Exemplo: análise de risco do DEI

- **Descrição do cenário**

  - **Utilizadores**
    - 600 alunos
    - 40 docentes
    - 10 funcionários
    - NEEI, SASUC, CISUC, IPN, Quiosque, Visitantes

  - **Rede local**
    - 700 tomadas
    - backbone comutado a 1 Gbps
    - ligação comutada dos servidores a 100 Mbps
    - VLANs por áreas funcionais (alunos, docentes, administrativos, CISUC, etc.)

  - **Acesso à Internet (via CIUC)**
    - circuito de 2 Mbps
    - ligação Wireless a 2 Mbps

  - **Acesso comutado (RDIS e PSTN)**
    - 30 acessos RDIS
    - 16 acessos PSTN

Exemplo: análise de risco DEI (cont.)

- **Descrição do cenário (cont.)**
  - **Servidores**
    - + 20 servidores UNIX e NT (c/ UPS)
    - alguns expostos à Internet
    - servidor FTP de renome nacional e internacional
  - **Computadores pessoais**
    - + 300: W95, W98, W2000, WNT, MacOS
    - Software muito variado
    - Grande mobilidade
  - **Mecanismos de segurança**
    - Firewall e proxies
    - Autenticação centralizada
    - Uso de kerberos
    - Uso de Radius nos acessos do exterior
    - Uso de shadow passwords
    - Uso de mecanismos de monitorização
    - Uso frequente de mecanismos de auditoria
    - Câmaras de vigilância nas entradas do departamento
  - **Equipa técnica**
    - Um gestor sénior
    - Dois gestores juniores em parte time

Exemplo: análise de risco DEI (cont.)

- **Avaliação do potencial de ataque**
  - Acesso físico de público ao interior do edifício ? (é só entrar com um ar decidido…) **3**
  - Acesso aos recursos de estranhos à organização ? **3**
  - Suporte de serviços de comunicação para o público em geral ? (RCU, PPP, não é publico geral mas quase) **3**
  - Mais alguém para além da equipa de gestão tem acesso a privilégios de administração ? (laboratórios) **5**
  - Existe partilha de contas entre utilizadores ou contas genéricas ? (tem melhorado) **3**
  - A actividade da organização pode ser considerada controversa ? **1**
  - A actividade da organização está relacionada com a área financeira ? **1**
  - Existem servidores expostos à Internet ? **5**
  - São usadas redes públicas para dados sensíveis ? **4**
  - A actividade da organização é altamente especializada ? (investigação) **4**
  - A organização teve um crescimento muito rápido ? **4**
  - A organização tem tido muita visibilidade nos media ? (infelizmente) **3**
  - Os utilizadores são especialista de informática ? **5**

- **Total: 44 / 65 (Elevado)**

Exemplo: análise de risco DEI (cont.)

- **Bens a proteger**
  - **Hardware**
    - Computadores (+ 300)
    - Servidores (+ 30)
    - Impressoras (+ 20)
    - Equipamento de comunicações
    - Etc.
      - **Valor total:** mais de 50 M Escudos
  - **Software**
    - Sistemas operativos (+ 300)
    - MS Office (+ 100)
    - Oracle
    - Ambientes de desenvolvimento
    - Macromedia
    - Simulação, etc., etc.
      - **Valor total:** mais de 20 M Escudos
  - **Informação**
    - Administrativa
    - Documentos pessoais
    - Trabalhos académicos
    - Trabalhos científicos, etc., etc.
      - **Valor total:** indefinido mas MUITO ELEVADO

Exemplo: análise de risco DEI (cont.)

- **Bens a proteger (cont.)**
  - **Tempo**
    - **de paragem das actividades:**
      - 6 M escudos por docente por ano (média) x 40
      - 4 M escudos por funcionário por ano (média) x 10
      - 1 M escudos por aluno (média) x 600
      - Total 880 M escudos ano = 4 M escudos por dia útil = 500 c por hora
      - Custo de aula teórica (50 alunos + 1 Prof) = 100 c ?
      - Custo de aula prática (20 alunos + 1 Prof) = 50 c ?
    - **de reparação**
      - equipa técnica (600 contos mês)
  - **Outros bens**
    - Equipamento laboratorial ? Talvez ...
    - Recursos financeiros ? Sim, contas de projectos.
    - Consumíveis ? Não dependem do SI
    - Vida humana ? Só se alguém se suicidar ...
    - Imagem exterior
    - Imagem interna
    - Má preparação dos alunos, etc., etc.
      - **Valor total:** indefinido mas MUITO ELEVADO
  - **Valor global dos bens a proteger**
    - É só fazer as contas …
      - **O DEI sobrevivia a uma perda total no SI ?**

Exemplo: análise de risco do DEI (cont.)

- **Classificação das probabilidades**

	frequência	**classificação**
–	1 vez em 10000 anos	1
–	1 vez em 1000 anos	2
–	1 vez em 100 anos	3
–	1 vez em 10 anos	4
–	1 vez por ano	5
–	1 vez por mês	6
–	1 vez por semana	7
–	1 vez por dia	8
–	1 vez por hora	9
–	1 vez por minuto	10

- **Classificação dos danos/ custos/ganhos**

	valor	**classificação**
–	danos totais	10
–	10 000 000 contos	9
–	1 000 000 contos	8
–	100 000 contos	7
–	10 000 contos	6
–	1 000 contos	5
–	100 contos	4
–	10 contos	3
–	1 conto	2
–	100$00	1

Exemplo: análise de risco do DEI (cont.)

- **Ameaças (probabilidades / danos)**
  - **Calamidades**
    - Incêndio (ninguém liga aos alarmes…) 3/8
    - Inundações (rebentamento da Barragem da Aguieira) 2/9
    - Terramoto (zona de baixa actividade sísmica, edifício novo) 3/8
    - Guerra nuclear (vale a pena tomar medidas para tentar acautelar os efeitos ?) 2/10
  - **Ameaças físicas**
    - Corte ou sobrecarga de corrente (muito frequente) 7/3
    - Roubo (já aconteceu) 5/5
    - Sabotagem (ex. para não haver aulas práticas) 6/4
    - Vandalismo (em situações de desespero e não só) 6/3
    - Acidente com equipamento 7/3
    - Avaria de hardware 8/3
    - Avaria nos servidores 6/4
    - Corte na rede local 6/4
    - Corte no acesso à Internet 7/4
  - **Ameaças lógicas**
    - Erros nos programas 10/1
    - Erros humanos 7/3
    - Vírus 7/3
    - Fraude (ex. nas notas) 5/5
    - Hackers nos servidores 5/4
    - Acesso não autorizado (ex. enunciados) 7/4
    - Divulgação não autorizada 5/4
    - Sniffing 6/2

Exemplo: análise de risco DEI (cont.)

- **Análise de vulnerabilidades**
  - **Confidencialidade**
    - Uso reduzido de mecanismos de garantia de confidencialidade
    - Fraco controlo dos mecanismos de partilha de informação em NetBIOS em alguns grupos
    - Não é conhecida a política de monitorização e auditoria
    - Os assuntos de segurança são debatidos nas aulas
  - **Autenticação**
    - É utilizada autenticação centralizada por username / password com Kerberos
    - Não existe nenhum mecanismo que impeça ou dificulte a partilha de passwords entre utilizadores
    - Mecanismo de autenticação dos acessos do exterior não impede utilização abusiva
    - Não é feita autenticação de emissor nas mensagens de Email
  - **Integridade**
    - São utilizados de mecanismos de controlo de integridade nos servidores (vigilância de executáveis)
    - Não são usados mecanismos de integridade na troca de mensagens
    - Não são usados mecanismos de integridade nos arquivos de software
    - Não são usados mecanismos de controlo de integridade no controlo dos conteúdos WWW

Exemplo: análise de risco DEI (cont.)

