| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insira aqui a designação da entidade jurídica registada | | | | | | | |
| Número do documento:<br>P30S | | | | | Título do documento:<br>**Política de Resposta a Incidentes** | | | | | | | |
| Versão:<br>1.0 | | Data de entrada em vigor:<br>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 | Cláusulas 6.1, 6.3, 8 | Gestão de incidentes, melhoria contínua, controlo operacional |
| ISO/IEC 27002:2022 | Controlos 5.24, 5.25 | Deteção de incidentes, preparação e aprendizagem |
| NIST SP 800-53 Rev.5 | IR-4, IR-5, IR-6 | Tratamento, monitorização e comunicação de incidentes |
| RGPD da UE | Artigo 33 | Requisitos de notificação de violações de dados pessoais |
| Diretiva NIS2 da UE | Artigo 23 | Notificação obrigatória de incidentes de cibersegurança |
| DORA da UE | Artigo 17 | Gestão de incidentes relacionados com TIC |
| COBIT 2019 | DSS02, DSS04 | Gestão de serviços/incidentes e continuidade |

**1. Finalidade**

1.1. Esta política define a forma como a organização deteta, comunica e responde a incidentes de segurança da informação que afetem os seus sistemas digitais, dados ou serviços.

1.2. Esta política permite à organização minimizar danos, proteger os dados dos clientes e cumprir obrigações regulamentares, incluindo o requisito de notificação de violações no prazo de 72 horas previsto no RGPD da UE.

1.3. Esta política assegura a definição clara de responsabilidades, etapas de comunicação e acompanhamento pós-incidente, incluindo em pequenas organizações sem uma equipa de segurança dedicada.

**2. Âmbito**

**2.1. Esta política aplica-se a:**

2.1.1. Todos os trabalhadores, contratados e prestadores externos de serviços de TI

2.1.2. Todos os sistemas e serviços geridos pela empresa, incluindo websites, plataformas na nuvem, dispositivos móveis, computadores portáteis e contas de correio eletrónico

**2.1.3. Todos os tipos de incidentes, incluindo:**

2.1.3.1. Acesso não autorizado a dados ou sistemas

2.1.3.2. Infeções por malware ou ransomware

2.1.3.3. Tentativas de phishing ou engenharia social

2.1.3.4. Indisponibilidade de sistemas devido a ciberataque ou utilização indevida

2.1.3.5. Divulgação acidental ou eliminação de informação sensível

2.1.3.6. Perda ou furto de dispositivos empresariais ou suportes de armazenamento

**3. Objetivos**

3.1. Estabelecer um processo claro para identificação e escalonamento de incidentes de segurança.

3.2. Assegurar que os incidentes são comunicados, registados e tratados dentro de prazos predefinidos.

3.3. Permitir a contenção célere dos danos, a recuperação de dados e o restabelecimento dos serviços.

3.4. Assegurar que as partes afetadas (por exemplo, clientes e reguladores) são notificadas sempre que tal seja legalmente exigido.

3.5. Prevenir recorrências através da análise de causa raiz, da implementação de ações corretivas e da melhoria da política.

3.6. Permitir às PME cumprir os requisitos de certificação ISO/IEC 27001 e demonstrar responsabilização durante auditorias.

## 4. Papéis e responsabilidades

### 4.1. Diretor-Geral (GM)

4.1.1. É responsável por esta política e assegura a sua implementação.

4.1.2. Supervisiona as atividades de resposta a incidentes e aprova notificações a reguladores ou clientes.

4.1.3. Revê os relatórios pós-incidente e assegura que a política é atualizada quando necessário.

4.1.4. Pode delegar funções de coordenação, mantendo, no entanto, a responsabilização.

### 4.2. Prestador de suporte de TI / administrador de sistemas (interno ou externo)

4.2.1. Deteta e investiga potenciais incidentes de segurança.

4.2.2. Implementa ações de contenção e recuperação (por exemplo, desativar acessos, restaurar cópias de segurança).

4.2.3. Notifica o Diretor-Geral (GM) de todos os incidentes confirmados ou suspeitos no prazo de 1 hora após a sua deteção.

