

Política de Segurança da Informação e Cibersegurança

Princípios de proteção da informação, serviços digitais, infraestruturas e relações com clientes e parceiros.

REFERÊNCIA	VERSÃO	DATA	CLASSIFICAÇÃO
NW-SEG-001	3.0	10/10/2026	PÚBLICO

NEXTWEB – PRESTAÇÃO DE SERVIÇOS NA ÁREA DA INTERNET LDA.

Rua António Lima Fragoso, 145 · 3060-216 Cantanhede · www.nextweb.pt

1. Enquadramento, finalidade e compromisso

A segurança da informação é um elemento essencial da relação de confiança da Nextweb com clientes, colaboradores, parceiros e fornecedores. A presente política estabelece princípios e responsabilidades para reduzir os riscos que afetem a confidencialidade, integridade, disponibilidade e autenticidade da informação, sem divulgar arquitetura ou procedimentos técnicos reservados.

A Gerência promove uma abordagem baseada no risco, na proteção proporcional dos ativos e na melhoria contínua, adequada às dimensões e operações da empresa e aos compromissos contratuais que assuma. O objetivo é prevenir incidentes, detetar anomalias, limitar impactos e suportar a continuidade dos serviços.

2. Âmbito de aplicação e destinatários

A política abrange os serviços de consultoria e assistência informática, alojamento e infraestruturas, redes e telecomunicações, serviços cloud, gestão de sistemas, dispositivos e aplicações, portal de clientes, backups e atividades comerciais e administrativas. Aplica-se a colaboradores, prestadores e terceiros autorizados sempre que utilizem recursos ou informação sob responsabilidade da Nextweb.

A proteção abrange informação eletrónica ou em papel, comunicações verbais, dispositivos móveis, sistemas virtuais e físicos, credenciais, contas, documentação, registos e conteúdos de clientes. Obrigações adicionais podem resultar de contratos e de procedimentos técnicos internos.

3. Terminologia e princípios orientadores

Ativo: recurso físico, digital, humano ou informacional relevante para a organização. Ameaça: circunstância capaz de provocar dano. Vulnerabilidade: fragilidade passível de exploração. Risco: efeito da incerteza sobre os objetivos, considerado segundo probabilidade e impacto. Incidente: evento que compromete ou ameaça a segurança. SGSI: sistema de gestão de segurança da informação. CISO: função de coordenação de segurança da informação, quando formalmente atribuída.

Confidencialidade significa impedir acesso ou divulgação não autorizados; integridade significa preservar exatidão e ausência de alterações indevidas; disponibilidade significa garantir acesso oportuno por utilizadores autorizados. A estes juntam-se autenticidade, rastreabilidade, minimização, segregação de funções e defesa em profundidade.

4. Governo, funções e responsabilidades

A Gerência define prioridades, assegura recursos proporcionais, aprecia riscos relevantes e determina medidas corretivas. A função responsável pela segurança coordena a avaliação de riscos, acompanhamento de eventos, recomendações de controlo e articulação com direção técnica e responsáveis pelos serviços.

As equipas técnicas implementam e documentam as configurações autorizadas, monitorizam sistemas e comunicam desvios. Os colaboradores devem respeitar regras de utilização, proteger credenciais e reportar anomalias. Os fornecedores devem cumprir as cláusulas de segurança contratadas. Os clientes devem salvaguardar as suas próprias credenciais, utilizadores e infraestruturas sob a sua administração.

5. Gestão de ativos e classificação da informação

Os ativos críticos devem ser inventariados e ter responsáveis identificados. A informação deverá ser classificada, proporcionalmente ao risco, em pública, interna, confidencial ou de acesso especialmente restrito. A divulgação, reprodução e armazenamento obedecem à classificação e ao princípio da necessidade de conhecimento.

Os meios de armazenamento, documentos e equipamentos devem ser devolvidos, eliminados ou reutilizados com métodos compatíveis com a sensibilidade dos dados e com os acordos contratuais.

6. Gestão de identidades e controlo de acessos

O acesso a recursos e informações é atribuído apenas quando necessário à função ou ao serviço, com perfis definidos, autorização adequada e revisão periódica. As contas devem ser individualizadas sempre que tecnicamente possível; credenciais partilhadas devem ser excecionais, justificadas e controladas.

São promovidas práticas de autenticação robusta e autenticação multifator nos sistemas em que seja tecnicamente viável e proporcional ao risco, sobretudo em acessos administrativos e remotos. A criação, alteração e desativação de acessos acompanha as necessidades operacionais e a cessação das autorizações.

