					Insira aqui a designação da entidade jurídica registada							
Número do documento: P31S					Título do documento: **Política de Recolha de Evidência e Preparação 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**

Aviso legal (direitos de autor e restrições de utilização)

(C) 2025 Clarysec LLC. All rights reserved.

Este documento é propriedade intelectual da Clarysec LLC. Nenhuma parte deste documento pode ser copiada, reutilizada, distribuída ou modificada para fins comerciais ou de implementação sem autorização prévia, expressa e por escrito.

A utilização não autorizada é estritamente proibida e pode dar origem a ações legais.

Para efeitos de licenciamento, contacte: info@clarysec.com

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 6.1, 6.3, 8	Planeamento baseado no risco, ações de melhoria e controlos operacionais para a integridade da evidência
ISO/IEC 27002:2022	Controlos 5.24–5.27	Orienta o tratamento seguro, as revisões pós-incidente e as melhorias baseadas em evidência
ISO/IEC 27035-3:2016	Cláusulas 6.3, 6.4, 7	Assegura o planeamento adequado, a recolha lícita e o tratamento seguro da evidência digital, com documentação da cadeia de custódia
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Preparação forense, proteção de registos de auditoria e integração eficaz na resposta a incidentes
RGPD da UE	Artigos 33, 34	Documentação e rastreabilidade de violações de dados pessoais
Diretiva NIS2 da UE	Artigo 23	Notificação rastreável de incidentes e tratamento seguro da evidência
DORA da UE	Artigo 17(1), 17(2)	Assegura a recolha, o armazenamento e a retenção de evidência para incidentes relacionados com TIC, a robustez forense e as solicitações de informação regulamentares
COBIT 2019	DSS05.06, DSS05.07	Registo fiável e tratamento estruturado da evidência para investigações seguras e auditáveis

1. Finalidade

1.1. Esta política define a forma como a organização trata a evidência digital relacionada com incidentes de segurança, violações de dados ou investigações internas. Assegura que a evidência é recolhida, armazenada e preservada de forma juridicamente robusta e apta a demonstrar conformidade em auditoria, apoiando tanto a tomada de decisão interna como eventuais ações externas.

1.2. A política permite às pequenas organizações proteger a integridade de registos, ficheiros e imagens de sistema, demonstrando a devida diligência ao abrigo da ISO/IEC 27001, do RGPD da UE e de normas relacionadas.

1.3. A política suporta a preparação forense sem exigir recursos técnicos avançados nem uma equipa de TI a tempo inteiro, através da definição de responsabilidades, processos e requisitos de retenção claros.

2. Âmbito

2.1. Esta política aplica-se a:

2.1.1. Todos os trabalhadores, prestadores externos de serviços de TI e consultores externos envolvidos na resposta a incidentes, investigação ou análise de violações

2.1.2. Todos os sistemas da empresa, incluindo computadores portáteis, dispositivos móveis, servidores, contas de correio eletrónico, plataformas SaaS e armazenamento na nuvem (por exemplo, Microsoft 365, Google Workspace)

2.1.3. Qualquer evento que exija evidência para medidas disciplinares internas, defesa jurídica, pedidos de indemnização junto de seguradoras ou interação com reguladores

2.2. Isto inclui eventos reais e suspeitos que envolvam:

2.2.1. Fuga de dados

2.2.2. Ameaça interna ou utilização indevida

2.2.3. Violações de segurança (por exemplo, malware, acesso não autorizado)

2.2.4. Reclamações de clientes que exijam validação digital

2.2.5. Solicitações de informação por parte de reguladores ou autoridades de aplicação da lei

3. Objetivos

3.1. Assegurar que toda a evidência é recolhida e tratada de forma a manter a sua integridade, autenticidade e cadeia de custódia.

3.2. Prevenir a modificação acidental, eliminação ou tratamento inadequado de registos, ficheiros ou imagens de sistema que possam ser necessários para investigações.

3.3. Estabelecer uma abordagem consistente e auditável à gestão da evidência que cumpra as expectativas legais e regulamentares (por exemplo, notificação de violação ao abrigo do RGPD, rastreabilidade exigida pela NIS2).

3.4. Definir papéis e responsabilidades claros para assegurar a recolha rápida, segura e legalmente conforme de evidência durante incidentes de segurança.

3.5. Apoiar a preparação forense ao nível das PME, minimizando a complexidade e evitando perturbações nas operações do dia a dia.

