# POLÍTICA DE UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS

## PROJETO RGPD

Câmara de Lobos, 23 de abril de 2025.

| | |
|---|---|
| **Documento Ref.** | **P000004** |
| **Versão:** | **1** |
| **Data:** | **23/04/2026** |
| **Autor:** | **Equipa RGPD/Cibesegurança ebtorre** |
| **Proprietário:** | **Escola Básica dos 2.º e 3.º Ciclos da Torre** |

**Revisões - Histórico**

| Versão | Data | Autor da Revisão | Sumário das Alterações |
|---|---|---|---|
| | | | |
| | | | |

**Distribuição**

| Nome | Função |
|---|---|
| Hélder Miranda | Responsável Cibersegurança/Conselho Executivo |
| | |
| | |
| | |

**Aprovação**

| Nome | Cargo | Assinatura | Data |
|---|---|---|---|
| Hélder Miranda | Vice-Presidente<br>Conselho Executivo | Assinado por: **HÉLDER JOSÉ VIEIRA MIRANDA**<br>Num. de Identificação: 08154288<br>Data: 2026.04.29 09:54:15+01'00' | |

# Índice

# 0. INTRODUÇÃO

À medida que os dispositivos móveis se tornam menores e mais poderosos, aliado ao fato de um crescente número de tarefas poder ser alcançado fora das instalações da Organização, a sua utilização passa mais comumente a fazer parte da vida quotidiana.

Invariavelmente, à medida que as capacidades destes dispositivos aumentam, também aumentam os riscos a eles associados. Os controlos de segurança para este tipo de dispositivos são facilmente ignorados, potenciando os riscos associados à sua utilização.

São dispositivos móveis:

- computadores portáteis;
- *tablets*;
- telemóveis e equiparados;
- dispositivos de armazenamento móvel;
- outros.

O objetivo desta Política é definir os controlos de segurança em vigor na utilização de dispositivos móveis.

Destina-se a minimizar os seguintes riscos:

- perda, destruição, furto ou roubo de dispositivos móveis, incluindo danos;
- exposição de informações e dados ao público;
- introdução de *malware* e vírus nas redes internas;
- perda de reputação da Organização.

É extremamente importante que os controlos estabelecidos nesta política sejam cumpridos em todos os momentos, desde a utilização até ao transporte.

Esta política aplica-se a todos as pessoas, sistemas, processos e procedimentos que constituem os sistemas de informação.

# 1. POLÍTICA DE DISPOSITIVOS MÓVEIS

## Dispositivos móveis disponibilizados pela Escola Básica dos 2.º e 3.º Ciclos da Torre (EB23Torre)

- Devem ser utilizados dispositivos móveis disponibilizados pela EB23Torre no que diz respeito aos dados pertencentes à Organização.
- Os dispositivos móveis devem ser configurados de acordo com as Políticas da Organização, sendo o suporte prestado pela mesma, podendo aceder ao dispositivo para resolução de problemas e manutenção dos equipamentos.
- Deve garantir que o dispositivo é transportado de forma segura e não seja exposto a situações que possam provocar danos.
- Não é permitido deixar o dispositivo desacompanhado e/ou à vista do público.
- Não é permitida a remoção de qualquer marca de identificação do dispositivo.
- Não são permitidas ligações a *hardware* periférico, sem a aprovação prévia da EB23Torre.
- Certifique-se que o ecrã do computador ou tablet tem bloqueio automatizado e exige um código de acesso ou senha para o seu desbloqueio.
- Os dispositivos fornecidos não se destinam ao uso pessoal. Não devem partilhados com familiares ou amigos, nem para atividades do foro pessoal. Poderá ser necessária a devolução do dispositivo a qualquer momento e sempre que para tal lhe for solicitado para inspeção e auditoria.
- Não deve instalar nenhum tipo de software não autorizado, nem alterar a configuração do dispositivo, sem autorização prévia da EB23Torre.
- Caso o dispositivo seja dado como perdido, furtado, roubado ou destruído, o proprietário deve informar a Equipa de TIC/Cibersegurança, o mais rapidamente possível, fornecendo detalhes das circunstâncias da perda e da classificação das informações nele armazenadas. Pode ficar estabelecido o direito da EB23Torre a limpar remotamente o dispositivo (parcialmente, apenas a informação institucional, ou na totalidade), sempre que possível, como medida de segurança (pode envolver a eliminação de dados não institucionais, pertencentes ao proprietário, caso não seja possível a eliminação da informação exclusiva à organização).
- Caso o proprietário do dispositivo deixe de prestar os seus serviços, qualquer que seja o motivo, deve permitir que o dispositivo seja auditado e permitir que todos os dados e aplicativos relacionados com a EB23Torre sejam removidos.
- Os dispositivos não devem, tanto quanto possível, estar conectados a redes não corporativas.

# Utilização de dispositivos móveis pessoais

A democratização da utilização de dispositivos móveis tem alimentado o desejo, entre os trabalhadores e as Organizações, do uso de dispositivos pessoais para uso institucional. Esta prática é designada por "**B**ring **Y**our **O**wn **D**evice" (***BYOD***). Em certas circunstâncias, esta prática pode trazer maior flexibilidade e eliminar a necessidade do funcionário transportar mais do que um dispositivo regularmente.

O *BYOD* pode incorporar alguns desafios e problemas de segurança:

- uso do dispositivo por familiares e amigos;
- backups pré-definidos na nuvem;
- aumento da exposição a potenciais perdas, danos, furtos ou roubos;
- potencial acesso a sites que não respeitem a Política de Uso Aceitável da Organização;
- conexões a redes inseguras;
- inexistência de proteção antivírus;
- instalação de aplicativos potencialmente mal-intencionados.

Estas questões devem ser alvo de análise, deste modo, deve ser avaliada a adequação de qualquer dispositivo para conter dados específicos pertencentes à Organização.

Alguns passos importantes na utilização de dispositivos móveis pessoais no âmbito institucional:

- manter o sistema operativo e as aplicações atualizadas;
- ativar as atualizações automáticas ou verificar regularmente se há atualizações disponíveis;
- definir senhas fortes com combinação de letras, números e caracteres especiais para criar senhas seguras;
- usar o bloqueio do ecrã para evitar o acesso não autorizado;
- utilizar um software antivírus confiável para proteger o seu dispositivo contra malware, vírus e outras ameaças;
- realizar *backups* periódicos;
- para fazer *backup* das informações profissionais utilizar a nuvem *OneDrive* da sua conta profissional;
- evitar fazer o *download* e instalação de aplicações não confiáveis ou desconhecidas.