					Insira aqui a designação da entidade jurídica registada							
Número do documento: P35					Título do documento: **Política de Segurança de IoT / 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**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	
ISO/IEC 27002:2022	Controlos 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
RGPD da UE	Artigos 5, 25, 32	
Diretiva NIS2 da UE	Artigos 21, 23	
DORA da UE	Artigos 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Objetivo

1.1 A presente política estabelece os requisitos obrigatórios de segurança da informação para a implementação, operação, monitorização e desativação de sistemas de Internet das Coisas (IoT) e de Tecnologia Operacional (OT) na organização.

1.2 Garante que estes sistemas são integrados no sistema de gestão de cibersegurança mais abrangente da organização e protegidos contra comprometimento, uso indevido ou sabotagem operacional.

1.3 A política visa impor controlos técnicos, organizacionais e processuais robustos para proteger sistemas IoT/OT que interagem com infraestruturas físicas, processos de produção e ambientes críticos para a segurança.

1.4 Dá suporte às obrigações regulatórias e contratuais em matéria de cibersegurança, segurança, controlo ambiental e continuidade.

2. Âmbito

2.1 Esta política aplica-se a todos os sistemas IoT e OT — quer sejam propriedade da organização, alugados ou fornecidos por terceiros — utilizados nos ambientes operacionais, administrativos ou de produção da organização.

2.2 Os sistemas abrangidos incluem, entre outros:

2.2.1 Dispositivos IoT, tais como sensores ambientais, sistemas de controlo de acessos, iluminação inteligente, equipamentos de videovigilância e dispositivos vestíveis

2.2.2 Plataformas de tecnologia operacional, tais como PLC, sistemas de supervisão, controlo e aquisição de dados (SCADA), sistemas de controlo distribuído (DCS), painéis de interface homem-máquina (IHM), interfaces do sistema de execução da produção (MES) e controladores de campo

2.2.3 Redes de controlo industrial ou ativos ligados à nuvem que monitorizam operações físicas

2.3 A política abrange:

2.3.1 Todos os ambientes (on-premises, edge e cloud gerida)

2.3.2 Todas as partes interessadas (utilizadores internos, integradores, fornecedores terceiros, contratados)

2.3.3 Todas as fases do ciclo de vida (conceção, aquisição, implementação, operação e desativação)

3. Objetivos

3.1 Proteger a infraestrutura de IoT e OT contra ameaças internas e externas de cibersegurança, incluindo negação de serviço, acessos não autorizados, propagação de ransomware e adulteração de firmware.

3.2 Garantir que as plataformas IoT/OT não se tornam vetores de ataque de ligação entre TI e OT nem comprometem sistemas críticos para a segurança.

3.3 Aplicar os princípios de segurança desde a conceção e de defesa em profundidade ao longo do ciclo de vida destas tecnologias.

3.4 Permitir a integração fiável, segura e auditável das plataformas IoT e OT no Centro de Operações de Segurança (SOC) da organização e nos planos de resposta a incidentes.

3.5 Assegurar que todas as implementações estão alinhadas com os controlos da ISO/IEC 27001 e com as orientações setoriais aplicáveis (por exemplo, IEC 62443, ISO 27019, NIST SP 800-82).

4. Papéis e responsabilidades

4.1 Chief Information Security Officer (CISO) / Responsável de Segurança da Informação

4.1.1 Define políticas e normas técnicas para a cibersegurança de IoT/OT

4.1.2 Supervisiona as avaliações de risco, a validação de controlos e a coordenação interdepartamental

4.2 Engenheiros de OT / Gestores de Instalações e de Produção

4.2.1 Validam as configurações dos sistemas OT e asseguram o cumprimento da política nas áreas de produção

4.2.2 Mantêm salvaguardas físicas e lógicas para a integridade e segurança dos sistemas OT

[... 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 e atualizada com base em:

9.1.1 Alterações na arquitetura, nos fornecedores ou nas plataformas dos sistemas OT ou IoT

9.1.2 Atualizações regulatórias relevantes (por exemplo, revisões da DORA da UE, da Diretiva NIS2 da UE ou de diretivas setoriais)

9.1.3 Surgimento de novas vulnerabilidades ou padrões de ameaça em sistemas de controlo

9.1.4 Constatações de auditorias internas ou externas, testes de penetração ou exercícios de red team

9.2 O CISO, o Responsável de Segurança de OT e os responsáveis dos departamentos relevantes são responsáveis por iniciar conjuntamente o processo de revisão.

9.3 Devem ser desencadeadas revisões intercalares após:

9.3.1 Qualquer incidente relacionado com IoT/OT que resulte em falha do sistema ou perda de dados

9.3.2 Introdução de novos equipamentos de elevado impacto, software de monitorização ou plataformas de firmware

9.3.3 Integração de computação inteligente de edge ou automatização reforçada por IA ao nível operacional

9.4 Todas as alterações às políticas devem ser:

9.4.1 Documentadas no histórico de versões e no registo de alterações à política

9.4.2 Comunicadas a todos os utilizadores, fornecedores e operadores de TI/OT afetados

9.4.3 Novamente aprovadas pela direção de topo

10. Políticas relacionadas e articulações

10.1 Esta política funciona em articulação com as seguintes políticas de segurança da informação e é suportada por elas:

10.1.1 P1 – Política de Segurança da Informação: Estabelece princípios fundamentais de segurança que se estendem à segurança dos sistemas IoT e OT.

