

POLÍTICA DE UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS

PROJETO RGPD

Data

Documento Ref.	RGPD-DOC-11-3
Versão:	1
Data:	
Autor:	
Proprietário:	

Revisões - Histórico

Versão	Data	Autor da Revisão	Sumário das Alterações

Distribuição

Nome	Função

Aprovação

Nome	Cargo	Assinatura	Data

Índice

0. INTRODUÇÃO	4
1. POLÍTICA DE DISPOSITIVOS MÓVEIS	5
Dispositivos móveis disponibilizados pela Escola Básica dos 2.º e 3.º Ciclos da Torre (eb23torre)	5
Utilização de dispositivos móveis pessoais	5

0. INTRODUÇÃO

À medida que os dispositivos móveis se tornam menores e mais poderosos, aliado ao fato de um crescente número de tarefas pode ser alcançado fora das instalações da organização, a utilização de dispositivos móveis faz parte da vida quotidiana.

No entanto, 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.

Destinam-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 todas 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 de 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 exclusivamente da 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 pelo uso de dispositivos pessoais para uso institucional. Esta prática é designada por “Bring Your Own Device” (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, ao avaliar 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.