					Insira aqui a designação da entidade jurídica registada							
Número do documento: P38					Título do documento: **Política de Comunicações Seguras e Autenticação Multifator**							
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	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
RGPD da UE	Art. 32(1)(b)	
Diretiva NIS2 da UE	Art. 21(2)(j)	
DORA da UE	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Finalidade

1.1 Definir os requisitos para a utilização de soluções de autenticação multifator ou autenticação contínua no acesso aos sistemas, em conformidade com o artigo 21(2)(j) da Diretiva NIS2 da UE.

1.2 Estabelecer controlos para comunicações seguras de voz, vídeo, texto e emergência, de modo a proteger a confidencialidade e a integridade da informação.

2. Âmbito

2.1 Esta política aplica-se a todos os mecanismos de autenticação e sistemas de comunicação (chamadas de voz, videoconferência, mensagens e sistemas de notificação de emergência) utilizados pela organização.

2.2 Abrange todos os colaboradores e prestadores de serviços, bem como quaisquer partes externas que utilizem os canais de comunicação da organização ou acedam às suas redes e sistemas de informação.

3. Objetivos

3.1 Assegurar que apenas utilizadores devidamente autenticados obtêm acesso aos sistemas, reduzindo o risco de acesso não autorizado através da implementação de autenticação multifator.

3.2 Garantir que as comunicações internas e de emergência são transmitidas através de métodos seguros (por exemplo, canais cifrados), prevenindo escuta indevida ou adulteração.

3.3 Cumprir os requisitos da Diretiva NIS2 da UE em matéria de autenticação forte e comunicações seguras, reforçando a resiliência cibernética global.

4. Papéis e responsabilidades

4.1 Responsável pela Segurança da Informação / Segurança de TI: definir e manter os mecanismos de autenticação multifator e as ferramentas de comunicação segura; assegurar a implementação técnica desta política.

4.2 Administradores de TI: implementar a autenticação multifator nos sistemas aplicáveis e configurar as plataformas de comunicação segura aprovadas; monitorizar o cumprimento.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Monitorização e auditoria

9.1 A Segurança de TI deve monitorizar continuamente os registos de autenticação para identificar tentativas de autenticação com fator único ou falhas anómalas de autenticação multifator. Os registos dos sistemas de comunicação segura, quando aplicável, devem ser monitorizados para detetar tentativas de acesso não autorizado ou alterações de configuração.

9.2 A Auditoria Interna / Função de Conformidade deve rever anualmente a conformidade da implementação da autenticação multifator, assegurando que todos os sistemas críticos a aplicam, e verificar que os canais seguros aprovados são utilizados em exclusivo para comunicações sensíveis. As constatações devem ser comunicadas à gestão com as respetivas recomendações.

10. Revisão e manutenção

10.1 Esta política será revista pelo menos anualmente e sempre que ocorra um incidente de segurança relevante ou seja identificado um novo risco relacionado com autenticação ou comunicações (por exemplo, novos vetores de ameaça contra a autenticação multifator ou deteção da utilização de comunicações inseguras).

10.2 As revisões serão efetuadas sempre que necessário para responder à evolução tecnológica (por exemplo, adoção de soluções de autenticação contínua mais robustas) ou para cumprir orientações regulamentares atualizadas, tais como futuras recomendações da ENISA sobre comunicações seguras.

11. Políticas relacionadas e ligações

11.1 P01 – Política de Segurança da Informação. Estabelece salvaguardas de autenticação e comunicações aplicáveis a toda a organização.

11.2 P04 – Política de Controlo de Acessos. Estabelece a governação de acessos cuja aplicação é reforçada pela autenticação multifator prevista na P38.

11.3 P11 – Política de Gestão de Contas de Utilizador e Privilégios. Relaciona a autenticação multifator com o ciclo de vida do acesso privilegiado.

11.4 P18 – Política de Controlos Criptográficos. Define a gestão aprovada da criptografia e das chaves para comunicações seguras.

11.5 P21 – Política de Segurança de Redes. Protege os canais de transporte utilizados por voz, vídeo e mensagens.

11.6 P22 – Política de Registo e Monitorização. Monitoriza eventos de autenticação e a utilização de canais seguros.

11.7 P32 – Política de Continuidade do Negócio e Recuperação de Desastre. Protege as comunicações de emergência durante situações de crise.

11.8 P08 – Política de Sensibilização e Formação em Segurança da Informação. Capacita os utilizadores em autenticação multifator e boas práticas na utilização dos canais.

12. Referências

12.1 Diretiva NIS2 (UE 2022/2555), artigo 21(2), alínea (j) (utilização de autenticação multifator e comunicações seguras).

12.2 Regulamento de Execução da Comissão (UE) 2024/2690, secção 11 do anexo (requisitos de controlo de acessos, incluindo autenticação multifator para contas privilegiadas).

12.3 ISO/IEC 27001:2022 e ISO/IEC 27002: