					Insira aqui a designação da entidade jurídica registada							
Número do documento: P36					Título do documento: **Política de Redes Sociais e Comunicações Externas**							
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	Processos definidos e governação baseada em funções para gerir comunicações públicas, assegurando exatidão, fluxos de aprovação e escalonamento de incidentes.
ISO/IEC 27002:2022	Controlos 5.10, 5.11, 5.35, 5.36	Regula a utilização da informação, a utilização aceitável, o contacto externo/comunicação com autoridades e o reporte de conformidade.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Regras para a utilização de sistemas e comunicações, notificações aos utilizadores e retenção de registos de auditoria.
RGPD da UE	Artigos 5, 25, 32, 33	Princípios do tratamento de dados, proteção de dados desde a conceção e por defeito, segurança do tratamento e obrigações de notificação de violação de dados pessoais.
Diretiva NIS2 da UE	Artigo 21	Medidas de gestão do risco das TIC e da cibersegurança, bem como obrigações relativas a incidentes e comunicações públicas relacionadas com risco.
DORA da UE	Artigos 9, 16	Gestão do risco das TIC e estratégia de comunicação para prestadores críticos.
COBIT 2019	APO09, DSS05	Governação de acordos de serviço e comunicações, e práticas de comunicação segura e gestão de incidentes.

1. Finalidade

1.1 A presente política estabelece regras e responsabilidades obrigatórias que regem a utilização de redes sociais e todas as formas de comunicação externa por pessoal com vínculo à organização.

1.2 Garante que as mensagens públicas — planeadas ou espontâneas — são exatas, respeitosas, seguras, conformes com os requisitos legais e consistentes com a marca.

1.3 A política visa minimizar os riscos associados a danos reputacionais, incumprimento regulamentar, fuga de propriedade intelectual e divulgações não autorizadas através de canais públicos.

1.4 Promove ainda a responsabilização e uma governação estruturada em todas as formas de comunicação digital que envolvam ou afetem a organização.

2. Âmbito

2.1 Esta política aplica-se a todos os trabalhadores, contratados, estagiários e representantes de terceiros que:

2.1.1 Comuniquem em nome da organização, de forma oficial ou informal

2.1.2 Façam referência à organização ou insinuem afiliação com a mesma em contexto público

2.1.3 Utilizem contas pessoais ou corporativas para participar em discussões públicas que envolvam a organização

2.2 Os canais de comunicação abrangidos incluem, entre outros:

2.2.1 Plataformas de redes sociais (por exemplo, LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 Blogues, wikis, fóruns e painéis públicos de discussão

2.2.3 Correio eletrónico ou mensagens diretas para partes externas (por exemplo, clientes, reguladores, meios de comunicação social)

2.2.4 Entrevistas à imprensa, painéis de oradores ou participações gravadas em meios de comunicação social

2.2.5 Participação em comunidades online nas quais a organização seja referida

2.3 Esta política rege conteúdos em tempo real e conteúdos pré-agendados e aplica-se a todos os dispositivos e contas, pessoais ou corporativos, utilizados para divulgar comunicações.

3. Objetivos

3.1 Prevenir a divulgação acidental ou intencional de informação confidencial, sensível ou regulada através de canais de comunicação externos.

3.2 Assegurar que as declarações públicas oficiais e os conteúdos em redes sociais são exatos, autorizados e alinhados com a marca corporativa, a ética e as mensagens estratégicas.

3.3 Prevenir danos reputacionais e assegurar a consistência das mensagens entre departamentos internos e plataformas externas.

3.4 Cumprir as obrigações legais aplicáveis relacionadas com declarações públicas, incluindo, entre outras, o RGPD da UE, a Diretiva NIS2 da UE, o DORA da UE e regras setoriais de comunicação.

3.5 Definir responsabilidades claras, utilizações permitidas e protocolos de aplicação para todo o pessoal envolvido em atividades com exposição pública.

