					Insira aqui a designação da entidade jurídica registada							
Número do documento: P21					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**

Alinhada com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	N/A
ISO/IEC 27002:2022	Controlos 8.20-8.22	N/A
NIST SP 800-53 Rev. 5	SC-7, AC-4, SC-32	N/A
RGPD da UE	Artigo 32	N/A
Diretiva NIS2 da UE	Artigo 21(2)(d)	N/A
DORA da UE	Artigo 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Finalidade

1.1 A finalidade desta política é definir os requisitos da organização para proteger as suas redes internas e externas contra acessos não autorizados, interrupções de serviço, interceção de dados e utilização indevida.

1.2 Garante que toda a infraestrutura de rede, incluindo componentes físicos, virtuais, em nuvem e híbridos, é protegida por controlos em camadas, tais como segmentação, aplicação de regras de firewall, encaminhamento seguro e monitorização centralizada.

1.3 Esta política assegura o cumprimento da Cláusula 8.1 da ISO/IEC 27001 e dos Controlos 8.20 a 8.22 do Anexo A, bem como das obrigações legais e regulamentares aplicáveis ao abrigo do Artigo 32 do RGPD, do Artigo 21 da Diretiva NIS2 e do Artigo 9 da DORA da UE.

2. Âmbito

2.1 Esta política aplica-se a todas as redes e respetivos componentes de infraestrutura, incluindo:

2.1.1 Routers, switches, pontos de acesso sem fios e firewalls

2.1.2 Redes virtuais na nuvem (por exemplo, AWS VPC, Azure VNET), concentradores VPN e sistemas SD-WAN

2.1.3 LAN internas, DMZ, vias de acesso remoto e ligações entre localizações ou com terceiros

2.1.4 Sistemas de suporte, como DNS, DHCP, servidores proxy e appliances de monitorização

2.2 A política é vinculativa para todo o pessoal e para os prestadores de serviços terceiros que gerem, configurem, monitorizem ou estabeleçam ligação com as redes da organização, quer em instalações próprias quer na nuvem.

2.3 Todos os sistemas e aplicações ligados às redes da organização, independentemente da localização ou titularidade, devem cumprir estes requisitos de segurança de rede.

3. Objetivos

3.1 Assegurar a confidencialidade, integridade e disponibilidade dos dados transmitidos através das redes, mediante controlos de acesso robustos, encaminhamento seguro e monitorização.

3.2 Prevenir acessos não autorizados, movimentação lateral e exploração de recursos de rede através da aplicação de segmentação, zonamento e proteção de perímetro.

3.3 Manter configurações de rede consistentes, com base em normas do setor e inteligência sobre ameaças, para defesa contra ciberameaças em evolução.

3.4 Proteger as comunicações externas, a interligação com a nuvem e o acesso remoto através de canais cifrados, autenticação forte e validação de endpoints.

3.5 Proporcionar visibilidade sobre a atividade de rede através de registo centralizado, inspeção de tráfego em tempo real e geração automática de alertas.

3.6 Assegurar a conformidade regulamentar através do alinhamento de todas as operações de rede com os requisitos da ISO/IEC 27001:2022, do RGPD, da NIS2, da DORA da UE e do COBIT 2019.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É responsável por esta política e assegura a sua revisão e o seu alinhamento com a estratégia global de cibersegurança da organização.

4.1.2 Aprova os modelos de segmentação de rede, os conjuntos de regras de firewall para sistemas sensíveis e os pedidos de exceção.

4.2 Responsável pela Segurança de Redes / Responsável pela Segurança de Infraestruturas

4.2.1 Gere a arquitetura de defesa de rede, incluindo firewalls, sistemas de deteção/prevenção de intrusões (IDS/IPS), VPN e encaminhamento seguro.

4.2.2 Assegura a supervisão da segmentação de rede, das atribuições de VLAN, do zonamento de tráfego e da conectividade externa.

4.2.3 Garante a revisão contínua da filtragem de tráfego de entrada e saída e a aplicação do modelo de confiança zero entre os diferentes níveis de rede.

