					Insira aqui a designação da entidade jurídica registada							
Número do documento: P30					Título do documento: **Política de resposta a incidentes**							
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 8.1, Cláusula 9	Processos estruturados para gestão de riscos e resposta a incidentes
ISO/IEC 27002:2022	Controlos 5.25–5.27	Papéis, notificação, resposta e melhoria contínua na gestão de incidentes
NIST SP 800-53 Rev.5	IR-1 a IR-9	Ciclo de vida abrangente de resposta a incidentes
RGPD da UE	Artigo 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Prazos de notificação de violações de dados, reporte e comunicação aos titulares dos dados
Diretiva NIS2 da UE	Artigo 23(1)–(4)	Notificação à autoridade nacional e reporte estruturado
DORA da UE	Artigo 17(1)–(3)	Reporte de incidentes graves relacionados com TIC por entidades financeiras
COBIT 2019	DSS02, DSS04, MEA	Define, monitoriza e avalia a gestão de incidentes, a continuidade e a avaliação

1. Finalidade

1.1 Esta política estabelece uma estrutura formal para a identificação, notificação, análise, contenção, resposta, recuperação e avaliação pós-incidente de incidentes de segurança da informação que afetem a organização.

1.2 Assegura respostas atempadas, coordenadas e eficazes para minimizar a interrupção operacional, as perdas financeiras, os danos reputacionais e o incumprimento regulamentar.

1.3 Esta política promove igualmente a melhoria contínua da postura de ciber-resiliência da organização, através das lições aprendidas e da integração das conclusões pós-incidente na governação, nas ferramentas e nos programas de formação.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todo o pessoal, incluindo trabalhadores, contratados, consultores e prestadores de serviços terceiros

2.1.2 Todos os sistemas de informação, aplicações, infraestruturas, redes e dados, quer em instalações próprias, na nuvem ou em ambientes híbridos

2.1.3 Todos os tipos de incidentes de segurança, incluindo, entre outros:

2.1.3.1 Acesso não autorizado ou elevação de privilégios

2.1.3.2 Ataques de malware e ransomware

2.1.3.3 Ataques de negação de serviço (DoS/DDoS)

2.1.3.4 Perda, fuga ou exfiltração de dados

2.1.3.5 Utilização indevida por ameaças internas ou violações da política

2.1.3.6 Violações de segurança física com impacto em ativos digitais

2.2 Esta política abrange a deteção, triagem, investigação, escalonamento, contenção, tratamento de evidência, notificação, recuperação e análise de causa raiz.

3. Objetivos

3.1 Estabelecer uma capacidade de resposta a incidentes repetível e escalável, que permita a deteção, classificação e mitigação rápidas de incidentes de segurança.

3.2 Minimizar o impacto no negócio dos eventos de segurança através de procedimentos estruturados de contenção, erradicação e recuperação de sistemas.

3.3 Assegurar que a notificação e a resposta a incidentes estão alinhadas com os requisitos legais, regulamentares e contratuais, em particular os relativos a prazos de notificação de violações e ao tratamento de evidência.

3.4 Apoiar a transparência e a responsabilização através de registo adequado, documentação e monitorização de métricas para todos os incidentes de segurança.

3.5 Promover a melhoria contínua através de revisões pós-incidente, ações corretivas e formação das partes interessadas.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É responsável pelo quadro de resposta a incidentes, assegura a aplicação desta política e supervisiona a coordenação de incidentes em toda a organização.

4.1.2 Atua como principal ponto de contacto junto de reguladores, da direção executiva e da assessoria jurídica externa durante incidentes de maior gravidade.

4.2 Coordenador de Resposta a Incidentes

4.2.1 Coordena equipas de resposta multidisciplinares, gere os fluxos de trabalho e acompanha o estado da contenção e da recuperação.

