					Insira aqui a designação da entidade jurídica registada							
Número do documento: P31					Título do documento: **Política de Recolha de Evidência e Análise Forense**							
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	
ISO/IEC 27002:2022	Controlos 5.25–5.27, 8	
ISO/IEC 27035:2016	Partes 1 e 3	
NIST SP 800-53 Rev. 5	IR-1 a IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Análise forense de dispositivos móveis e suportes	Análise forense de dispositivos móveis e suportes
NIST SP 800-86	Integração de técnicas forenses	Integração de técnicas forenses na resposta a incidentes
RGPD da UE	Artigo 5, 33–34	
Diretiva NIS2 da UE	Artigo 23(1)–(4)	
DORA da UE	Artigo 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Finalidade

1.1 A presente política estabelece um quadro estruturado e juridicamente defensável para a identificação, recolha, preservação, análise e eliminação de evidência digital durante incidentes de segurança reais ou suspeitos.

1.2 Assegura que os processos de preparação forense e de tratamento da evidência:

1.2.1 Mantêm a integridade da evidência e a documentação da cadeia de custódia.

1.2.2 Suportam investigações internas, processos judiciais ou reporte regulamentar.

1.2.3 Estão alinhados com normas forenses internacionalmente reconhecidas e critérios de admissibilidade legal.

1.3 A política suporta o compromisso da organização com uma resposta a incidentes proativa, o cumprimento legal e a transparência da governação, minimizando simultaneamente a disrupção operacional.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os trabalhadores, contratados, fornecedores e prestadores de serviços envolvidos na administração de sistemas, no tratamento de incidentes ou em atividades de investigação.

2.1.2 Todos os endpoints, servidores, aplicações, redes e plataformas na nuvem sob controlo organizacional ou responsabilidade contratual.

2.1.3 Qualquer incidente ou evento que exija tratamento de evidência, incluindo:

2.1.3.1 Ameaças internas, violações de dados ou investigações de fraude.

2.1.3.2 Utilização indevida de sistemas ou credenciais de autenticação.

2.1.3.3 Incidentes de Tecnologia Operacional (OT) ou de controlo industrial.

2.1.3.4 Violações de acesso físico envolvendo ativos digitais.

2.2 A política regula igualmente qualquer interação com serviços forenses de terceiros ou autoridades policiais durante escalonamentos legais ou processos regulamentares.

3. Objetivos

3.1 Permitir a aquisição rápida, segura e conforme com a política de evidência durante eventos de segurança ou investigações.

3.2 Preservar a integridade, autenticidade e admissibilidade da evidência digital recolhida através de controlo rigoroso de acessos, registo e procedimentos de verificação.

3.3 Assegurar que todas as atividades forenses são coordenadas com as obrigações legais e regulamentares, incluindo proteção de dados, legislação laboral e restrições a transferências internacionais.

3.4 Suportar a análise pós-incidente, a determinação da causa-raiz e a melhoria dos controlos através de resultados forenses de elevada qualidade.

3.5 Integrar a preparação forense no Sistema de Gestão da Segurança da Informação (SGSI), apoiando auditorias, notificações de violação e a tomada de decisão executiva.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É o responsável por esta política e assegura que todas as operações forenses são juridicamente defensáveis, auditáveis e baseadas no risco.

4.1.2 Autoriza o escalonamento para entidades legais externas e prestadores de serviços forenses.

4.2 Analistas forenses / Responsáveis pelo tratamento de incidentes

4.2.1 Lideram a aquisição, preservação e análise técnica da evidência.

4.2.2 Asseguram que a cadeia de custódia é devidamente registada e mantida.

4.2.3 Documentam todas as ações, conclusões e configurações das ferramentas utilizadas durante as investigações.

[... 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 refletir:

9.1.1 Alterações na legislação, regulamentação ou jurisprudência que afetem os procedimentos forenses ou o tratamento de dados.

9.1.2 Atualizações de normas ou conjuntos de ferramentas forenses reconhecidos pelo setor.

9.1.3 Lições aprendidas em revisões pós-incidente, litígios ou constatações de auditoria.

9.1.4 Alterações tecnológicas em plataformas, dispositivos ou sistemas sob investigação.

9.2 O processo de revisão é da responsabilidade do CISO e deve incluir consulta a:

9.2.1 Jurídico e Conformidade.

9.2.2 Encarregado da Proteção de Dados (EPD).

9.2.3 Equipas de Operações de Segurança e Análise Forense.

9.2.4 Auditoria Interna.

9.3 Todas as revisões devem ser:

9.3.1 Sujeitas a controlo de versões e armazenadas no repositório de políticas.

9.3.2 Comunicadas às partes interessadas afetadas, incluindo equipas forenses e de resposta.

9.3.3 Acompanhadas de atualizações aos procedimentos operacionais e materiais de formação relevantes.

9.4 As revisões intercalares devem ser acionadas após qualquer incidente crítico que envolva tratamento incorreto de evidência, falha da cadeia de custódia ou problemas de admissibilidade legal.

