					Insira aqui a designação da entidade jurídica registada							
Número do documento: P09					Título do documento: **Política de Trabalho Remoto**							
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**

1. Finalidade

1.1 Esta política define os requisitos obrigatórios para a realização segura de trabalho remoto, incluindo a utilização dos sistemas da organização, o acesso a dados e o desempenho de funções fora das instalações corporativas.

1.2 Assegura a Confidencialidade, Integridade e Disponibilidade dos ativos de informação acedidos remotamente e estabelece controlos para mitigar os riscos associados a ambientes de trabalho distribuídos.

1.3 Esta política dá cumprimento ao Controlo 6.7 do Anexo A da ISO/IEC 27001:2022, através da implementação de salvaguardas técnicas e processuais adaptadas às condições de trabalho remoto.

2. Âmbito

2.1 Esta política aplica-se a todo o pessoal autorizado a trabalhar remotamente, incluindo:

2.1.1 Colaboradores (a tempo inteiro, a tempo parcial e contratados)

2.1.2 Prestadores externos de serviços, consultores e fornecedores

2.1.3 Trabalhadores temporários e pessoal afeto a projetos com acesso remoto aprovado (VPN, gestão de dispositivos móveis)

2.2 Abrange:

2.2.1 O acesso a sistemas da organização através de VPN ou de ferramentas de acesso remoto aprovadas

2.2.2 O tratamento de informação sensível e sujeita a regulamentação fora de instalações seguras

2.2.3 A utilização de equipamentos propriedade da organização ou em regime Traga o Seu Próprio Dispositivo (BYOD)

2.2.4 As proteções físicas e lógicas em ambientes remotos

2.3 Esta política aplica-se a todas as geografias e fusos horários em que a organização permita trabalho remoto, de forma regular, pontual ou no contexto de eventos de continuidade do negócio.

3. Objetivos

3.1 Assegurar que apenas indivíduos autorizados possam aceder remotamente a sistemas internos e a informação.

3.2 Impor cifragem, autenticação multifator e proteção de endpoint em todos os canais de acesso remoto.

3.3 Manter uma postura de segurança robusta face a ameaças como phishing, malware, exfiltração de dados e exposição não autorizada de sistemas.

3.4 Estabelecer regras para a transmissão, o armazenamento ou a impressão de dados sensíveis em ambientes fora das instalações.

3.5 Integrar medidas de segurança física que reduzam a visibilidade e a observação não autorizada durante sessões remotas.

3.6 Cumprir os requisitos regulamentares internacionais aplicáveis ao acesso remoto a dados, incluindo o RGPD, a NIS2 e a DORA.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova esta política, assegura a disponibilização dos recursos necessários e garante a sua integração nas operações de Recursos Humanos, TI e Segurança da Informação.

4.1.2 Autoriza os critérios de elegibilidade para trabalho remoto e a respetiva aplicabilidade por unidade de negócio.

4.2 Diretor de Segurança da Informação / Gestor do SGSI

4.2.1 É responsável por esta política, assegura a sua manutenção e o seu alinhamento com a postura de risco e com os requisitos regulamentares.

4.2.2 Define os controlos de segurança para o acesso remoto (por exemplo, cifragem, proteção de endpoint e tempos limite de sessão).

4.2.3 Aprova o tratamento de exceções e monitoriza a eficácia dos controlos.

[... 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 Frequência de revisão

9.1.1 Esta política deve ser revista anualmente, ou com maior frequência em caso de:

9.1.1.1 Introdução de novas tecnologias de acesso remoto

9.1.1.2 Expansão significativa do trabalho remoto (por exemplo, iniciativas de força de trabalho híbrida)

9.1.1.3 Surgimento de novas ameaças, vulnerabilidades ou incidentes associados a ambientes remotos

9.1.1.4 Alterações aos quadros legais ou regulamentares aplicáveis

9.2 Titularidade e processo de revisão

9.2.1 O responsável pela política é o Diretor de Segurança da Informação. A revisão deve ser coordenada com:

9.2.1.1 Operações e arquitetura de TI

9.2.1.2 Recursos Humanos e Gestão de instalações e ativos (para implicações operacionais e do espaço de trabalho)

9.2.1.3 Encarregado da Proteção de Dados (para controlos de privacidade e dados transfronteiriços)

9.2.2 As atualizações da política devem:

9.2.2.1 Ser aprovadas pelo Comité de Direção do SGSI

9.2.2.2 Ser comunicadas a todo o pessoal e prestadores de serviços afetados

9.2.2.3 Ser integradas nos materiais de integração e de formação de reciclagem

9.3 Controlo documental e distribuição

9.3.1 A política deve incluir controlo de versões, data de entrada em vigor e histórico de alterações.

9.3.2 As versões substituídas devem ser retidas de acordo com a Política de Gestão Documental (P14).

9.3.3 As versões revistas devem desencadear nova confirmação obrigatória para os utilizadores elegíveis para trabalho remoto.

10. Políticas relacionadas e ligações

10.1 Esta política funciona em articulação com:

10.1.1 P1 – Política de Segurança da Informação: Estabelece a linha de base para o tratamento seguro de ativos, aplicável a todos os ambientes de trabalho, incluindo os remotos.

10.1.2 P3 – Política de Utilização Aceitável: Regula a utilização adequada de dispositivos e sistemas da organização durante sessões de trabalho remoto.

