					Insira aqui a designação da entidade jurídica registada							
Número do documento: P34					Título do documento: **Política de Dispositivos Móveis e BYOD**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Aplica controlos de segurança e requisitos de conformidade
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Fornece controlos detalhados para a gestão de dispositivos móveis
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Controlo de acesso, acesso remoto, configuração e requisitos de segurança para dispositivos móveis
RGPD da UE	5(1)(f), 25, 32	Requisitos obrigatórios de privacidade, cifragem de dados e segurança do tratamento
Diretiva NIS2 da UE	21(2)(d)	Medidas técnicas e organizativas de proteção para acesso móvel
DORA da UE	9, 10	Gestão do risco das TIC e requisitos de segurança para dispositivos móveis
COBIT 2019	APO13.02, DSS01.04, BAI09	Planos de segurança da informação, configuração de ativos e controlos para ambientes móveis

Finalidade

1. Finalidade

1.1 Esta política estabelece os requisitos de segurança, conformidade e operação aplicáveis à utilização de dispositivos móveis e de tecnologia pessoal no âmbito do Bring Your Own Device (BYOD), quando utilizados para aceder a sistemas, aplicações ou dados da organização.

1.2 Tem como objetivo assegurar a Confidencialidade, Integridade e Disponibilidade da informação da organização acedida ou tratada através de endpoints móveis, incluindo smartphones, tablets, computadores portáteis e dispositivos híbridos.

1.3 Esta política estabelece ainda os controlos técnicos e processuais necessários para mitigar riscos como fuga de dados, acesso não autorizado, perda ou furto de dispositivos e comprometimento de aplicações móveis.

1.4 Esta política suporta o cumprimento de requisitos regulamentares e contratuais, permitindo simultaneamente uma utilização móvel segura e produtiva por trabalhadores, prestadores de serviços e terceiros autorizados.

2. Âmbito

2.1 Esta política aplica-se a todo o pessoal, incluindo trabalhadores, contratados, estagiários e prestadores de serviços terceiros, que utilizem dispositivos móveis para aceder a dados, sistemas, aplicações ou plataformas de comunicação da organização.

2.2 Abrange todos os dispositivos de computação móvel, incluindo, entre outros:

2.2.1 Smartphones e tablets (iOS, Android, etc.)

2.2.2 Computadores portáteis e ultrabooks (Windows, macOS, Linux)

2.2.3 Dispositivos vestíveis e dispositivos inteligentes híbridos com capacidade de sincronização de dados

2.3 Aplica-se independentemente de o dispositivo ser propriedade da organização ou propriedade pessoal ao abrigo de um acordo BYOD.

2.4 A política abrange todos os vetores de acesso, incluindo VPN, ambientes de trabalho remotos, aplicações na cloud, correio eletrónico, plataformas de colaboração (por exemplo, SharePoint, Teams) e ferramentas de sincronização de ficheiros (por exemplo, OneDrive, Dropbox, quando autorizadas).

2.5 Inclui a utilização em regimes de trabalho remoto, em infraestruturas on-premises, em deslocação profissional ou em modelos de trabalho híbrido.

3. Objetivos

3.1 Reduzir o risco de comprometimento, fuga ou perda de dados decorrente da utilização insegura de dispositivos móveis.

3.2 Assegurar a aplicação consistente e exequível de controlos de segurança em todos os endpoints móveis, independentemente do modelo de propriedade (corporativo ou BYOD).

3.3 Garantir que a utilização de dispositivos móveis cumpre a ISO/IEC 27001 e outros referenciais regulamentares aplicáveis à privacidade, proteção de dados e cibersegurança.

3.4 Facilitar a integração segura dos dispositivos móveis nos fluxos de trabalho operacionais, de comunicação e de colaboração da organização.

3.5 Estabelecer responsabilidades e processos claramente definidos para a gestão de dispositivos móveis (MDM), incluindo registo, inscrição, apagamento remoto, cifragem, autenticação e monitorização.