10.1.2 P3 – Política de Utilização Aceitável: Define restrições à utilização pessoal e não autorizada de dispositivos, incluindo em ambientes operacionais.

10.1.3 P6 – Política de Gestão de Riscos: Orienta a avaliação, aceitação e mitigação de riscos relacionados com sistemas embebidos e de controlo.

10.1.4 P12 – Política de Gestão de Ativos: Assegura que todos os sistemas IoT e OT são formalmente inventariados e têm proprietários responsáveis atribuídos.

10.1.5 P20 – Política de Proteção de Endpoints / Malware: Aplica-se a controladores ligados, gateways inteligentes e sistemas de edge em produção.

10.1.6 P22 – Política de Registo e Monitorização: Estende-se aos procedimentos de recolha e revisão de logs para ambientes OT.

10.1.7 P30 – Política de Resposta a Incidentes: Rege diretamente a forma como violações, anomalias ou falhas de sistema de IoT/OT devem ser escalonadas e geridas.

10.1.8 P33 – Política de Monitorização de Auditoria e Conformidade: Fornece mecanismos de garantia para validar o cumprimento contínuo desta política.

11. Normas e quadros de referência

11.1 Esta política está alinhada com normas internacionalmente reconhecidas e quadros regulatórios que asseguram a segurança, resiliência e conformidade dos sistemas de Internet das Coisas (IoT) e de Tecnologia Operacional (OT) em ambientes industriais, de produção e empresariais.

11.2 ISO/IEC 27002:2022 – Controlos 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Controlo 5.7 – Informações sobre ameaças: Apoia a monitorização de ambientes OT e a identificação de vulnerabilidades específicas de IoT.

11.2.2 Controlo 5.23 – Segurança da informação na utilização de serviços em cloud: Aplica-se quando dispositivos IoT interagem com plataformas na nuvem para telemetria, controlo ou análise.

11.2.3 Controlo 5.27 – Arquitetura segura de sistemas e princípios de engenharia: Rege os princípios de segurança desde a conceção para sistemas embebidos e redes de controlo.

11.2.4 Controlo 5.31 – Segurança nos processos de desenvolvimento e suporte: Impõe validação de software/firmware, controlos de patches e requisitos para fornecedores em implementações OT.

11.2.5 Controlo 5.36 – Cumprimento de requisitos legais e contratuais: Assegura o cumprimento, pelos ativos OT, de obrigações em matéria de segurança, ambiente e regulação.

11.2.6 Estes controlos estabelecem, em conjunto, melhores práticas da indústria para proteger sistemas IoT/OT ao longo do respetivo ciclo de vida, incluindo conceção da arquitetura, implementação segura, aplicação de patches, deteção de anomalias e cumprimento de requisitos setoriais.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Proteção de perímetro: Assegura que as redes OT são segmentadas e protegidas contra acessos não autorizados.

11.3.2 SI-4 – Monitorização do sistema: Exige a implementação de mecanismos contínuos de monitorização e deteção de anomalias em ambientes ICS.

11.3.3 CM-2 – Configuração de referência: Determina o controlo da configuração e o endurecimento de dispositivos das plataformas IoT/OT.

11.3.4 AC-6 – Menor privilégio: Aplica-se ao acesso de utilizadores e à assistência remota por fornecedores em sistemas de controlo embebidos.

11.3.5 PL-8 – Arquiteturas de segurança e privacidade: Rege o planeamento da integração segura de sistemas, especialmente em projetos de modernização de OT.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 5 – Princípios relativos ao tratamento de dados pessoais: Aplica-se a plataformas IoT que tratam dados baseados em sensores ou dados comportamentais associados a indivíduos.

11.4.2 Artigo 25 – Proteção de dados desde a conceção e por defeito: Exige salvaguardas de privacidade incorporadas na conceção do produto IoT e no firmware.

11.4.3 Artigo 32 – Segurança do tratamento: Impõe cifragem, controlo de acesso e comunicações seguras para transmissões de dados de dispositivos inteligentes.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigos 21 e 23: Impõem obrigações de segurança às entidades essenciais e importantes que utilizam sistemas OT. Estas incluem avaliação de riscos, notificação de incidentes e validação da cadeia de fornecimento de fornecedores IoT/OT e da integridade do firmware.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 9 – Gestão do risco das TIC: Exige a integração segura de sistemas embebidos e tecnologias OT no programa de governação do risco das TIC.

11.6.2 Artigo 10 – Requisitos de segurança das TIC: Determina medidas de proteção para plataformas OT interligadas utilizadas em ambientes financeiros e de serviços críticos.

11.7 COBIT 2019

11.7.1 DSS05.01 – Proteger contra malware: Inclui deteção e resposta a ameaças específicas de ICS e campanhas de malware dirigidas a IoT.

11.7.2 BAI09.01 – Estabelecer e manter requisitos de segurança: Corresponde ao provisionamento e à operação seguros de infraestruturas inteligentes ou embebidas.

11.7.3 APO13.02 – Estabelecer e manter um plano de segurança da informação: Exige a inclusão dos sistemas OT e das respetivas vulnerabilidades na estratégia de cibersegurança de toda a organização.