					Insira aqui a designação da entidade jurídica registada							
Número do documento: P21S					Título do documento: **Política de Segurança de Redes**							
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**

Aviso legal (direitos de autor e restrições de utilização)

(C) 2025 Clarysec LLC. All rights reserved.

Este documento é propriedade intelectual da Clarysec LLC. Nenhuma parte deste documento pode ser copiada, reutilizada, distribuída ou modificada para fins comerciais ou de implementação sem autorização prévia, expressa e por escrito.

A utilização não autorizada é estritamente proibida e pode dar origem a ações legais.

Para efeitos de licenciamento, contacte: info@clarysec.com

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	-
ISO/IEC 27002:2022	Controlo 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
RGPD da UE	Artigo 32	-
Diretiva NIS2 da UE	Artigos 21(2)(d), (e)	-
DORA da UE	Artigos 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Finalidade

1.1. A finalidade desta política é assegurar que todas as comunicações de rede internas e externas estejam protegidas contra acesso não autorizado, adulteração, interceção ou utilização indevida, através de controlos de segurança claramente definidos.

1.2. Esta política estabelece regras para a conceção segura, utilização e gestão da infraestrutura de rede, incluindo routers, pontos de acesso sem fios, ligações de acesso remoto e redes segmentadas.

1.3. Esta política visa minimizar a exposição a ameaças baseadas na Internet, assegurar a confidencialidade dos dados transmitidos através de redes internas e externas e manter a disponibilidade dos serviços críticos.

1.4. Esta política suporta a certificação ISO/IEC 27001:2022 e contribui diretamente para o cumprimento das obrigações legais e regulamentares ao abrigo do RGPD da UE, da Diretiva NIS2 da UE e da DORA da UE, proporcionando simultaneamente garantias técnicas a clientes e auditores.

2. Âmbito

2.1. Esta política aplica-se a todos os componentes da rede de TI da organização, incluindo:

2.1.1. Infraestrutura com e sem fios nas localizações de escritório

2.1.2. Routers, switches, pontos de acesso, firewalls e gateways

2.1.3. Ligações de acesso remoto, incluindo VPN, RDP e túneis na cloud

2.1.4. Aplicações alojadas na cloud acedidas a partir de redes internas ou externas

2.1.5. Dispositivos ligados à rede por trabalhadores, contratados ou convidados

2.2. Esta política rege os segmentos de rede físicos e lógicos, incluindo zonas de convidados, dispositivos da Internet das Coisas (IoT) e sistemas de back-office.

2.3. A política abrange todo o pessoal com acesso à rede da organização, incluindo:

2.3.1. Trabalhadores internos

2.3.2. Trabalhadores remotos e pessoal em regime híbrido

2.3.3. Fornecedores externos, consultores e prestadores de serviços

2.3.4. Convidados que utilizem acesso Wi-Fi temporário

3. Objetivos

3.1. Assegurar que a rede da organização está protegida contra acesso não autorizado e ameaças externas de cibersegurança

3.2. Assegurar a segmentação adequada entre redes de confiança e redes não confiáveis (por exemplo, Wi-Fi de convidados, acesso de fornecedores)

3.3. Permitir conectividade remota segura sem comprometer os sistemas internos

3.4. Impedir a propagação de malware e a exfiltração de dados através de canais de rede

3.5. Assegurar a monitorização, os alertas e a auditoria da atividade de rede para apoiar a deteção de incidentes e a conformidade

3.6. Assegurar que apenas dispositivos aprovados e protegidos podem ligar-se às redes internas

3.7. Cumprir obrigações ao abrigo da ISO 27001, do RGPD da UE e de referenciais de cibersegurança relacionados

4. Papéis e responsabilidades

4.1. Diretor-Geral (GM)

4.1.1. É responsável por esta política e assegura a afetação de recursos adequados para a conceção e gestão seguras da rede

4.1.2. Revê exceções aos controlos de segurança de rede e aprova acordos de acesso de fornecedores à rede

4.1.3. Revê incidentes ou constatações de auditoria relacionadas com fragilidades de segurança de rede

4.2. Prestador de suporte de TI / função interna de TI

4.2.1. Implementa, configura e mantém todas as firewalls, routers, switches e controladores sem fios

4.2.2. Gere a segmentação entre redes internas, redes de convidados e redes externas

4.2.3. Monitoriza logs e alertas relativos a tentativas de acesso não autorizado ou anomalias de rede

4.2.4. Assegura que as atualizações de firmware e de configuração são aplicadas de forma segura e atempada

[... 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 Diretor-Geral, em conjunto com o prestador de suporte de TI e o Coordenador de Privacidade.