4.2.2 Convoca e conduz revisões pós-incidente (PIR) e assegura que as ações corretivas são registadas e implementadas.

[... 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 pelo menos anualmente e atualizada sempre que necessário para incorporar:

9.1.1 Alterações no panorama de ameaças, nos tipos de incidentes ou nos vetores de ataque

9.1.2 Lições aprendidas de incidentes relevantes, quase incidentes ou conclusões regulatórias

9.1.3 Atualizações de leis e regulamentos aplicáveis (por exemplo, RGPD da UE, DORA da UE, Diretiva NIS2 da UE)

9.1.4 Feedback de exercícios de resposta a incidentes e de revisões pós-incidente

9.2 O CISO é responsável por iniciar e coordenar o processo de revisão, em consulta com:

9.2.1.1 Assessoria jurídica e EPD

9.2.1.2 SOC e Operações de TI

9.2.1.3 Equipas de Continuidade de Negócio e Gestão de Riscos

9.2.1.4 Direção executiva

9.3 As alterações à política devem ser:

9.3.1 Documentadas num repositório sujeito a controlo de versões

9.3.2 Comunicadas a todas as equipas afetadas e refletidas na formação de sensibilização

9.3.3 Validadas através de exercícios de mesa ou exercícios de resposta a incidentes em ambiente real no prazo de três meses após a aprovação

9.4 As atualizações urgentes desencadeadas por ameaças emergentes, conclusões de auditoria ou novas obrigações legais devem ser implementadas de imediato e registadas no histórico de revisões da política.

10. Políticas relacionadas e interdependências

10.1 Esta política é suportada pelas seguintes políticas organizacionais e depende das mesmas:

10.1.1 P1 – Política de Segurança da Informação: Estabelece o requisito global para operações preparadas para incidentes e baseadas no risco.

10.1.2 P5 – Política de Gestão de Alterações: Assegura que as atividades de contenção e recuperação que envolvam infraestruturas ou serviços seguem procedimentos formais.

10.1.3 P13 – Política de Classificação e Rotulagem da Informação: Suporta a classificação da gravidade dos incidentes com base na sensibilidade dos dados.

10.1.4 P15 – Política de Cópias de Segurança e Restauro: Permite a recuperação de incidentes de ransomware ou de ataques destrutivos com garantia de integridade.

10.1.5 P18 – Política de Controlos Criptográficos: Define medidas de cifragem que reduzem o impacto dos incidentes e os riscos de exposição de dados.

10.1.6 P22 – Política de Registo de Logs e Monitorização: Fornece a visibilidade de eventos, a geração de alertas e a retenção de logs essenciais para uma deteção eficaz e para fins forenses.

10.1.7 P29 – Política de Dados de Teste e Ambientes de Teste: Assegura que os incidentes que afetem sistemas de não produção também são tratados de forma estruturada e segura.

10.1.8 P33 – Política de Monitorização de Auditoria e Conformidade: Valida a preparação para incidentes e a eficácia da resposta através de auditorias estruturadas e avaliações de conformidade.

11. Normas e referenciais aplicáveis

11.1 ISO/IEC 27001: Cláusula 8.1 – Planeamento e Controlo Operacional: Processos estruturados para gerir riscos e planear a resposta a incidentes.

11.2 ISO/IEC 27002:2022 – Controlos 5.25–5.27: Responsabilidades pela gestão de incidentes, notificação, resposta, comunicação e melhoria contínua.

11.3 NIST SP 800-53 Rev.5: IR-1 a IR-9, AU-6, PL-2: Requisitos abrangentes para o ciclo de vida da resposta a incidentes, auditoria e planeamento de segurança.

11.4 RGPD da UE: Artigos 33/34: Obrigações de reporte às autoridades de controlo e requisitos de notificação aos titulares dos dados (com exceções definidas).

11.5 Diretiva NIS2 da UE (2022/2555): Artigo 23: Reporte nacional obrigatório, com obrigações de reporte intermédio e final.

11.6 DORA da UE (2022/2554): Artigo 17: Requisitos de reporte de incidentes relacionados com TIC às autoridades competentes por instituições financeiras.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Gestão de incidentes de serviço e continuidade, bem como monitorização do desempenho e da conformidade.