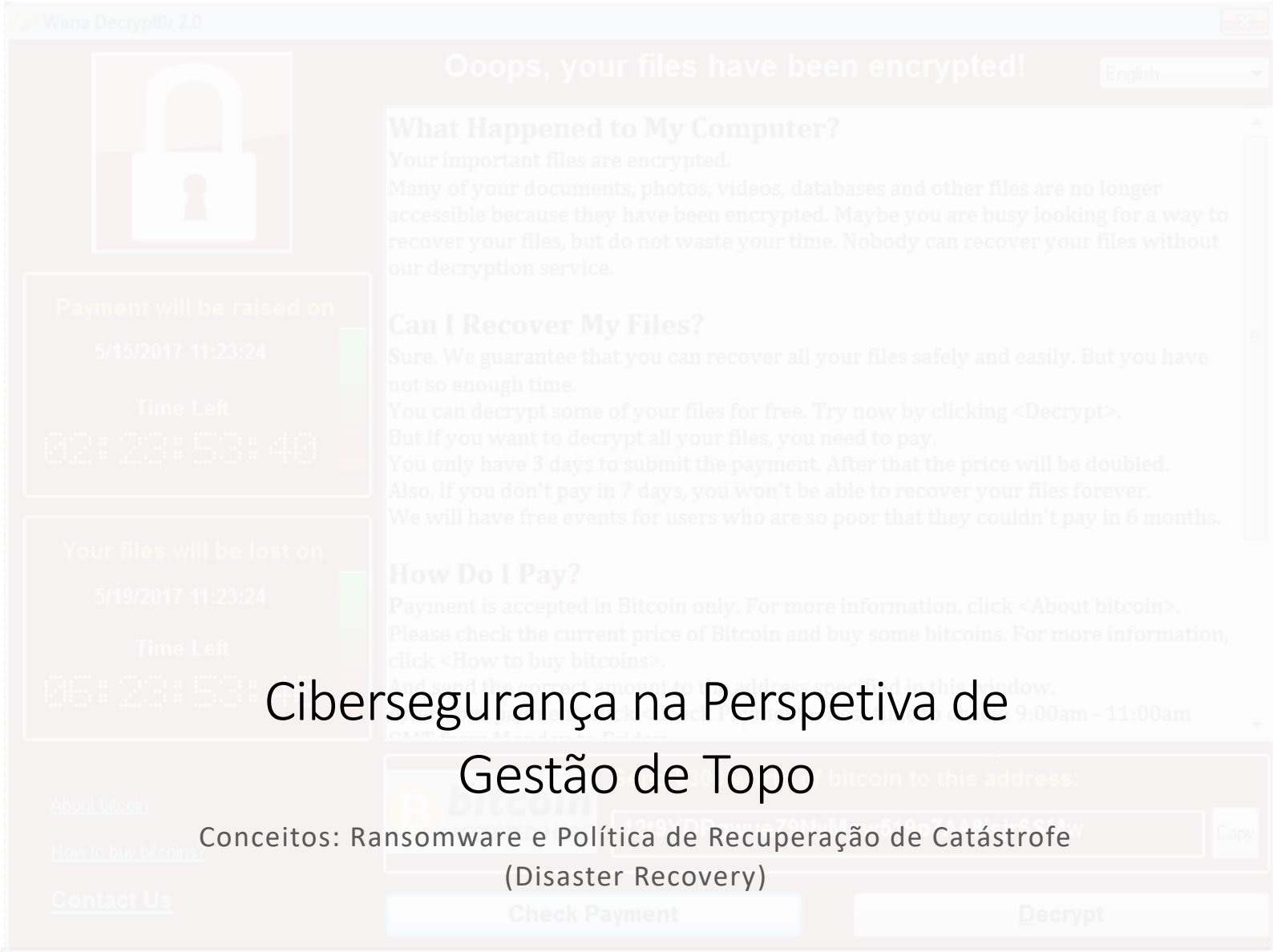


Cibersegurança na Perspetiva de Gestão de Topo

Conceitos: Ransomware e Política de Recuperação de Catástrofe (Disaster Recovery)

Unidade Curricular: Sistema de Informação para a Gestão (MBA34)

Semestre: 1.º Semestre – 2025/2026

Aluno: Bruno Silva

15/12/2025

Cibersegurança na Perspetiva de Gestão de Topo

1. Introdução

A cibersegurança tornou-se um tema central na gestão de topo por três razões: (i) a crescente dependência dos processos críticos em sistemas digitais, (ii) o aumento da sofisticação e frequência do cibercrime, e (iii) o impacto real em continuidade de negócio, reputação e, no setor da saúde, **segurança do doente**. Neste contexto, este trabalho aprofunda dois conceitos abordados frequentemente em programas de cibersegurança: **Ransomware** e **Política de Recuperação de Catástrofe (Disaster Recovery – DR)**.

A escolha destes temas é particularmente relevante no setor hospitalar, onde ataques a sistemas de informação podem provocar disrupções operacionais significativas e aumentar o risco clínico. Em Portugal, por exemplo, foi publicamente reportado um ataque ao **Hospital Garcia de Orta** em **26 de abril de 2022**, com condicionamentos operacionais (incluindo consultas externas) e referência a ransomware por órgãos de comunicação social.

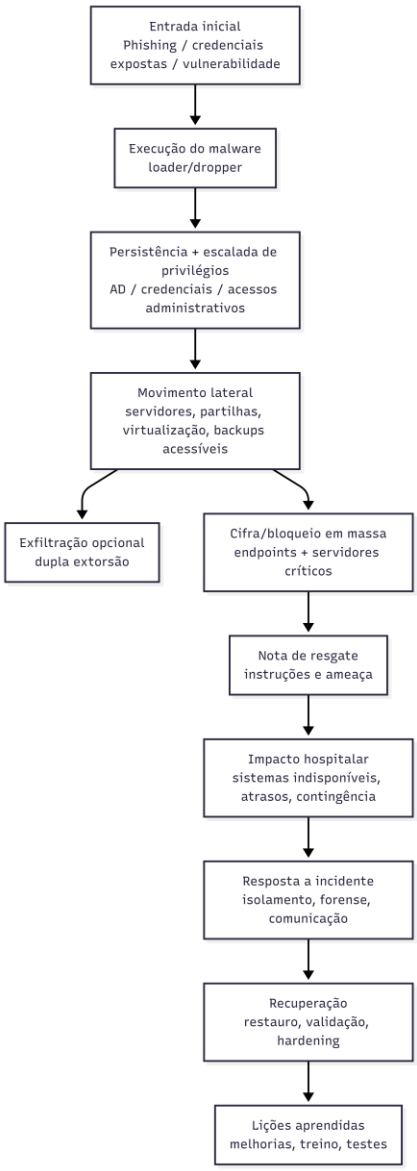
2. Conceito 1 — Ransomware

2.1 Descrição

Ransomware é um tipo de software malicioso que visa **bloquear o acesso a sistemas e/ou cifrar dados** para forçar a vítima a pagar um resgate. Em campanhas modernas é frequente a lógica de **"dupla extorsão"**: além da cifra, existe a ameaça de divulgação de dados exfiltrados.

No setor hospitalar, o impacto vai além do incómodo tecnológico. Quando sistemas clínicos e operacionais ficam indisponíveis, a organização é empurrada para processos manuais, atrasos e reagendamentos, com potenciais efeitos em diagnósticos, terapêuticas, continuidade assistencial e capacidade de resposta. Estes efeitos são coerentes com o que foi relatado publicamente no caso do Hospital Garcia de Orta, onde houve disrupções e limitações operacionais após o incidente.

2.2 Diagrama — Cadeia típica de um ataque de ransomware (exemplo Portugal: HGO, 26/04/2022)



2.3 Descrição do diagrama

- **Entrada inicial:** normalmente por **phishing** ou **credenciais comprometidas**.
- **Escalada e movimento lateral:** o objetivo é atingir contas privilegiadas e servidores críticos (ex.: diretório, ficheiros, virtualização, integrações).
- **Cifra e extorsão:** a organização perde disponibilidade e entra em modo de crise.
- **Resposta e recuperação:** isolamento, investigação, restauro e reforço de controlos para evitar reinfeção.

2.4 Análise crítica (gestão de topo)

Do ponto de vista executivo, ransomware deve ser tratado como **risco estratégico** (operacional, financeiro, reputacional e regulatório) e, em saúde, como **risco clínico**.

Decisões e responsabilidades chave:

1. **Segurança do doente e continuidade assistencial** como KPI de risco: cibersegurança não pode estar desligada de gestão de risco clínico.
2. **Política prévia sobre resgates:** a decisão de pagar ou não não pode ser improvisada "no dia". Deve existir posição e processo (jurídico, compliance, seguradora, comunicação, liderança).
3. **O custo real é o custo total do incidente**: mesmo quando não se paga, a recuperação implica custos internos (equipas, horas extra, paragens) e externos (forense, consultoria, fornecedores, reimplementação e reforço de segurança).
4. **Dependência de fornecedores e integrações:** em hospitais, a superfície de ataque inclui terceiros. Gestão de topo deve exigir requisitos contratuais de segurança, SLAs de recuperação e evidência de testes.
5. **Resiliência como requisito de gestão:** as orientações de entidades como o CNCS descrevem ransomware como cifra/roubo de dados e reforçam a importância de medidas preventivas e de preparação. C

---

3. Conceito 2 — Política de Recuperação de Catástrofe (Disaster Recovery)

3.1 Descrição

Uma **Política de Recuperação de Catástrofe (DR)** define como a organização recupera **serviços e dados críticos** após eventos disruptivos, incluindo ciberataques, incêndios, falhas de energia, inundações, furtos ou erro humano. A política deve ser:

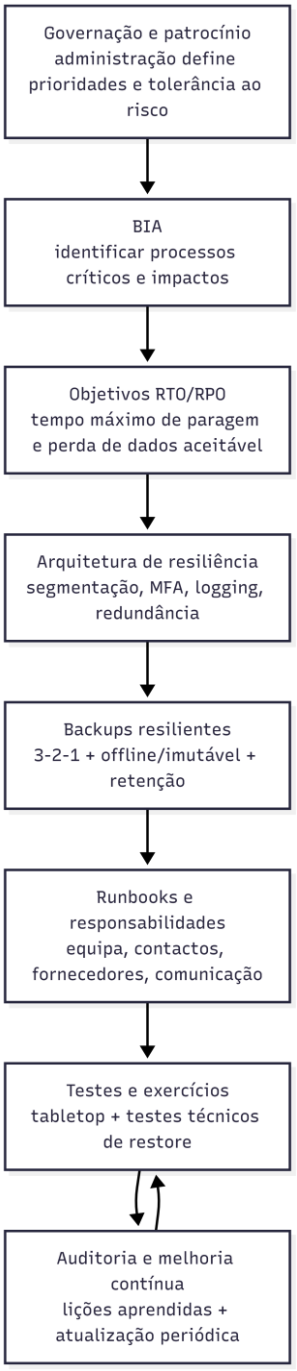
- **Eficaz:** garante restauro consistente e validado.
- **Eficiente:** cumpre tempos e perdas de dados aceitáveis com custos sustentáveis.

Referenciais reconhecidos incluem:

- **NIST SP 800-34 Rev.1** — guia de planeamento de contingência, incluindo BIA e estruturação de planos.
- **ISO/IEC 27031** — orientações para prontidão de TIC para continuidade e recuperação.

Além disso, guias operacionais anti-ransomware (ex.: CISA) sublinham que a recuperação depende de **backups offline/encriptados** e de **testes regulares de restauro**.

3.2 Diagramav— Política de DR (do planeamento ao ciclo de melhoria)



3.3 Explicação do diagrama

- **Governação:** a gestão de topo define o “quanto dói” (tolerância à paragem e perda de dados).
- **BIA (Business Impact Analysis):** identifica o que não pode falhar (em saúde: urgência, prescrição, laboratório, imagiologia, blocos, etc.).
- **RTO (Recovery Time Objective)/POR (Recovery Point Objective):** transforma ambições em métricas verificáveis.

- **Backups resilientes:** não basta "existir backup"; é essencial ter cópia offline/imutável e **testar o restauro** (há guias que reforçam explicitamente testes e integridade dos backups).
- **Runbooks e exercícios:** reduzem improviso e tempo de decisão.
- **Melhoria contínua:** DR é um ciclo, não um documento estático.

3.4 Análise crítica (gestão de topo)

1. **DR é um investimento com racional económico (probabilidade × impacto):** a gestão decide o equilíbrio entre custo e risco residual.
2. **RTO/RPO são compromissos de negócio, não de TI:** se o topo exigir "recuperar tudo em poucas horas", tem de financiar arquitetura e operações compatíveis.
3. **Evidência substitui intenção:** a pergunta executiva correta não é "temos plano?", é "quando foi o último teste completo e quais foram os tempos reais?".
4. **Integração com comunicação de crise:** numa organização com impacto público (como hospitais), comunicação interna e externa deve estar prevista no plano (stakeholders, reguladores, parceiros, doentes).
5. **Preparação para múltiplos cenários:** a política deve cobrir ciberataques e também ameaças físicas e ambientais. O ponto de maturidade é a capacidade de recuperar com controlo, mesmo sob pressão.

4. Conclusão

Ransomware e Recuperação de Catástrofe são dois lados do mesmo problema: **o ataque pode acontecer; a diferença está na capacidade de resistir e recuperar**. Em particular no setor hospitalar, a disrupção tecnológica transforma-se rapidamente em risco operacional com potenciais implicações clínicas. Assim, a perspetiva de gestão de topo deve ser pragmática: investir em prevenção, sim, mas sobretudo garantir resiliência mensurável (RTO/RPO), backups robustos, testes regulares e uma governação clara para decisões críticas.

5. Bibliografia

- ULS Almada-Seixal — Comunicado "Ataque informático HGO" (26/04/2022). ULSAS
- NIST — SP 800-34 Rev. 1: *Contingency Planning Guide for Federal Information Systems*. NIST Segurança Informática+1
- ISO — ISO/IEC 27031 (ICT readiness for business continuity). ISO+1
- CISA — *StopRansomware Guide* (backups offline + testes de restauro). CISA+1
- CNCS — Contexto atual: Ransomware. Centro Nacional de Cibersegurança

6. Mermaid code

```
flowchart TD
  A[Entrada inicial<br/>Phishing / credenciais expostas / vulnerabilidade] --> B[Execução do malware<br/>loader/dropper]
  B --> C[Persistência + escalada de privilégios<br/>AD / credenciais / acessos administrativos]
  C --> D[Movimento lateral<br/>servidores, partilhas, virtualização, backups acessíveis]
  D --> E[Exfiltração opcional<br/>dupla extorsão]
  D --> F[Cifra/bloqueio em massa<br/>endpoints + servidores críticos]
  F --> G[Nota de resgate<br/>instruções e ameaça]
  G --> H[Impacto hospitalar<br/>sistemas indisponíveis, atrasos, contingência]
  H --> I[Resposta a incidente<br/>isolamento, forense, comunicação]
  I --> J[Recuperação<br/>restauro, validação, hardening]
  J --> K[Lições aprendidas<br/>melhorias, treino, testes]
```

```
flowchart TD
  A[Governação e patrocínio<br/>administração define prioridades e tolerância ao risco] --> B[BIA<br/>identificar processos críticos e impactos]
  B --> C[Objetivos RTO/RPO<br/>tempo máximo de paragem e perda de dados aceitável]
  C --> D[Arquitetura de resiliência<br/>segmentação, MFA, logging, redundância]
  D --> E[Backups resilientes<br/>3-2-1 + offline/imutável + retenção]
  E --> F[Runbooks e responsabilidades<br/>equipa, contactos, fornecedores, comunicação]
  F --> G[Testes e exercícios<br/>tabletop + testes técnicos de restore]
  G --> H[Auditoria e melhoria contínua<br/>lições aprendidas + atualização periódica]
  H --> G
```