9.2. Fatores desencadeadores de revisão intercalar

9.2.1. A revisão da política deve também ser desencadeada por:

9.2.1.1. Alterações de maior impacto na arquitetura de rede (por exemplo, novos sistemas de VPN ou firewall)

9.2.1.2. Um incidente relacionado com a rede (por exemplo, intrusão, propagação de ransomware ou exfiltração de dados)

9.2.1.3. Atualizações legais, regulamentares ou de referenciais que afetem a proteção da rede

9.2.1.4. Novas plataformas de fornecedores que exijam métodos de acesso ou protocolos alternativos

9.3. Gestão de versões e documentação

9.3.1. As revisões da política devem ser registadas com número da versão, data e resumo das alterações

9.3.2. As versões anteriores devem ser arquivadas por um período não inferior a 3 anos

9.3.3. As atualizações devem ser comunicadas aos trabalhadores afetados, com aceitação obrigatória quando sejam introduzidas alterações significativas de comportamento

10. Políticas relacionadas e ligações

10.1. Esta política deve ser implementada em conjunto com as seguintes políticas de segurança SME:

10.1.1. P9S – Política de Trabalho Remoto: estabelece métodos seguros de acesso remoto, requisitos de VPN e proteção de endpoint para utilizadores fora das instalações.

10.1.2. P12S – Política de Gestão de Ativos: assegura que todos os sistemas ligados à rede são identificados, categorizados e acompanhados com estados de segurança atualizados.

10.1.3. P17S – Política de Proteção de Dados e Privacidade: assegura que a segmentação de rede, os controlos de acesso e o registo suportam os princípios de privacidade e proteção de dados ao abrigo do RGPD da UE.

10.1.4. P22S – Política de Registo e Monitorização: especifica requisitos para recolha e revisão de logs de dispositivos de rede, ligações remotas e controladores sem fios.

10.1.5. P30S – Política de Resposta a Incidentes: define as ações exigidas em resposta a violações de rede, tentativas de acesso não autorizado ou propagação de malware através de redes internas.

11. Normas e referenciais

11.1. ISO/IEC 27001

11.1.1. Cláusula 8.1 – Exige a implementação de controlos para assegurar operações seguras e resilientes, incluindo redes.

11.2. ISO/IEC 27002

11.2.1. Controlo 8.20 – Fornece orientação técnica e processual para proteger o acesso à rede, a segmentação e a monitorização.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Exige o controlo do fluxo de informação dentro das redes e entre sistemas.

11.3.2. SC-7 – Exige proteção de perímetro, encaminhamento seguro e segmentação de rede para reduzir o risco de acesso não autorizado.

11.4. RGPD da UE

11.4.1. Artigo 32 – Exige medidas técnicas e organizativas adequadas para assegurar a confidencialidade, integridade e disponibilidade dos sistemas e serviços em rede que tratam dados pessoais.

11.5. Diretiva NIS2 da UE

11.5.1. Artigo 21(2)(d) – Exige medidas técnicas baseadas no risco, incluindo segurança de rede e controlo de acesso.

11.5.2. Artigo 21(2)(e) – Exige segmentação e isolamento de sistemas para impedir a propagação de incidentes de cibersegurança.

11.6. DORA da UE

11.6.1. Artigo 9 – Exige que as entidades implementem controlos de gestão do risco das TIC, incluindo os aplicáveis a redes e comunicações seguras.

11.6.2. Artigo 10 – Exige que as estratégias de resiliência digital incluam proteção da infraestrutura de rede e da conetividade remota.

11.7. COBIT 2019

11.7.1. DSS05.02 – Exige proteção eficaz da infraestrutura de TI e dos ambientes de rede contra ameaças internas e externas.

11.7.2. APO13.01 – Exige estratégias de gestão de riscos que incluam segmentação e monitorização de rede como parte da mitigação de ameaças.