- **Análise de vulnerabilidades (cont.)**
  - **Controlo do acesso**
    - Acesso às instalações muito permissivo
    - Acesso físico aos recursos muito permissivo
    - Grande número de utilizadores com conhecimentos de informática
    - Grande numero de serviços remotos a utilizar passwords em texto
    - Número razoável de servidores expostos à Internet
  - **Disponibilidade**
    - PCs apenas com redundância de componentes
    - Alguma redundância nas impressoras
    - Alguns serviços sem redundância
    - Servidores sem redundância
    - Rede local sem redundância no backbone
    - Acesso à Internet sem redundância
  - **Não repudiação**
    - Não é garantida não repudiação de envio Email

Exemplo: análise de risco do DEI (cont.)

- **Medidas a implementar e custos**

  - **Confidencialidade**
    - Generalização da utilização de mecanismos de encriptação nas comunicações 5
    - Procedimentos mais restritivos na utilização de NetBIOS 4

  - **Autenticação**
    - Controlo de identidade por equipa de segurança 5
    - Autenticação com cartão Multibanco ou Smart Card (será viável) 6
    - Reforço dos mecanismos de autenticação nos PCs dos funcionários e de docentes (em NT) 4
    - Utilização obrigatória de mecanismos de autenticação de Email (assinaturas digitais) 4

  - **Integridade**
    - Implementação de mecanismos de controlo de integridade nos arquivos FTP e páginas WWW 4
    - Implementação de mecanismos de controlo de integridade na troca de mensagens 5
    - Vigilância central de Vírus em attachs ao Email 5

Exemplo: análise de risco do DEI (cont.)

- **Medidas a implementar e custos (cont.)**
  - **Controlo do acesso**
    - Controlo de acesso ao DEI por equipa de segurança 5
    - Câmaras de vigilância nas salas de PCs de acesso livre 5
    - Generalização do uso de mecanismos de password encriptada 5
    - Limitar o acesso directo à Internet a situações de excepção 4
    - Reduzir o número de servidores expostos 4
  - **Disponibilidade**
    - Redundância física (Cold Site) (fora de questão) 7
    - Redundância nos servidores principais 6
    - Redundância nos serviços principais 5
    - Spares e backups remoto nos PCs 4
    - Redundância na rede local 6
    - Redundância no acesso à Internet 5
    - Implementar procedimentos de reacção a alarmes de incêndio 5
    - Instalar cofre anti-fogo para guardar backups 5
    - UPS nos equipamentos de rede 5
  - **Não repudiação**
    - Utilização obrigatória de mecanismos de não repudiação de origem no Email (assinaturas digitais) 4

Exemplo: análise de risco do DEI (cont.)

- **Análise de investimento**
  - **Investimento total**
    - > 500 M Escudos
    - fora de questão
  - **Investimento total sem Cold Site**
    - próximo dos 30 M Escudos
    - igual orçamento anual do DEI
  - **Sem medidas de nível 6 e 7**
    - da ordem dos 10 M Escudos
    - reforço da equipa técnica de gestão
    - pode ser faseado em dois ou três anos

Exemplo: análise de risco do DEI (cont.)

- **Avaliação do impacto das medidas a implementar (probabilidade /custo)**

	antes	depois	ganho
– Calamidades			
• Incêndio	3/8	**2/8**	**5**
• Inundações	2/9	2/9	
• Terramoto	3/8	3/8	
• Guerra nuclear	2/10	2/10	
– Ameaças físicas			
• Corte ou sobre de corrente	7/3	**7/2**	**4**
• Roubo	5/5	**4/5**	**5**
• Sabotagem	6/4	**4/4**	**5**
• Vandalismo	6/3	**4/3**	**5**
• Acidente com equipamento	7/3	**7/2**	**4**
• Avaria de hardware	8/3	**7/3**	**4**
• Avaria nos servidores	6/4	**5/4**	**5**
• Corte na rede local	6/4	**5/4**	**5**
• Corte no acesso à Internet	5/4	**7/4**	**5**
– Ameaças lógicas			
• Erros nos programas	10/1	10/1	
• Erros humanos	7/3	7/3	
• Vírus	7/3	**6/3**	**4**
• Fraude	5/5	**4/5**	**5**
• Hackers nos servidores	5/4	**4/4**	**4**
• Acesso não autorizado	7/4	**6/4**	**4**
• Divulgação não autorizada	5/4	5/4	**4**
• Sniffing	6/2	5/2	**4**

