

Diário de resposta a incidentes

**Instruções**

O **Diário do Responsável pelo Tratamento de Incidentes** é uma ferramenta usada por profissionais de segurança cibernética para **registrar e documentar cada passo na investigação e resposta a um incidente de segurança**, como ataques de ransomware, invasões ou vazamentos de dados.

Ele ajuda a manter um histórico detalhado do que aconteceu, quando aconteceu, quem foi afetado, quais ferramentas foram usadas na resposta e quais foram as decisões tomadas. Isso é essencial para:

* **Análise posterior do incidente**
* **Prevenção de futuros ataques**
* **Cumprimento de obrigações legais e regulatórias**
* **Treinamento e aprendizado contínuo**

|  |  |
| --- | --- |
| **Data:**  23/06/2025 | **Entrada:**  1 |
| Descrição | Incidente de ransomware em uma clínica de saúde que causou paralisação dos serviços e criptografia de dados sensíveis. |
| Ferramenta(s) usada(s) | Nenhuma ferramenta mencionada explicitamente no cenário. Ferramentas como EDR, antivírus e logs de e-mail provavelmente serão usadas na análise posterior. |
| Os 5 W's | Capture os 5 W's de um incidente.   * **Quem causou o incidente? Um grupo de hackers antiéticos conhecido por atacar organizações de saúde e transporte.** * **O que aconteceu? A clínica foi alvo de um ataque de ransomware, iniciado por e-mails de phishing contendo anexos maliciosos que, quando abertos, instalaram malware e criptografaram os arquivos da empresa.** * **Quando ocorreu o incidente? Na terça-feira pela manhã, por volta das 9h.** * **Onde aconteceu o incidente? Em uma pequena clínica de saúde nos Estados Unidos.** * **Por que o incidente aconteceu? Porque funcionários abriram anexos de e-mails de phishing, permitindo a instalação do ransomware.** |
| Notas adicionais | Esse incidente destaca a necessidade urgente de treinamento contra phishing e da implementação de medidas preventivas, como filtros de e-mail, backups regulares e planos de resposta a incidentes. Vale investigar se a clínica estava em conformidade com regulações como a HIPAA. |

|  |  |
| --- | --- |
| **Data:**  Registre a data do lançamento contábil manual. | **Entrada:**  Registre o número do lançamento contábil manual. |
| Descrição | Forneça uma breve descrição sobre o lançamento contábil manual. |
| Ferramenta(s) usada(s) | Liste todas as ferramentas de segurança cibernética que foram usadas. |
| Os 5 W's | Capture os 5 W's de um incidente.   * **Quem** causou o incidente? * **O que** aconteceu? * **Quando** ocorreu o incidente? * **Onde** aconteceu o incidente? * **Por que** o incidente aconteceu? |
| Notas adicionais | Inclua quaisquer pensamentos, perguntas ou descobertas adicionais. |

|  |  |
| --- | --- |
| **Data:**  Registre a data do lançamento contábil manual. | **Entrada:**  Registre o número do lançamento contábil manual. |
| Descrição | Forneça uma breve descrição sobre o lançamento contábil manual. |
| Ferramenta(s) usada(s) | Liste todas as ferramentas de segurança cibernética que foram usadas. |

|  |  |
| --- | --- |
| Os 5 W's | Capture os 5 W's de um incidente.   * **Quem** causou o incidente? * **O que** aconteceu? * **Quando** ocorreu o incidente? * **Onde** aconteceu o incidente? * **Por que** o incidente aconteceu? |
| Notas adicionais | Inclua quaisquer pensamentos, perguntas ou descobertas adicionais. |

|  |  |
| --- | --- |
| **Data:**  Registre a data do lançamento contábil manual. | **Entrada:**  Registre o número do lançamento contábil manual. |
| Descrição | Forneça uma breve descrição sobre o lançamento contábil manual. |
| Ferramenta(s) usada(s) | Liste todas as ferramentas de segurança cibernética que foram usadas. |
| Os 5 W's | Capture os 5 W's de um incidente.   * **Quem** causou o incidente? * **O que** aconteceu? * **Quando** ocorreu o incidente? * **Onde** aconteceu o incidente? * **Por que** o incidente aconteceu? |
| Notas adicionais | Inclua quaisquer pensamentos, perguntas ou descobertas adicionais. |

|  |  |
| --- | --- |
| **Data:**  Registre a data do lançamento contábil manual. | **Entrada:**  Registre o número do lançamento contábil manual. |
| Descrição | Forneça uma breve descrição sobre o lançamento contábil manual. |
| Ferramenta(s) usada(s) | Liste todas as ferramentas de segurança cibernética que foram usadas. |
| Os 5 W's | Capture os 5 W's de um incidente.   * **Quem** causou o incidente? * **O que** aconteceu? * **Quando** ocorreu o incidente? * **Onde** aconteceu o incidente? * **Por que** o incidente aconteceu? |
| Notas adicionais | Inclua quaisquer pensamentos, perguntas ou descobertas adicionais. |

|  |  |
| --- | --- |
| **Data:**  Registre a data do lançamento contábil manual. | **Entrada:**  Registre o número do lançamento contábil manual. |

|  |  |
| --- | --- |
| Descrição | Forneça uma breve descrição sobre o lançamento contábil manual. |
| Ferramenta(s) usada(s) | Liste todas as ferramentas de segurança cibernética que foram usadas. |
| Os 5 W's | Capture os 5 W's de um incidente.   * **Quem** causou o incidente? * **O que** aconteceu? * **Quando** ocorreu o incidente? * **Onde** aconteceu o incidente? * **Por que** o incidente aconteceu? |
| Notas adicionais | Inclua quaisquer pensamentos, perguntas ou descobertas adicionais. |

Precisa de outro modelo de lançamento contábil?

Se você quiser adicionar mais entradas de diário, copie uma das tabelas acima e cole-a no modelo para usar em entradas futuras.

Reflexos/Notas: Grave notas adicionais.