					Insira aqui a designação da entidade jurídica registada							
Número do documento: P35S					Título do documento: **Política de Segurança da Internet das Coisas (IoT) / Tecnologia Operacional (OT)**							
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**

Alinhada com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controlos 5.23, 5	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
RGPD da UE	Artigo 32	
Diretiva NIS2 da UE	Artigo 21(2)(a), (d), (f)	
DORA da UE	Artigo 9(2), 10(1)	

1. Finalidade

1.1. A presente política estabelece as regras obrigatórias para a utilização e gestão seguras de dispositivos de Internet das Coisas (IoT) e de Tecnologia Operacional (OT) na organização. Estes dispositivos podem incluir sensores inteligentes, câmaras de segurança, máquinas de produção, controladores de AVAC ou quaisquer sistemas industriais ligados à rede.

1.2. A finalidade desta política é:

1.2.1. Proteger as operações físicas e digitais contra interrupções ou manipulação através de dispositivos conectados insuficientemente protegidos

1.2.2. Assegurar a implementação, monitorização e manutenção seguras de sistemas de IoT e OT

1.2.3. Assegurar o cumprimento da ISO/IEC 27001:2022, da Diretiva NIS2 da UE e de referenciais regulatórios relacionados

1.2.4. Estabelecer controlos práticos e aplicáveis para PME que operam em ambientes de escritório, armazém ou produção

2. Âmbito

2.1. Esta política aplica-se a todas as pessoas envolvidas no planeamento, instalação, configuração, utilização, suporte ou eliminação de dispositivos de IoT ou OT. Isto inclui:

2.1.1. Trabalhadores, prestadores de serviços ou estagiários com acesso físico ou remoto aos dispositivos

2.1.2. Fornecedores terceiros ou técnicos de assistência que instalem ou mantenham sistemas conectados

2.1.3. Diretores-gerais ou colaboradores responsáveis pela supervisão das políticas de segurança

2.2. A política abrange:

2.2.1. Dispositivos IoT, tais como fechaduras inteligentes, sistemas de videovigilância, contadores inteligentes ou impressoras

2.2.2. Sistemas de OT, incluindo PLC (controladores lógicos programáveis), painéis SCADA ou gateways industriais

2.2.3. Hardware de suporte, aplicações de gestão e redes de comunicação utilizadas por estes sistemas

2.3. Esta política aplica-se em todos os locais de trabalho: ambientes de escritório, instalações remotas, áreas de produção e plataformas na cloud com interface com estes dispositivos.

3. Objetivos

3.1. Implementação segura: assegurar que todos os sistemas de IoT/OT são configurados de forma segura antes de serem colocados em exploração.

3.2. Limitação da exposição: prevenir o acesso não autorizado, a utilização indevida ou a tomada de controlo de dispositivos conectados através da aplicação de controlos de acesso robustos e de segmentação de rede.

3.3. Monitorização contínua: manter visibilidade sobre as operações de IoT/OT através do registo de atividades e da monitorização de comportamentos anómalos.

3.4. Responsabilização dos fornecedores: assegurar que os prestadores terceiros seguem práticas seguras de instalação, configuração e manutenção.

3.5. Cumprimento regulamentar: demonstrar alinhamento integral com as normas aplicáveis, tais como a ISO/IEC 27001, o RGPD da UE (caso sejam recolhidos dados pessoais) e a Diretiva NIS2 da UE para a resiliência de infraestruturas críticas.

4. Papéis e responsabilidades

4.1. Diretor-Geral (GM)

4.1.1. Detém a responsabilidade global pela segurança dos sistemas de IoT e OT

4.1.2. Aprova a presente política e assegura a sua aplicação em todas as áreas de trabalho

4.1.3. Verifica que os fornecedores e prestadores de serviços seguem práticas seguras de configuração inicial e manutenção

4.1.4. Autoriza o acesso à rede para qualquer sistema de IoT/OT

4.2. Colaborador designado ou Gestor de Operações (quando aplicável)

4.2.1. Supervisiona o inventário, a localização e a configuração dos dispositivos de IoT/OT

4.2.2. Regista a localização de cada dispositivo, a respetiva afetação à rede e a documentação de suporte

4.2.3. Assegura que quaisquer alterações (por exemplo, atualizações de firmware ou substituições de dispositivos) são documentadas

[... 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. Revisão anual

9.1.1. Esta política deve ser revista pelo menos uma vez por ano pelo GM

9.1.2. A revisão deve avaliar se a política continua eficaz, se abrange os tipos de dispositivos em utilização e se está alinhada com novos riscos ou tecnologias

9.2. Atualizações desencadeadas por eventos

9.2.1. As atualizações da política devem também ser iniciadas quando:

9.2.2. Forem introduzidos novos tipos de sistemas de IoT ou OT

9.2.3. Os fornecedores emitirem avisos de segurança ou notificações de fim de vida útil

9.2.4. Um incidente ou auditoria identificar lacunas nos controlos de IoT/OT

9.2.5. Novas leis ou normas impuserem requisitos adicionais

9.3. Documentação e controlo de versões

9.3.1. Todas as atualizações devem ser documentadas, incluindo a data, o número da versão e o resumo das alterações

9.3.2. O GM deve manter o histórico das versões da política para efeitos de auditoria

9.4. Comunicação de alterações

9.4.1. Quaisquer atualizações à política devem ser comunicadas a todos os colaboradores e fornecedores relevantes

9.4.2. As versões atualizadas devem estar acessíveis através de unidades partilhadas ou de materiais impressos nos locais de instalação ou centros de controlo

10. Políticas relacionadas e ligações

10.1. Esta política deve ser implementada em alinhamento com as seguintes políticas PME relacionadas:

10.1.1. P4S – Política de Controlo de Acesso: aplica controlos de autenticação ao nível do dispositivo, utilização de palavras-passe robustas e procedimentos de acesso autorizado para plataformas de IoT e OT

10.1.2. P9S – Política de Trabalho Remoto: impede a utilização de acesso remoto a painéis de IoT/OT através de canais inseguros ou não aprovados

10.1.3. P17S – Política de Proteção de Dados e Privacidade: aplica-se quando dispositivos IoT (por exemplo, câmaras de segurança) tratam ou gravam dados pessoais, assegurando o cumprimento do RGPD da UE

10.1.4. P30S – Política de Resposta a Incidentes: define procedimentos para deteção, comunicação e resolução de incidentes de IoT ou OT, incluindo suspeitas de adulteração ou falha operacional

10.1.5. P36S – Política de Redes Sociais e Comunicações Externas: assegura que nenhuma informação sobre dispositivos ou arquitetura de rede é partilhada externamente sem aprovação

10.2. Cada política relacionada reforça a aplicação e a utilização prática desta política através de orientação procedimental específica.

11. Normas e referenciais de referência

11.1. ISO/IEC 27001

11.1.1. Cláusula 6.1 – Identificação de riscos e tratamento de riscos: exige que os riscos relacionados com sistemas de IoT e OT sejam avaliados e mitigados de forma sistemática

11.1.2. Cláusula 8.1 – Planeamento e controlo operacional: assegura controlo operacional seguro sobre dispositivos conectados

11.2. ISO/IEC 27002

11.2.1. Controlo 5.23 – Segurança da informação na utilização de Tecnologia Operacional: define a utilização segura de OT em ambientes físicos e digitais

11.2.2. Controlo 5.31 – Configuração segura de sistemas de informação: exige configurações seguras para dispositivos de IoT/OT e a não utilização de predefinições inseguras

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Integridade de software, firmware e informação: exige validação da integridade do firmware e das atualizações

11.3.2. CM-7 – Funcionalidade mínima: os dispositivos não devem ter funcionalidades não utilizadas ou inseguras ativadas

11.3.3. AC-6 – Menor privilégio: o acesso aos dispositivos deve estar limitado apenas a utilizadores autorizados

11.3.4. PE-20 – Monitorização de ativos: monitorização física e operacional de ativos de IoT e OT

11.3.5. SC-7 – Proteção de perímetro: segmentação e controlo das comunicações de rede para sistemas conectados

11.4. RGPD da UE (2016/679)

11.4.1. Artigo 32 – Segurança do tratamento: se forem captados dados pessoais (por exemplo, através de câmaras de vigilância), a organização deve implementar medidas técnicas e organizativas adequadas para proteger esse tratamento

11.5. Diretiva NIS2 da UE (2022/2555)

11.5.1. Artigo 21(2)(a) – Medidas de gestão de riscos

11.5.2. Artigo 21(2)(d) – Configuração e utilização seguras de dispositivos

11.5.3. Artigo 21(2)(f) – Segurança da cadeia de fornecimento e dos sistemas

11.6. DORA da UE (2022/2554)

11.6.1. Artigo 9(2) – Âmbito da gestão do risco das TIC: inclui dispositivos industriais e incorporados utilizados em ambientes operacionais

11.6.2. Artigo 10(1) – Continuidade das TIC: exige que as configurações dos dispositivos suportem a resiliência e as operações de recuperação

11.7. COBIT 2019

11.7.1. DSS01 – Gerir operações: aplica-se à supervisão das operações tecnológicas, incluindo dispositivos físicos

11.7.2. DSS05 – Gerir serviços de segurança: assegura que os sistemas conectados são adequadamente monitorizados e protegidos

11.7.3. APO13 – Gerir segurança: reforça políticas de proteção de ativos operacionais em PME