10.1.3 P4 – Política de Controlo de Acessos: Assegura que os privilégios de acesso remoto seguem o princípio do menor privilégio e mecanismos de autenticação adequados.

10.1.4 P6 – Política de Gestão de Riscos: Define como os riscos do trabalho remoto são identificados, tratados e monitorizados no âmbito do SGSI.

10.1.5 P12 – Política de Gestão de Ativos: Exige inventário e gestão da configuração para todos os dispositivos utilizados remotamente.

10.1.6 P22 – Política de Registo e Monitorização: Assegura que as sessões remotas são monitorizadas, auditadas e retidas de acordo com os requisitos de conformidade.

10.1.7 P14 – Política de Retenção e Eliminação de Dados: Define regras de tratamento de dados relevantes para o trabalho remoto, incluindo suportes amovíveis e eliminação de dispositivos.

10.2 Estas políticas, em conjunto, asseguram que o trabalho remoto é seguro, conforme e passível de aplicação em todas as funções e geografias.

11. Normas e quadros de referência

11.1 Esta política está alinhada com quadros de segurança, proteção de dados e gestão do risco das TIC internacionalmente reconhecidos, para assegurar práticas de trabalho remoto seguras, rastreáveis e conformes.

11.2 ISO/IEC 27001

11.2.1 Cláusula 6.1.3 – Planeamento do tratamento de riscos: Esta política contribui para o tratamento dos riscos associados ao acesso remoto e a ambientes de trabalho distribuídos.

11.2.2 Cláusula 8.1 – Planeamento e controlo operacional: Exige a implementação de controlos para sistemas acedidos fora das instalações da organização.

11.2.3 Controlo 6.7 do Anexo A – Trabalho remoto: Esta política dá resposta integral aos controlos exigidos para a segurança da informação quando o pessoal trabalha fora das instalações da organização, incluindo proteções físicas e lógicas, governação de acessos e monitorização do comportamento dos utilizadores.

11.3 ISO/IEC 27002:2022 – Controlo 6

11.3.1 Este controlo exige salvaguardas processuais e técnicas para trabalho remoto. Inclui requisitos para segurança dos dispositivos, métodos de acesso, tratamento de dados, salvaguardas ambientais e gestão de terceiros, todos aplicados por esta política.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Acesso Remoto): Suportado diretamente através de controlos de VPN, MFA, registo de sessões e autorização de acesso baseada em funções para utilizadores remotos.

11.4.2 AC-2 (Gestão de Contas): Controla a elegibilidade de acesso, a atribuição de privilégios remotos e a desativação de contas.

11.4.3 SC-12 a SC-13 (Proteção Criptográfica, Estabelecimento de Chaves Criptográficas): Implementados através da utilização obrigatória de VPN e cifragem integral de disco para endpoints remotos.

11.4.4 MP-5 (Proteção no Transporte de Suportes) e PE-18 (Localização de Componentes do Sistema de Informação): As orientações para trabalho remoto exigem proteção no transporte e salvaguardas físicas em ambientes fora das instalações.

11.4.5 AU-2, AU-6: O registo e a monitorização de sessões remotas suportam os requisitos de auditoria e de resposta a incidentes.

11.5 RGPD da UE (2016/679)

11.5.1 Artigo 32 – Segurança do Tratamento: Esta política aplica os controlos de segurança de acesso remoto, cifragem e registo necessários para proteger os dados pessoais acedidos ou tratados remotamente.

11.5.2 Artigo 5(1)(f): Assegura que os dados pessoais acedidos fora das instalações são protegidos contra tratamento não autorizado ou ilícito e contra perda acidental.

11.5.3 Considerando 39: Realça a limitação de acesso, a integridade e a confidencialidade, especialmente relevantes quando os dispositivos saem de instalações seguras.

11.6 Diretiva NIS2 da UE (2022/2555)

11.6.1 Artigo 21(2)(a, b, d): Exige que o acesso remoto seja protegido no âmbito do quadro de gestão do risco das TIC de uma organização. Esta política cumpre o requisito de medidas de segurança que abranjam controlo de acessos, segurança dos dados e políticas organizacionais para ambientes remotos.

11.6.2 Artigo 21(3): Promove a sensibilização para a segurança e o cumprimento da política entre o pessoal que trabalha fora das instalações centrais.

11.7 DORA da UE (2022/2554)

11.7.1 Artigo 5 – Quadro de governação e controlo interno: Esta política suporta as expectativas de controlo do risco das TIC para todos os cenários operacionais, incluindo modelos híbridos e remotos.

11.7.2 Artigo 8 – Quadro de gestão do risco das TIC: Os riscos de acesso remoto são identificados, mitigados e governados através dos controlos técnicos e organizacionais aqui aplicados.

11.7.3 Artigo 9 – Mecanismos de partilha de informação: Protege contra fuga remota de informação partilhada em redes de resiliência operacional digital.

11.8 COBIT 2019

11.8.1 DSS01 – Operações Geridas: Esta política suporta a continuidade segura das operações do negócio independentemente da localização física.

11.8.2 BAI06 – Alterações de TI Geridas e BAI09 – Ativos Geridos: Asseguram que os dispositivos de trabalho remoto são rastreados, configurados de forma segura e tratados como ativos críticos.

11.8.3 APO13 – Segurança Gerida: Promove um quadro definido de governação da segurança para ambientes remotos.

11.8.4 MEA03 – Monitorizar, Avaliar e Analisar o Cumprimento: Estabelece que a atividade de trabalho remoto deve ser registada, revista e auditada.