4. Papéis e responsabilidades

4.1. Diretor-Geral (GM)

4.1.1. Aprova todas as investigações formais que exijam recolha de evidência.

4.1.2. Revê e aprova formalmente os relatórios de incidente que envolvam potenciais ações jurídicas ou disciplinares.

4.1.3. Decide se devem ser notificadas a assessoria jurídica externa ou as entidades reguladoras.

4.1.4. Assegura que a política é revista e atualizada regularmente.

4.2. Prestador de suporte de TI / administrador de sistemas

4.2.1. Recolhe e preserva evidência digital de acordo com procedimentos seguros.

4.2.2. Documenta as marcas temporais, os detalhes dos sistemas e as etapas de tratamento.

4.2.3. Protege todos os materiais recolhidos num local seguro.

4.2.4. Apoia a análise forense, quando necessário.

[... 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. Revisão anual da política

9.1.1. Esta política deve ser revista pelo menos uma vez a cada 12 meses pelo Diretor-Geral (GM) para confirmar:

9.1.1.1. O cumprimento dos controlos do Anexo A da ISO/IEC 27001

9.1.1.2. A relevância contínua para as plataformas digitais e os serviços de TI atuais

9.1.1.3. A adequação dos procedimentos de registo, retenção de evidência e preparação forense

9.2. Eventos desencadeadores de revisão da política

9.2.1. A política deve também ser revista e atualizada após:

9.2.1.1. Qualquer incidente relevante que exija recolha de evidência

9.2.1.2. Uma auditoria sem êxito ou uma solicitação regulatória em que a integridade da evidência tenha sido questionada

9.2.1.3. A adoção de novas ferramentas ou procedimentos de resposta a incidentes ou de monitorização de sistemas

9.2.1.4. Alterações legais (por exemplo, orientações atualizadas do RGPD da UE ou da NIS2)

9.3. Aprovação e distribuição de alterações

9.3.1. Todas as alterações devem ser revistas e aprovadas pelo Diretor-Geral (GM)

9.3.2. A versão atualizada deve ser partilhada com:

9.3.2.1. Prestadores externos de serviços de TI e consultores envolvidos em investigações

9.3.2.2. Quaisquer trabalhadores com responsabilidades de administração de sistemas

9.3.3. Deve ser mantida uma cópia atualizada no arquivo de políticas da empresa e disponibilizada aos auditores mediante solicitação

10. Políticas relacionadas e interligações

10.1. Esta política é interdependente com as seguintes políticas alinhadas com PME:

10.1.1. P2S – Política de Papéis e Responsabilidades de Governação: estabelece a autoridade sobre investigações de incidentes, decisões relativas à evidência e escalonamento jurídico.

10.1.2. P4S – Política de Controlo de Acesso: assegura que apenas pessoal autorizado pode aceder a sistemas e registos sensíveis durante investigações.

10.1.3. P22S – Política de Registo e Monitorização: fornece os dados brutos utilizados como evidência forense e estabelece requisitos de retenção, controlo de acesso e registo.

10.1.4. P30S – Política de Resposta a Incidentes: desencadeia a necessidade de recolha de evidência e define o fluxo operacional que conduz à preservação forense.

10.1.5. P17S – Política de Proteção de Dados e Privacidade: assegura que quaisquer dados pessoais recolhidos como evidência são tratados licitamente ao abrigo do RGPD da UE e de regulamentos relacionados.

10.2. Estas políticas funcionam em conjunto para apoiar a defensabilidade jurídica, a integridade da investigação e a plena capacidade de demonstrar conformidade em auditoria ao abrigo da ISO/IEC 27001:2022.

11. Normas e referenciais aplicáveis

11.1. ISO/IEC 27001

11.1.1. Cláusula 6.1 – O planeamento baseado no risco inclui a preparação da resposta e os procedimentos relativos à evidência.

11.1.2. Cláusula 6.3 – Suporta ações de melhoria com base em evidência proveniente de incidentes.

11.1.3. Cláusula 8.1 – Exige controlos operacionais para a integridade da evidência.

11.2. ISO/IEC 27002

11.2.1. Controlos 5.24–5.27 – Orientam o tratamento seguro, as revisões pós-incidente e as melhorias baseadas em evidência.

11.3. ISO/IEC 27035-3

11.3.1. Cláusulas 6.3, 6.4 e 7.3 para assegurar o planeamento adequado, a recolha lícita e o tratamento seguro da evidência digital durante a resposta a incidentes, incluindo a preservação e a documentação da cadeia de custódia.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 e AU-12 asseguram a preparação forense, a proteção de registos de auditoria e a integração eficaz da recolha de evidência no ciclo de vida da resposta a incidentes

11.5. NIST SP 800-86

11.5.1. Define boas práticas para aquisição, análise e proteção de evidência digital durante a resposta a incidentes.

11.6. RGPD da UE

11.6.1. Artigos 33–34 – Exigem documentação e rastreabilidade de incidentes e evidência quando são reportadas violações de dados pessoais.

11.7. Diretiva NIS2 da UE (2022/2555)

11.7.1. Artigo 23 – Exige notificação rastreável de incidentes e tratamento seguro da evidência para entidades essenciais e importantes.

11.8. DORA da UE

11.8.1. Artigo 17(1) – Assegura que a evidência relacionada com incidentes de TIC é recolhida e armazenada de modo a suportar investigações forenses.

11.8.2. Artigo 17(2) – Exige que as entidades financeiras retenham todos os dados e registos relevantes associados a eventos de segurança, em alinhamento com a robustez forense e as solicitações de informação regulamentares.

11.9. COBIT 2019

11.9.1. DSS05.06 – Monitorizar, detetar e reportar incidentes: enfatiza o registo fiável para apoio à investigação.

11.9.2. DSS05.07 – Investigar e agir sobre incidentes: exige tratamento estruturado da evidência para permitir investigações seguras e auditáveis.