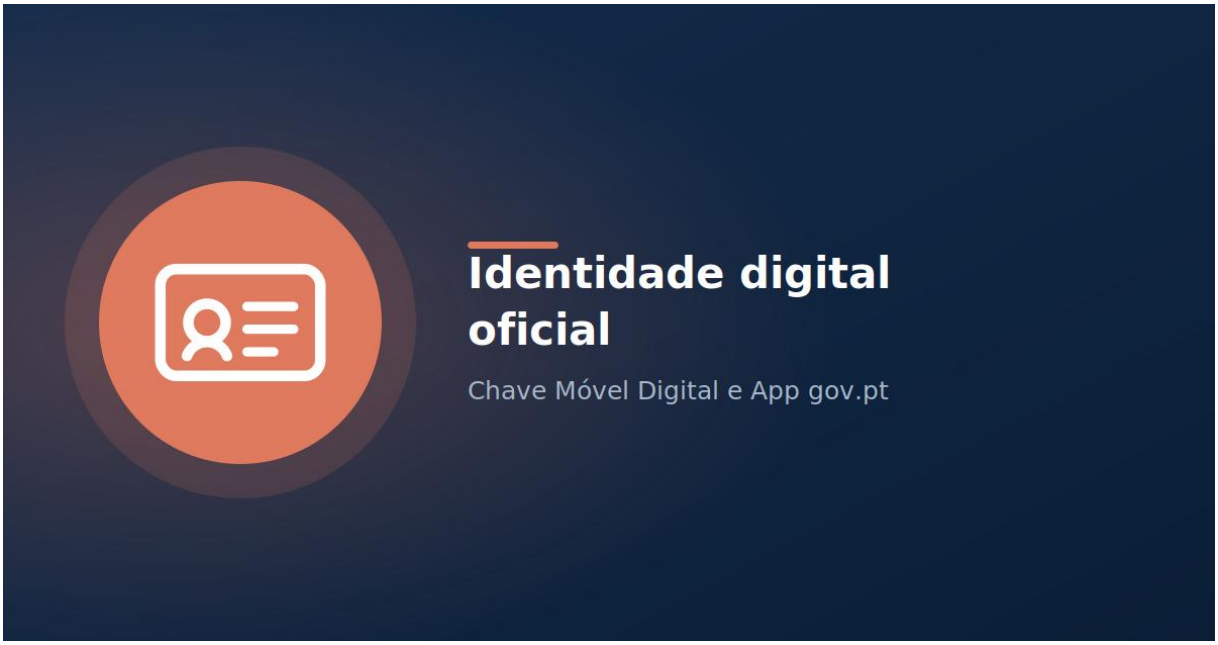
A cifra garante que, mesmo que um dispositivo seja perdido, roubado ou intercetado, a informação nele contida permanece ilegível a quem não tem autorização para a aceder — assegurando confidencialidade, autenticidade e integridade.

- **Encriptar discos e dispositivos:** usar uma ferramenta nativa de cifra de disco (ex.: BitLocker no Windows) em portáteis, discos externos e pens USB.
- **Encriptar comunicações e ficheiros sensíveis:** recorrer a ferramentas de cifra ponta-a-ponta (ex.: OpenPGP/Kleopatra) para email e documentos confidenciais.
- **Guardar a chave em local seguro:** conta associada ou ficheiro protegido, nunca junto do próprio dispositivo.

**Nota**

• Para as entidades, a encriptação é também um requisito de conformidade com quadros regulatórios como o RGPD e o NIS2.

# 09 Identidade digital oficial — Chave Móvel Digital e app gov.pt




**Aplica-se a:** **Cidadão** **Trabalhador** **Entidade**

A app gov.pt e a Carteira Digital de Identificação permitem autenticar, assinar e partilhar documentos de forma segura, substituindo fotocópias ou envios por email de documentos de identificação.

- **Carteira Digital:** adicionar documentos (Cartão de Cidadão, carta de condução, entre outros) e ativar a partilha segura por código QR, com validade temporária (1 hora, 1 dia, 1 semana ou 1 mês).
- **Autenticação em serviços públicos:** usar a Chave Móvel Digital para aceder e gerir processos próprios ou de dependentes.
- **Assinatura eletrónica:** mais segura do que a assinatura em papel, permite atribuir selos temporais e garantir que os documentos não foram alterados.
- **Atributos profissionais:** nas entidades, associar à assinatura eletrónica os atributos profissionais relevantes (ex.: diretor, gestor, responsável de cibersegurança), sem custos, através do site gov.pt.

# 10 Reportar incidentes e investir em formação contínua


**Aplica-se a:** **Trabalhador** **Cidadão** **Entidade**

Uma parte significativa dos incidentes de cibersegurança resulta de falhas comportamentais. A verdadeira força da cibersegurança reside na prevenção, não na reação — e a prevenção começa no conhecimento e na rapidez a reportar.

- **Reportar de imediato:** qualquer incidente ou suspeita deve ser comunicado sem demora à equipa de TI/cibersegurança da entidade (ou, para cidadãos, aos canais oficiais competentes).
- **Não tentar resolver sozinho:** ações isoladas podem destruir evidência necessária para a investigação e resposta ao incidente.
- **Formação contínua:** apostar na sensibilização de todos os utilizadores, através de plataformas como a NAU (nau.edu.pt), SeguraNet (seguranet.pt) e C-Academy do CNCS (c-academy.pt).
- **Consequências de não agir:** roubo de identidade e credenciais, fuga de dados pessoais, instalação de malware, extorsão, perdas financeiras e danos reputacionais — para pessoas, empresas e entidades públicas.

## Fontes e recursos complementares

- Centro Nacional de Cibersegurança (CNCS) — Boas Práticas: dyn.cncs.gov.pt/pt/boaspraticas
- CNCS — Cibersegurança em Teletrabalho: cncs.gov.pt/pt/ciberseguranca-em-teletrabalho
- CNCS — Recursos para o Cidadão: cncs.gov.pt/pt/cidadao
- CNCS — Recursos para Empresas: cncs.gov.pt/pt/empresas
- CNCS — Recursos para a Administração Pública: cncs.gov.pt/pt/administracao-publica
- CNCS / C-Academy — formação em cibersegurança: c-academy.pt
- Plataforma NAU — cursos abertos, incluindo “Cidadão Ciberseguro” e “Gestão de Riscos de Cibersegurança”: nau.edu.pt
- SeguraNet — literacia digital e segurança para escolas e famílias: seguranet.pt
- Verificação de exposição de credenciais: haveibeenpwned.com
- Exercício prático de deteção de phishing: phishingquiz.withgoogle.com
- Material interno de formação e sensibilização “Boas Práticas de Cibersegurança” (apresentação de suporte, setembro de 2026).