**Diário do Responsável pelo Incidente**

**Data:** 9 de fevereiro de 2025  
**Entrada:** #1

**Descrição:**  
Documentação de um incidente de segurança cibernética envolvendo um ataque de ransomware em uma pequena clínica de saúde.

**Ferramenta(s) utilizada(s):**  
Nenhuma.

**As 5 Perguntas (5 W's):**

* **Quem:** Um grupo organizado de hackers antiéticos conhecido por atacar os setores de saúde e transporte.
* **O que:** Um incidente de segurança com ransomware que criptografou os arquivos da empresa e exigiu um resgate.
* **Onde:** Uma pequena clínica de saúde nos EUA.
* **Quando:** Terça-feira, às 9h00.
* **Por que:** O incidente ocorreu porque os hackers conseguiram acesso por meio de um ataque de phishing. Após obterem acesso, implantaram o ransomware, criptografando arquivos essenciais. A motivação dos atacantes parece ser financeira, pois deixaram uma nota de resgate exigindo uma grande quantia de dinheiro pela chave de descriptografia.

**Notas adicionais:**

1. Como a clínica poderia evitar que um incidente como esse ocorresse novamente?
2. A clínica deveria pagar o resgate para recuperar a chave de descriptografia?
3. A implementação de treinamentos sobre phishing, soluções de detecção e resposta em endpoint (EDR) e backups seguros poderia mitigar ataques futuros.