3.6 Proteger os direitos de privacidade das pessoas que utilizam os seus próprios dispositivos, salvaguardando simultaneamente a informação sensível da organização.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO) / Responsável de Segurança de TI

4.1.1 Define a política e as normas técnicas aplicáveis à utilização de dispositivos móveis e BYOD.

4.1.2 Assegura a supervisão do cumprimento, da resposta a incidentes e da gestão de exceções relativas aos controlos de dispositivos móveis.

4.1.3 Coordena com as áreas Jurídica e de Recursos Humanos para assegurar que a aplicação da política é juridicamente adequada e alinhada com a organização.

4.2 Administrador de Tecnologias da Informação (TI) / Administrador de MDM

4.2.1 Gere o provisionamento de acessos, a inscrição e a configuração de dispositivos móveis através de soluções MDM.

4.2.2 Aplica controlos ao nível do dispositivo (por exemplo, cifragem, códigos PIN e controlos sobre aplicações).

4.2.3 Executa o apagamento remoto, o bloqueio do dispositivo e a revogação de acessos, quando necessário.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Requisitos de revisão e atualização

9.1 Esta política deve ser revista pelo menos anualmente pelo CISO ou pelo Responsável de Segurança da Informação designado, para assegurar alinhamento com:

9.1.1 Alterações nas plataformas de sistemas operativos móveis, nas tecnologias MDM ou nas normas de autenticação

9.1.2 Alterações regulamentares ou contratuais que afetem a proteção de dados móveis (por exemplo, RGPD da UE, DORA da UE, Diretiva NIS2 da UE)

9.1.3 Revisões dos conjuntos de controlos da ISO/IEC 27001:2022, ISO/IEC 27002:2022 ou NIST SP 800-53 Rev.5

9.1.4 Feedback proveniente de auditorias, análises pós-incidente ou comunicações de trabalhadores

9.2 Podem ser desencadeadas revisões intercalares por:

9.2.1 Incidentes de segurança que envolvam dispositivos móveis ou plataformas BYOD

9.2.2 Notificação do fornecedor sobre vulnerabilidades de alto risco em plataformas suportadas

9.2.3 Introdução de novas aplicações móveis ou plataformas de colaboração utilizadas nas operações do negócio

9.3 As atualizações da política devem ser:

9.3.1 Documentadas no histórico de versões da política

9.3.2 Comunicadas a todo o pessoal e aos contratados afetados

9.3.3 Reconfirmadas mediante confirmação da política atualizada por todos os utilizadores BYOD

9.4 Todas as revisões e alterações devem ser formalmente aprovadas pela direção de topo e registadas no Registo de Alterações à Política.

10. Políticas relacionadas e articulações

10.1 Esta política é interdependente de várias políticas-chave do quadro do SGSI da organização. Entre as principais articulações, incluem-se:

10.1.1 P1 – Política de Segurança da Informação: Estabelece os princípios gerais de governação para todos os controlos de segurança da informação, incluindo os relativos à utilização de dispositivos móveis.

10.1.2 P3 – Política de Utilização Aceitável: Define os comportamentos permitidos e as restrições relacionadas com a utilização de tecnologia, aplicáveis diretamente ao acesso móvel e BYOD.

10.1.3 P9 – Política de Trabalho Remoto: Define obrigações adicionais de segurança para ambientes de trabalho móvel, complementando os controlos específicos de mobilidade definidos nesta política.

10.1.4 P13 – Política de Classificação e Rotulagem da Informação: Determina a forma como os dados em dispositivos móveis devem ser tratados com base no respetivo nível de classificação, com impacto no armazenamento, transferência e aplicação da cifragem.

10.1.5 P22 – Política de Registo de Logs e Monitorização: Suporta a recolha e revisão de registos de acesso móvel para deteção de anomalias ou violações.

10.1.6 P30 – Política de Resposta a Incidentes: Define a forma como os incidentes relacionados com dispositivos móveis (por exemplo, perda de dispositivo, acesso não autorizado) são tratados e escalonados.

10.1.7 P33 – Política de Monitorização de Auditoria e Conformidade: Fornece a base para verificações periódicas do cumprimento dos requisitos de segurança móvel, incluindo a adesão à política de BYOD.