Exemplo: análise de risco do DEI (conclusão)

- **Avaliação do impacto das medidas a implementar**

  - **Custos**
    - Da ordem dos 10 M Escudos
  - **Ganhos**
    - Da ordem dos 10 M Escudos / ano
  - **Conclusão**
    - Retorno do investimento (ROI) num ano !

  - **Exemplo de análise de ganho**

	antes	depois	ganho
• Avaria nos servidores	6/4	5/4	5

    - 6 -> 1 vez por mês
    - 5 -> 1 vez por ano
    - 4 -> custo de 100 contos

    - custo ano antes = 100 contos * 12 = 1200 contos
    - Custo ano depois = 100 contos * 1 = 100 contos
    - Ganho = 1100 contos -> 5

Exemplo: política de segurança do DEI

- **Âmbito**
- **Responsabilidades**
- **Regras de utilização dos recursos**
- **Penalidades por infracção**
- **Omissões**

Exemplo: política de segurança do DEI (cont.)

- **Âmbito**
  - Rede local
  - Acesso à Internet
  - Acesso ao DEI via RCU
  - Acesso ao DEI via PSTN
  - Servidores de utilização geral
  - Servidores dos laboratórios
  - PCs de uso geral
  - PCs de uso individual
  - PCs do NEEI e do Quiosque
  - Portáteis no DEI
  - Impressoras de uso geral
  - Impressoras de uso individual
  - Software servidor
  - Software das aulas
  - Software de investigação
  - Software de uso individual

Exemplo: política de segurança do DEI (cont.)

- **Responsabilidades**
  - **Equipa de gestão**
    - Gestão dos servidores
    - Gestão da comunicações
    - Gestão da segurança e desempenho
    - Ligação de PCs à rede e configuração base
    - Instalação de software nos servidores
    - Instalar software nos PCs de uso colectivo
    - Gestão do software (inventário, distribuição)
    - Help-desk aos utilizadores
  - **Utilizadores**
    - Utilizar software instalado
    - Instalar software nos PCs de uso pessoal
    - Segurança da informação pessoal
  - **Comissão Executiva**
    - Divulgar e fazer cumprir a Política de Segurança
    - Aplicar sanções aos prevaricadores
  - **CIUC**
    - Gestão do acesso à Internet
    - Gestão do backbone do Polo II

Exemplo: política de segurança do DEI (cont.)

- **Regas de utilização**
  - **Limitações acesso aos recursos**
    - Salas de PCs dentro do horário estipulado
    - Utilização para fins académicos tem prioridade sobre utilização lúdica
    - Impressoras implicam autorização e registo em Centro de Custos
  - **Autenticação**
    - Passwords seguras com validade de 60 dias
    - Passwords intransmissíveis
    - Autenticação para acesso aos serviços e recursos
    - PCs individuais com screen saver activado aos 5 minutos de inactividade e reactivado com autenticação password
    - PCs de uso colectivo com logout automático ao fim de 5 minutos de inactividade
  - **Vírus**
    - É feito o controlo central de vírus no ficheiros em attach a mensagens Email
    - Todos os PCs devem possuir anti-virus instalado
    - Nos PCs de uso privado é da responsabilidade dos utilizadores a actualização dos anti-vírus
    - Um suspeita de ataque de vírus deve ser imediatamente comunicada à equipa de gestão

Exemplo: política de segurança do DEI (cont.)