4. Papéis e responsabilidades

4.1 Diretor de Marketing ou Comunicação / Responsável de Relações Públicas

4.1.1 Aprova todas as mensagens oficiais da organização para publicação externa

4.1.2 Mantém calendários de conteúdos para redes sociais e orientações para a consistência da marca

4.1.3 Monitoriza menções online e exposição mediática envolvendo a organização

4.2 Diretor de Segurança da Informação (CISO) / Equipa de Segurança da Informação

4.2.1 Monitoriza plataformas digitais para indicadores de fuga de dados, usurpação de identidade ou tentativas de phishing

4.2.2 Coordena com as equipas de resposta a incidentes em caso de ataques ou violações baseadas em redes sociais

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

9. Aplicação e cumprimento

9.1 Esta política é obrigatória para todo o pessoal abrangido e para terceiros. O incumprimento pode resultar em:

9.1.1 advertências formais

9.1.2 revogação temporária ou permanente de acesso a plataformas ou sistemas

9.1.3 medidas disciplinares, incluindo cessação

9.1.4 ações judiciais, se a comunicação externa resultar em danos reputacionais, violação de dados ou incumprimento regulamentar

9.2 Medidas disciplinares

9.2.1 As violações internas (por exemplo, fuga de dados confidenciais, difamação da organização) implicam o envolvimento de Recursos Humanos, investigação formal e documentação no processo do trabalhador.

9.2.2 Quando aplicável, a área Jurídica promoverá vias cíveis de reparação ou notificará as autoridades quanto a atividade criminosa (por exemplo, usurpação de identidade, fugas relacionadas com abuso de informação privilegiada).

9.3 Monitorização do cumprimento

9.3.1 As equipas de Segurança e Comunicação devem realizar monitorização contínua de:

9.3.1.1 Menções à marca nas principais plataformas

9.3.1.2 Utilização não oficial de imagens da organização ou marcas registadas

9.3.1.3 Riscos conhecidos (por exemplo, trabalhadores descontentes, tentativas de usurpação de identidade)

9.3.2 A monitorização deve cumprir a legislação e regulamentação relativas à privacidade dos trabalhadores, devendo todos os casos sinalizados ser verificados por um revisor humano.

9.4 Denúncia e reporte de utilização indevida

9.4.1 Qualquer trabalhador que suspeite de uma violação desta política deve reportá-la à equipa de Segurança da Informação, à área Jurídica ou, de forma anónima, através do portal de denúncia.

9.4.2 Retaliações contra denunciantes são estritamente proibidas e estão sujeitas a ação disciplinar imediata.

10. Requisitos de revisão e atualização

10.1 Esta política deve ser revista anualmente, ou antes, se:

10.1.1 Existirem alterações significativas nos requisitos regulamentares (por exemplo, nova legislação da UE sobre comunicações digitais)

10.1.2 Forem adotadas novas plataformas sociais ou novos canais de comunicação

10.1.3 Ocorrer um incidente significativo ou violações repetidas que indiquem lacunas no processo

10.1.4 Ocorrer uma alteração estrutural ou de liderança nas funções de Relações Públicas, Jurídico ou Segurança

10.2 A revisão deve ser conduzida conjuntamente por:

10.2.1 O responsável de Marketing / Relações Públicas

10.2.2 O CISO ou o responsável pelo risco de segurança

10.2.3 Responsáveis Jurídicos e de Conformidade

10.3 As atualizações devem ser documentadas no Registo de Alterações à Política e comunicadas através dos canais internos de sensibilização. Quando ocorram alterações materiais, todo o pessoal afetado deve confirmar novamente a política.

11. Políticas relacionadas e articulações

11.1 Esta política é suportada e inter-relaciona-se com os seguintes componentes do Sistema de Gestão da Segurança da Informação (SGSI) da organização:

11.1.1 P1 – Política de Segurança da Informação: Estabelece princípios gerais para a salvaguarda da informação, incluindo a garantia de que as comunicações não conduzem a divulgação não autorizada.

11.1.2 P3 – Política de Utilização Aceitável: Define comportamentos aceitáveis para plataformas e tecnologias digitais, regulando diretamente a utilização pessoal e profissional de canais sociais.