10. Políticas relacionadas e ligações

10.1 Esta política está alinhada com e é suportada pelas seguintes políticas organizacionais:

10.1.1 P1 – Política de Segurança da Informação: Estabelece o mandato de base para investigação, controlo da evidência e cumprimento da legislação aplicável.

10.1.2 P5 – Política de Gestão de Alterações: Assegura que os sistemas sob investigação não são alterados durante processos forenses ativos.

10.1.3 P14 – Política de Retenção e Eliminação de Dados: Regula a eliminação segura e os períodos de retenção da evidência e dos dados relacionados com casos.

10.1.4 P18 – Política de Controlos Criptográficos: Define requisitos de cifragem para armazenamento e transferência de dados sensíveis ou com valor probatório.

10.1.5 P22 – Política de Registo e Monitorização: Assegura a disponibilidade de registos de eventos e telemetria para recolha de evidência e correlação forense.

10.1.6 P30 – Política de Resposta a Incidentes: Define a triagem de incidentes e as vias de escalonamento em que os procedimentos forenses são acionados.

10.1.7 P33 – Política de Auditoria e Monitorização da Conformidade: Valida o cumprimento dos protocolos forenses e dos requisitos da cadeia de custódia através de auditorias regulares.

11. Normas e referenciais aplicáveis

11.1 Esta política está alinhada com normas internacionais de análise forense e de tratamento de incidentes, assegurando a integridade da evidência, a sua defensabilidade jurídica e a conformidade em múltiplas jurisdições.

11.2 ISO/IEC 27001

11.2.1 Cláusula 8.1 – Suporta o controlo operacional da preparação forense e dos procedimentos de evidência.

11.3 ISO/IEC 27002

11.3.1 Controlo 5.25 do Anexo A – Responsabilidades na gestão de incidentes: Exige papéis definidos para o tratamento de incidentes de segurança da informação e investigações.

11.3.2 Controlo 5.26 do Anexo A – Reporte de eventos de segurança da informação: Suporta a recolha de artefactos relacionados com eventos como evidência.

11.3.3 Controlo 5.27 do Anexo A – Resposta a incidentes de segurança da informação: Impõe remediação e investigação estruturadas e orientadas pela evidência.

11.3.4 Controlo 8.27 do Anexo A – Desenvolvimento seguro e análise forense (quando aplicável): Aborda a proteção de sistemas e ferramentas durante investigações.

11.4 ISO/IEC 27035:2016 (Partes 1 e 3)

11.4.1 Descreve os princípios de deteção de incidentes, resposta e preparação forense, incluindo planeamento, cadeia de custódia e gestão da evidência de incidentes.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 a IR-9, AU-6, PL-2: Define requisitos estruturados para planeamento, deteção, análise, contenção e resposta a incidentes de segurança. Suporta a recolha e a auditabilidade da evidência (AU-6) e assegura o alinhamento com os planos de segurança e privacidade dos sistemas (PL-2) durante investigações forenses.

11.6 NIST SP 800-86

11.6.1 Fornece orientações sobre a integração de processos forenses no ciclo de vida alargado de resposta a incidentes e sobre a garantia de preparação forense.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Centra-se nas melhores práticas para adquirir, preservar e analisar evidência de suportes digitais e dispositivos móveis de forma juridicamente defensável.

11.8 RGPD da UE (2016/679)

11.8.1 Artigo 5.º – Princípios relativos ao tratamento de dados pessoais: Aplica-se a evidência que contenha dados pessoais ou sensíveis, assegurando minimização e limitação da finalidade.

11.8.2 Artigos 33–34 – Notificação de violação de dados: Os dados forenses suportam o cumprimento das obrigações de notificação de violação e dos processos de divulgação legal.

11.9 Diretiva NIS2 da UE (2022/2555)

11.9.1 Artigo 23 – Obrigações de reporte: A documentação e as conclusões forenses suportam relatórios de incidente exatos e atempados às autoridades competentes.

11.10 DORA da UE (2022/2554)

11.10.1 Artigo 17 – Reporte de incidentes relacionados com TIC: Exige análise de causa-raiz detalhada e registos com valor probatório relativos a incidentes relevantes relacionados com TIC, em especial no setor financeiro.

11.11 COBIT 2019

11.11.1 DSS01.07 – Gerir incidentes de segurança: Determina a documentação de incidentes e o rigor investigatório.

11.11.2 DSS05.04 – Gerir investigações de segurança: Enfatiza a preservação da evidência digital e o apoio a ações disciplinares e legais.