11. Normas e referenciais

11.1 Esta política está alinhada com referenciais de cibersegurança internacionalmente reconhecidos e com obrigações legais, de modo a assegurar a utilização segura de dispositivos móveis e de tecnologias pessoais (BYOD) em ambientes empresariais.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 5.10 – Utilização aceitável da informação e dos ativos: Exige controlos para a utilização responsável dos ativos corporativos, incluindo dispositivos móveis.

11.2.2 Cláusula 5.11 – Trabalho remoto: Estabelece práticas seguras para o acesso a sistemas a partir de fora das instalações da organização.

11.2.3 Cláusula 5.12 – Utilização de dispositivos móveis: Exige controlos baseados no risco para endpoints móveis e configurações BYOD.

11.2.4 Cláusula 5.13 – Transferência de informação: Exige a proteção da informação transferida através de canais móveis.

11.3 ISO/IEC 27002:2022 – Controlos 5.10 a 5.13:

11.3.1 Os controlos do Anexo A 5.10 a 5.13 especificam como o acesso móvel, a cifragem, a monitorização e a mitigação de perdas devem ser aplicados no âmbito de um Sistema de Gestão da Segurança da Informação (SGSI). Estes controlos fornecem orientações detalhadas de implementação para proteger endpoints móveis, impor a contentorização, monitorizar a integridade dos dispositivos e assegurar configurações BYOD com consideração pela privacidade.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Controlo de acesso para dispositivos móveis: Define proteções de base, incluindo cifragem, autenticação e aplicação de MDM.

11.4.2 AC-17 – Acesso remoto: Exige autenticação segura e proteções de sessão para utilizadores móveis remotos.

11.4.3 CM-7 – Funcionalidade mínima: Suporta a remoção de aplicações e funcionalidades desnecessárias dos endpoints móveis para reduzir o risco.

11.4.4 MP-5 – Proteção no transporte de suportes: Estabelece a transmissão segura de dados de sistemas móveis para destinos externos ou para a cloud.

11.4.5 SC-12 – Estabelecimento de chaves criptográficas: Exige a utilização de protocolos criptográficos seguros para comunicação e armazenamento móvel.

11.5 RGPD da UE (2016/679):

11.5.1 Artigo 5(1)(f) – Integridade e confidencialidade: Exige que as organizações protejam os dados pessoais em dispositivos móveis contra acesso não autorizado ou ilícito.

11.5.2 Artigo 25 – Proteção de Dados desde a Conceção e por Defeito: Exige que a privacidade esteja incorporada nos processos de BYOD e MDM.

11.5.3 Artigo 32 – Segurança do tratamento: Exige controlos baseados no risco (por exemplo, cifragem, autenticação, controlo de acesso) para dados pessoais em plataformas móveis.

11.6 Diretiva NIS2 da UE (2022/2555):

11.6.1 Artigo 21(2)(d): Exige que o acesso móvel a sistemas e informação críticos seja protegido através de medidas técnicas e organizativas adequadas, tais como controlo de endpoints, cifragem e monitorização.

11.7 DORA da UE (2022/2554):

11.7.1 Artigo 9 – Quadro de Gestão do Risco das TIC: Exige que as entidades do setor financeiro mitiguem os riscos do acesso móvel e remoto como parte da resiliência operacional.

11.7.2 Artigo 10 – Requisitos de segurança dos sistemas TIC: Exige arquitetura móvel segura, mecanismos de monitorização e capacidades de resposta a ameaças cibernéticas originadas em dispositivos móveis.

11.8 COBIT 2019:

11.8.1 APO13.02 – Estabelecer e manter um plano de segurança da informação: Exige que a utilização de dispositivos móveis, incluindo BYOD, seja integrada nas estratégias de segurança da organização.

11.8.2 DSS01.04 – Gerir a configuração e a integridade de ativos: Aplica-se ao controlo da configuração e à implementação segura de dispositivos móveis.

11.8.3 BAI09.01 – Estabelecer e manter controlos: Suporta a implementação de salvaguardas técnicas e processuais para operações móveis e remotas seguras.