- **Regas de utilização (cont.)**
  - **Acesso Remoto**
    - Para efeitos de acesso aos recursos informáticos do DEI e de autenticação, os acessos remotos por RCU e PSTN são considerados exteriores à rede interna do DEI
    - O acesso remoto por RDIS é reservado aos utilizadores abrangidos pelo serviço RCU
    - O processo de adesão ao serviço RCU é da exclusiva responsabilidade da Portugal Telecom e dos utilizadores
    - A utilização do serviço RCU obedece a regulamento próprio acordado entre a Portugal Telecom e o DEI
    - O acesso remoto por PSTN é disponibilizado a todos os utilizadores
    - É proibido o uso de acesso remoto por utilizadores externos ao DEI
    - O acesso remoto ao DEI é autorizado por RADIUS nas contas pessoais dos servidores de alunos e servidor geral
    - É proibida a utilização da facilidade de callback nos acessos remotos
    - Em situações de contenção nos acessos remotos poderão ser activados mecanismos de limitação de tempo de ligação

Exemplo: política de segurança do DEI (cont.)

- **Regas de utilização (cont.)**
  - **Acesso à Internet**
    - **objectivo:** o acesso à Internet deve ser usado para fins educativos em consonância com as actividades do DEI
    - **utilização para fins lúdicos:** é autorizada desde que não cause sobrecarga na rede e não colida com as leis em vigor
    - **WWW:** deve ser realizado através de servidores proxy locais
    - **Email:** através de servidores POP e SMTP locais com limite de 8 M bytes por utilizador
    - **News:** servidor de News local
    - **FTP anónimo:** deve ser feita via servidor proxy
    - **Acesso remoto:** deve ser realizado através de SSH ou de outra ferramenta que não use password em modo de texto.
    - **Áudio e Vídeo em tempo real:** deve ser feito através de SOCKS. Serviço de segunda prioridade que poderá ser desactivado nas horas de maior tráfego
    - **IRC, ICQ:** deve ser feito através de SOCKS. Serviços de segunda prioridade autorizados desde que não comprometam a utilização de recursos necessários a outros serviços
    - **Outros serviços:** mediante requerimento e autorização caso-caso da Comissão Executiva

Exemplo: política de segurança do DEI (cont.)

- **Regas de utilização (cont.)**
  - **Privacidade e monitorização/auditoria**
    - Todos os recursos informáticos são propriedade do DEI
    - O DEI reserva-se o direito de activar mecanismos de monitorização e auditoria que recolham informação completa sobre a actividade dos utilizadores, nomeadamente dos serviços WWW, Email e acessos FTP
    - O DEI reserva-se o direito de aceder às áreas de trabalho dos utilizadores para fins de auditoria de segurança
    - O DEI reserva-se o direito de impedir o acesso a sites cujos conteúdos colidam com os objectivos da organização
  - **Proibições expressas aos utilizadores**
    - Difusão de vírus
    - Divulgação de passwords
    - Cópia ilegal de software
    - Utilização de sniffers, crackers de passwords, ferramentas de monitorização e auditoria, exceptuando para fins académicos, em ambiente controlado, no âmbito da disciplina de Segurança em Redes
    - Implementar ligações alternativas de/ao exterior da rede do DEI (ex. através de modems em PCs)

Exemplo: política de segurança do DEI (conc.)

- **Penalidades**
  - O DEI mantém um cadastro de cada utilizador
  - Em função do cadastro e da gravidade do acto serão estabelecidas caso-a-caso pela penalidades de entre a seguinte panóplia:
    - **Repreensão**
    - **Corte temporário de conta pessoal**
    - **Corte de acesso remoto via PSTN ou RDIS**
  - Nos casos mais graves o utilizador poderá ser alvo de procedimento disciplinar ou judicial

- **Omissões**
  - Em todos os pontos em que o presente documento for omisso cabe à Equipa Técnica a definição das regras a aplicar, cabendo ao utilizadores o direito de recurso para a Comissão Executiva
  - Esclarecimentos podem ser solicitados para a Equipa Técnica e à Comissão Executiva