4.2.4. Mantém um registo de incidentes com data e hora, avaliação de impacto e ações de resposta.

[ ... 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 programada

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

9.1.1.1. Alinhamento com os controlos da ISO/IEC 27001:2022

9.1.1.2. Capacidade de resposta a novas ameaças, riscos e incidentes

9.1.1.3. Cumprimento continuado das obrigações legais e contratuais (por exemplo, RGPD da UE, DORA da UE)

### 9.2. Eventos desencadeadores

**9.2.1. A política deve igualmente ser revista e atualizada após:**

9.2.1.1. Qualquer incidente de severidade elevada ou notificação regulamentar

9.2.1.2. Introdução de nova infraestrutura de TI ou alterações aos sistemas

9.2.1.3. Alterações aos requisitos legais relacionados com violações de segurança

### 9.3. Documentação da revisão e distribuição

9.3.1. Todas as revisões e alterações devem ser documentadas no registo de alterações da política

9.3.2. As versões atualizadas devem ser distribuídas a todos os trabalhadores, fornecedores e prestadores de suporte de TI envolvidos na segurança ou nas operações dos sistemas

9.3.3. Deve ser mantida evidência da sensibilização dos trabalhadores (por exemplo, atas de reunião ou confirmações por correio eletrónico) para demonstrar conformidade em auditoria

## 10. Políticas relacionadas e articulações

**10.1. Esta política deve ser aplicada em articulação com as seguintes políticas SME:**

10.1.1. P1S – Política de Segurança da Informação: Define as expectativas gerais para manter a confidencialidade, integridade e disponibilidade durante as operações, incluindo o tratamento de incidentes.

10.1.2. P2S – Política de Papéis e Responsabilidades de Governação: Estabelece estruturas de autoridade e responsabilização para deteção, comunicação e escalonamento de incidentes.

10.1.3. P4S – Política de Controlo de Acesso: Permite a revogação imediata de direitos de acesso durante ações de resposta a incidentes.

10.1.4. P8S – Política de Sensibilização e Formação em Segurança da Informação: Assegura que todos os trabalhadores conseguem identificar e comunicar incidentes de segurança de forma eficaz.

10.1.5. P17S – Política de Proteção de Dados e Privacidade: Orienta os procedimentos legais de notificação de violações ao abrigo do RGPD da UE e apoia o cumprimento regulamentar durante incidentes.

10.1.6. P22S – Política de Registo de Eventos e Monitorização: Disponibiliza as ferramentas e a visibilidade necessárias para detetar, analisar e auditar eventos de segurança.

10.1.7. P31S – Política de Recolha de Evidência e Análise Forense: Apoia a investigação e a defensabilidade jurídica das ações relacionadas com incidentes, orientando o tratamento adequado da evidência.

10.2. Estas políticas estabelecem, em conjunto, o quadro operacional da PME para detetar, responder e recuperar de incidentes de segurança da informação.

## 11. Normas e referenciais aplicáveis

### 11.1. ISO/IEC 27001

11.1.1. Cláusula 6.1 – Exige o planeamento do tratamento de riscos, incluindo a preparação para incidentes.

11.1.2. Cláusula 6.3 – Apoia a melhoria contínua através das lições aprendidas com eventos de segurança.

11.1.3. Cláusula 8.1 – Dá ênfase ao controlo operacional para gerir incidentes e interrupções.

### 11.2. ISO/IEC 27002

11.2.1. Controlo 5.24 – Exige uma abordagem estruturada para comunicar, avaliar e responder a incidentes de segurança da informação.

11.2.2. Controlo 5.25 – Incide na aprendizagem com incidentes para melhorar a preparação futura e a resiliência dos sistemas.

### 11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Define procedimentos de tratamento de incidentes, incluindo contenção e recuperação.

11.3.2. IR-5 – Estabelece requisitos para monitorização e análise de incidentes.

11.3.3. IR-6 – Determina protocolos de comunicação interna e externa de incidentes.

### 11.4. RGPD da UE

11.4.1. Artigo 33 – Exige a notificação de violações de dados pessoais aos reguladores no prazo de 72 horas, com detalhe sobre o âmbito e a mitigação.

### 11.5. Diretiva NIS2 da UE (2022/2555)

11.5.1. Artigo 23 – Exige que entidades essenciais e importantes notifiquem as autoridades competentes de incidentes significativos, utilizando formatos normalizados de comunicação.

### 11.6. Regulamento DORA da UE (2022/2554)

11.6.1. Artigo 17 – Exige que as entidades financeiras classifiquem, comuniquem e acompanhem incidentes e interrupções relacionados com TIC.

**11.7. COBIT 2019**

11.7.1. DSS02 – Gerir Pedidos de Serviço e Incidentes: orienta o tratamento eficaz de incidentes operacionais e de segurança em alinhamento com os objetivos de governação.

11.7.2. DSS04 – Gerir Continuidade: relaciona a resposta a incidentes com estratégias mais amplas de continuidade e recuperação.