11.1.3 P6 – Política de Gestão de Riscos: Fornece o quadro de risco para avaliar ameaças relacionadas com comunicação pública e exposição reputacional.

11.1.4 P8 – Política de Sensibilização e Formação em Segurança da Informação: Impõe programas de sensibilização que instruem o pessoal sobre práticas seguras de comunicação e ameaças de engenharia social.

11.1.5 P13 – Política de Classificação e Rotulagem da Informação: Orienta o pessoal sobre o que constitui informação restrita ou confidencial, a qual não deve ser divulgada externamente.

11.1.6 P30 – Política de Resposta a Incidentes: Define como tratar incidentes relacionados com comunicação pública, incluindo fuga de dados, usurpação de identidade e incumprimento regulamentar.

11.1.7 P33 – Política de Monitorização de Auditoria e Conformidade: Rege os processos de auditoria que validam controlos de redes sociais, sistemas de monitorização e cumprimento das políticas de comunicação externa.

12. Normas e referenciais

12.1 ISO/IEC 27001:

12.1.1 Cláusula 8.1 – Planeamento e Controlo Operacional: Exige processos definidos e governação baseada em funções para gerir comunicações públicas, assegurando exatidão, fluxos de aprovação e escalonamento de incidentes envolvendo dados ou risco reputacional.

12.2 ISO/IEC 27002:2022:

12.2.1 Controlo 5.10 – Utilização da Informação: Regula a disseminação autorizada e ética de comunicações internas ou externas.

12.2.2 Controlo 5.11 – Utilização aceitável da informação e dos ativos: Reforça práticas aceitáveis para a partilha de conteúdos utilizando ativos corporativos ou contas pessoais.

12.2.3 Controlo 5.35 – Contacto com Autoridades: Exige comunicação externa estruturada e autorizada com entidades reguladoras e organismos públicos.

12.2.4 Controlo 5.36 – Cumprimento de Políticas e Normas: Impõe a aplicação consistente das políticas internas em todos os cenários de comunicação.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Regras de comportamento: Exige regras formais para a utilização de sistemas e comunicações, incluindo normas de divulgação pública.

12.3.2 AC-8 – Notificação de utilização do sistema: Sustenta avisos obrigatórios e advertências de conteúdo em plataformas com exposição externa.

12.3.3 AU-12 – Retenção de registos de auditoria: Aplica-se à preservação de logs e do histórico de comunicações para revisão de incidentes e fins de auditoria.

12.4 RGPD da UE (2016/679):

12.4.1 Artigo 5 – Princípios Relativos ao Tratamento de Dados Pessoais: Proíbe a partilha não autorizada de dados pessoais através de comunicação pública.

12.4.2 Artigo 25 – Proteção de Dados desde a Conceção e por Defeito: Exige salvaguardas de privacidade em ferramentas de comunicação e fluxos de conteúdos.

12.4.3 Artigo 32 – Segurança do tratamento: Aplica cifragem, controlo de acesso e processos de aprovação de conteúdos.

12.4.4 Artigo 33 – Notificação de violação: Exige notificação atempada de violações de dados pessoais através de canais públicos, quando aplicável.

12.5 Diretiva NIS2 da UE (2022/2555):

12.5.1 Artigo 21 – Medidas de Gestão de Risco em Cibersegurança: Inclui protocolos de comunicação e obrigações durante incidentes e mensagens públicas relacionadas com risco.

12.6 DORA da UE (2022/2554):

12.6.1 Artigo 9 – Gestão do risco das TIC: Aplica-se a riscos de comunicação desencadeados externamente, como usurpação de identidade, desinformação e perturbação reputacional.

12.6.2 Artigo 16 – Estratégia de comunicação: Exige que prestadores críticos financeiros ou de serviços gerem riscos de comunicação e respostas em cenários de crise.

12.7 COBIT 2019:

12.7.1 APO09 – Acordos de serviço geridos e comunicação: Exige governação estruturada sobre comunicações internas e externas.

12.7.2 DSS05 – Gerir serviços de segurança: Assegura que as atividades de comunicação não introduzem risco adicional nem comprometem os processos de tratamento de incidentes.