[... 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 anualmente pelo Responsável pela Segurança de Redes, em colaboração com o CISO, e atualizada com base em:

9.1.1 Ameaças emergentes (por exemplo, novas técnicas de ataque, vulnerabilidades de protocolo)

9.1.2 Alterações na infraestrutura (por exemplo, migrações para a nuvem, implementação de SD-WAN)

9.1.3 Atualizações regulamentares ou normativas que afetem as proteções de rede

9.1.4 Constatações de auditoria, tendências de incidentes ou degradação de desempenho causada pelos controlos

9.2 As revisões devem também ser desencadeadas por:

9.2.1 Alterações significativas à arquitetura de rede

9.2.2 Implementação de novas plataformas de firewall, VPN ou rede na nuvem

9.2.3 Desativação de ativos críticos ou de zonas de confiança

9.3 As atualizações devem ser registadas no Registo de Controlo Documental do SGSI e comunicadas a:

9.3.1 Infraestruturas e Operações de Rede

9.3.2 Equipas de SOC e de Engenharia de Segurança

9.3.3 Equipas de aplicações com dependências de sistema relativamente a fluxos de rede

9.3.4 Todos os prestadores de serviços terceiros com interligação ativa

9.4 Todas as versões anteriores da política devem ser arquivadas de forma segura com anotações do histórico de alterações, para preservar a auditabilidade e a rastreabilidade das alterações.

10. Políticas relacionadas e ligações

10.1 P1 - Política de Segurança da Informação. Estabelece princípios fundamentais de segurança e determina proteções em camadas, incluindo controlos de acesso e de ameaças baseados na rede.

10.2 P4 - Política de Controlo de Acessos. Assegura que a segmentação de rede é aplicada em alinhamento com os papéis dos utilizadores, os princípios do menor privilégio e as regras de aprovisionamento de acessos.

10.3 P5 - Política de Gestão de Alterações. Regula modificações em firewalls, ajustes de regras VPN e alterações de encaminhamento através de um processo documentado e auditável.

10.4 P12 - Política de Gestão de Ativos. Apoia a identificação e classificação dos sistemas em rede e assegura que todos os ativos ligados são geridos no âmbito definido pelas políticas.

10.5 P22 - Política de Registo e Monitorização. Regula a recolha, correlação e retenção de logs de rede, incluindo eventos de firewall, tentativas de acesso e deteção de anomalias.

10.6 P30 - Política de Resposta a Incidentes. Define os procedimentos de escalonamento, contenção e erradicação em resposta a ameaças ou intrusões propagadas pela rede, como DDoS, movimentação lateral ou acesso não autorizado.

11. Normas e referenciais aplicáveis

11.1 Esta política está alinhada com normas internacionais e obrigações regulamentares que definem operações de rede seguras, segmentação, proteção de perímetro e acesso remoto seguro.

11.2 ISO/IEC 27001

11.2.1 Cláusula 8.1 - Planeamento e controlo operacional: Exige que controlos técnicos, incluindo salvaguardas de rede, sejam integrados nos processos operacionais.

11.3 ISO/IEC 27002:2022

11.3.1 Controlos 8.20-8.22. Fornece orientações sobre proteção de redes, segmentação de serviços e segurança de serviços de rede através de controlos de acesso e monitorização.

11.4 NIST SP 800-53 Rev. 5

11.4.1 SC-7 - Proteção de fronteira: Exige controlos de perímetro, segmentação e interligações seguras.

11.4.2 AC-4 - Aplicação do fluxo de informação: Suporta zonamento e restrições de tráfego baseadas em regras.

11.4.3 SC-32 - Particionamento de sistemas de informação: Promove a separação lógica dos sistemas de informação.

11.5 RGPD da UE (2016/679)

11.5.1 Artigo 32 - Segurança do tratamento: Exige medidas técnicas, como firewalls e segmentação, para salvaguardar os dados pessoais.

11.6 Diretiva NIS2 da UE (2022/2555)

11.6.1 Artigo 21(2)(d): Exige segurança eficaz das redes e dos sistemas de informação, proteção de perímetro, configuração segura e controlos de segregação.

11.7 DORA da UE (2022/2554)

11.7.1 Artigo 9 - Gestão do risco das TIC: Obriga as entidades financeiras a proteger redes e interligações contra acessos não autorizados, fuga de dados e interrupção operacional.

11.8 COBIT 2019

11.8.1 DSS01.03 - Monitorizar a infraestrutura: Exige controlo proativo sobre o estado da rede e a conectividade.

11.8.2 DSS05.01 - Proteger contra malware: Inclui segmentação e controlo de fronteira para minimizar a propagação.

11.8.3 MEA03 - Monitorizar, avaliar e analisar a conformidade: Reforça a aplicação da política de rede e as avaliações de conformidade.