**Pesquise sobre outros casos de grande repercussão:**

* Bug do Milênio
* Queda do sistema de informática da British Airways
* Interrupção do Serviço AWS S3 da Amazon
* CrowdStrike e Microsoft: entenda a interrupção cibernética que deu 'tela azul' e vários países

**Responda as seguintes perguntas:**

1. Quais são os principais vilões nessas histórias?

* **Bug do Milênio (Y2K)**: O “vilão” foi um **erro de lógica** no armazenamento de datas (uso de apenas dois dígitos para o ano), uma escolha técnica e contábil dos desenvolvedores dos anos 1960‑70, e a consequência da **falta de atualizações contínuas**.
* **British Airways (2017)**: A falha foi causada por uma **sobre-sobrecarga no retorno de energia** que danificou servidores num data center. A situação piorou porque o plano de recuperação e redundância **não funcionou adequadamente**. Houve erro humano no manejo da infraestrutura.
* **AWS S3 (2017)**: Um operador executou um comando com um parâmetro errado, removendo **mais servidores que o previsto**, causando falha em cascata.
* **CrowdStrike + Microsoft (2024)**: Uma **atualização mal testada** do agente Falcon causou um erro de leitura de memória (“out-of-bounds”) que provocou crash em milhões de PCs com Windows.

1. O que poderia ser feito para evitar tais problemas?

* **Testes rigorosos** e **análise estática/dinâmica de segurança**, especialmente para updates que acessam kernel.
* Implantar **controle de versões**, janelas de liberação (“canary deployments”), e plano de reversão automático.
* **Redundância real e comprovada** (backup automático, failover) e simulações de desastre periódico.
* Em ambientes críticos, **automatizar verificações**, restrições de comandos sensíveis e **auditorias constantes** de scripts usadas em manutenção.
* No Y2K, a migração gradual proativa foi eficaz — destaca a importância da manutenção de longo prazo.

1. Como você avalia a qualidade desses softwares?

Todas as plataformas envolvidas eram robustas e amplamente usadas:

* O bug Y2K não causou crises graves, pois muitos sistemas foram atualizados a tempo.
* AWS S3 e Falcon são produtos de empresas renomadas, mas incidentes mostram que mesmo fornecedores de elite podem falhar. Qualidade alta, mas não infalível.
* Sistemas da British Airways já foram criticados por negligenciar modernização, sugerindo baixa eficácia na gestão de risco.

1. Qual é a relação entre os casos anteriores?

* Ariane‑501 (1996): Falha por overflow num tipo de dados convertido incorretamente.
* Therac‑25 (década de 1980): Letais doses de radiação por falta de validações e redundância lógica.
* Windows 98 (COMDEX 98): Demo ao vivo que travou, devido a falha de hardware/driver causando crash.
* Em comum entre os casos:
* Erro humano e presunção de cenários improváveis, sem testes completos.
* Falta de proteção contra casos extremos.
* Consequências graves geradas pela confiança excessiva no sistema.

1. Quais foram os impactos?

* **Y2K**: Pânico generalizado, custos bilionários com atualizações e auditorias, mas impacto real foi mínimo.
* **British Airways 2017**: ~75.000 passageiros afetados, cancelamentos por dias, custos altos e danos à reputação.
* **AWS S3 2017**: Intermitências por ~4 h na região us-east-1, economia global afetada (US$150 milhões só nas empresas da S&P 500).
* **CrowdStrike 2024**: ~8 a 8.5 milhões de PCs afetados, interrupção em bancos, voos, hospitais. Companhias aéreas, como Delta perderam ~US$500 milhões. Polêmica regulatória sobre acesso ao kernel. A CrowdStrike foi processada, mas manteve clientes e capitalização

**Resumo final**

Esses incidentes demonstram que inclusive sistemas robustos sofrem quando:

1. Erro humano, comandos errados ou testes insuficientes são feitos.
2. Ambientes críticos exigem redundância real e automação resistente.
3. Testes extremos e simulações de falhas deveriam ser rotina, não exceção**.**