7. Segurança de redes, sistemas e infraestruturas

Os sistemas e comunicações são geridos mediante arquitetura coerente com o risco, regras de rede e segmentação quando apropriadas, configuração segura, proteção de interfaces administrativas, atualizações controladas e gestão de vulnerabilidades. Os equipamentos e serviços expostos à Internet recebem atenção acrescida.

As operações de manutenção, correção de falhas e alterações significativas devem considerar o impacto nos serviços e, quando aplicável, prever janelas de intervenção, registos, planos de retorno e comunicação ao cliente.

8. Proteção de endpoints, correio eletrónico e utilização aceitável

Os utilizadores devem proteger os dispositivos contra utilização indevida, evitar software não autorizado e verificar a legitimidade de mensagens e pedidos inesperados. São promovidas medidas de proteção contra malware, phishing, utilização abusiva de credenciais, fraude por correio eletrónico e alterações maliciosas de sistemas.

Anexos suspeitos, pedidos de credenciais, alterações de dados bancários e ligações inesperadas devem ser confirmados por canal independente sempre que o risco o justifique. A formação e a sensibilização são componentes essenciais da prevenção.

9. Gestão de cópias de segurança e continuidade

Os serviços e ativos críticos são avaliados para definir necessidades de salvaguarda e recuperação, incluindo cópias de segurança, redundância e procedimentos de contingência quando contratualmente e tecnicamente aplicáveis. A existência de uma cópia de segurança não equivale a garantia de recuperação imediata; a restauração depende do estado das cópias, dependências técnicas e prioridades definidas.

A política específica de continuidade descreve princípios adicionais; os procedimentos detalhados, inventários, contactos e planos de recuperação são mantidos em documentação reservada.

10. Registos, monitorização e resposta a incidentes

São estabelecidos mecanismos de registo e acompanhamento adequados aos serviços geridos, tendo em conta privacidade e proporcionalidade. Uma anomalia relevante deve ser comunicada pelos canais de suporte ou segurança, investigada e classificada segundo impacto, urgência e extensão.

A resposta pode incluir contenção, preservação de evidências, análise técnica, correção, recuperação e comunicação ao cliente e às autoridades quando legalmente exigível. As comunicações externas observam as responsabilidades legais e contratuais e não substituem instruções de emergência.

11. Proteção de dados pessoais

Os tratamentos de dados pessoais são orientados pelos princípios do RGPD, incluindo licitude, minimização, limitação da conservação e medidas adequadas de proteção. Em serviços prestados como subcontratante, o acesso a dados de clientes deve limitar-se às instruções documentadas e ao âmbito necessário para prestar o serviço.

12. Fornecedores, parceiros e serviços externos

A seleção e utilização de fornecedores deverá considerar criticidade, adequação técnica, segurança, localização de dados quando relevante e compromissos contratuais. A certificação de um fornecedor não equivale a certificação da Nextweb e não deve ser apresentada como tal.

Nas prestações de serviços de telecomunicações ou satélite podem aplicar-se condições específicas dos operadores, incluindo manutenção programada, dependências de rede e equipamento terminal (CPE), as quais são articuladas com as condições comerciais e contratuais em vigor.

13. Gestão de risco, conformidade e melhoria contínua

Os riscos devem ser identificados, avaliados e tratados mediante medidas de prevenção, mitigação, transferência ou aceitação informada. A adequação dos controlos é revista perante alterações de sistemas, incidentes, requisitos legais, fornecedores ou novos serviços.

A empresa atende ao RGPD e à legislação nacional aplicável, incluindo o regime jurídico da cibersegurança aprovado pelo Decreto-Lei n.º 125/2025, de 4 de dezembro, na medida em que as suas atividades e o seu enquadramento legal o determinem. A referência a normas como ISO/IEC 27001 exprime boas práticas de orientação, não constituindo declaração de certificação.

14. Comunicação, formação e revisão

A presente política é disponibilizada aos destinatários relevantes, reforçada por procedimentos internos e revista periodicamente ou quando existam alterações significativas. As responsabilidades e medidas descritas devem ser concretizadas mediante documentação operacional, contratos e evidências adequadas.

15. Contacto institucional de segurança

As comunicações sobre anomalias, suspeitas de incidentes ou vulnerabilidades poderão ser dirigidas aos canais institucionais de suporte da Nextweb, através do portal ou de contacto publicado em www.nextweb.pt. Em emergências que envolvam perigo imediato para pessoas, devem ser utilizados os serviços públicos de emergência.