Introdução à Segurança da Informação

Boas Práticas da Segurança da Informação – Parte III

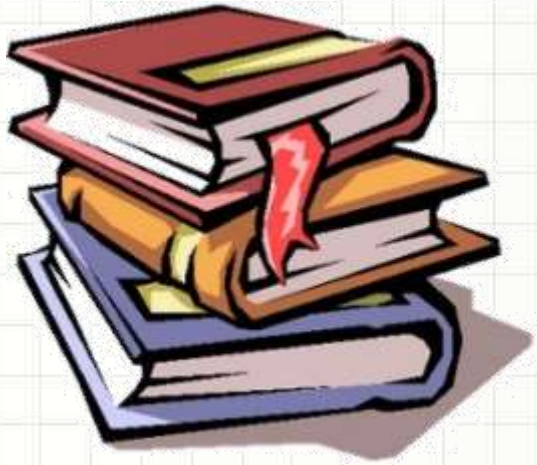
Prof. Dr. Daniel Caetano

2020 - 1

Objetivos

- Conhecer os conceitos de ambientes de operação alternativos
- Compreender os elementos envolvidos na contratação de terceiros
- Compreender procedimentos relacionados a incidentes de segurança

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 9)
Material Didático	Gestão de Segurança da Informação, Cap 5.
Leitura Adicional	http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf (Cartilha do TCU)

Ambientes Alternativos de Operação

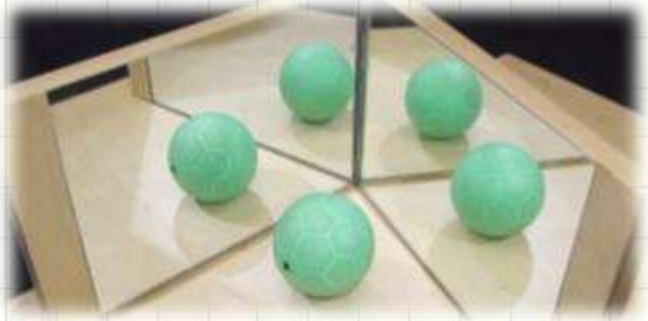
Ambientes Alternativos

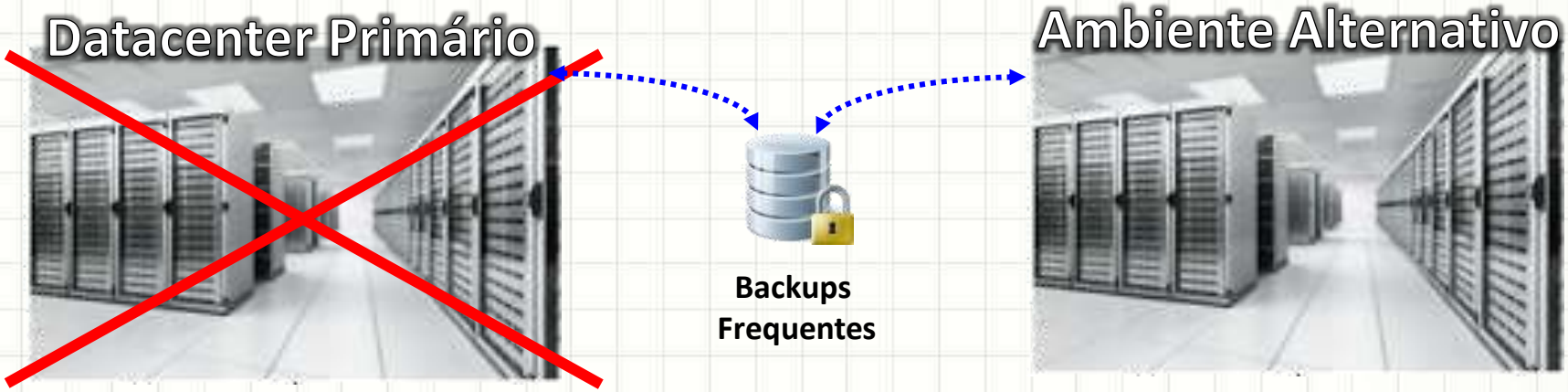
- Ocorreu um desastre...
  - E agora?

- Primeira ação: continuidade de operação
  - Até restaurar backups...
  - Veremos mais sobre isso mais adiante no curso...

Ambientes Alternativos

- Ajuda se existir um ambiente “espelho”
  - Ambientes de operação alternativos
- Três tipos
  - Cold Site
  - Warm Site
  - Hot Site



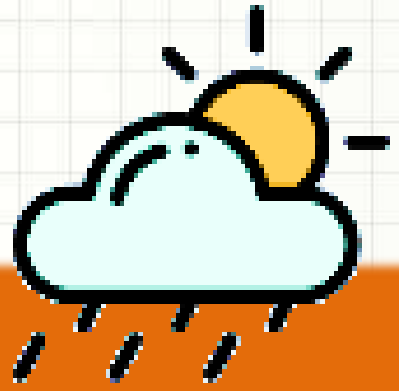


Ambiente Alternativo – Cold Site

- Recursos mínimos de infraestrutura
  - Assume (manualmente) até recomposição
- Pouco ou nenhum poder de processamento
  - Às vezes, nem conexão de rede!
  - Ex.: manter um website simples, alternativo
  - Ex.: Storages de backup
- Recomendado para...
  - Serviços tolerantes a falhas

Ambiente Alternativo – Warm Site

- Recursos básicos/médios de infraestrutura
  - Assume até recomposição
- Poder de processamento razoável
  - Ex.: manter serviços mais relevantes funcionais
- Recomendado para...
  - Serviços medianamente tolerantes a falhas



Ambiente Alternativo – Hot Site

- Espelho infraestrutura principal
  - Opera 24x7
  - Pode dividir carga com a principal...
  - ...e a assume totalmente na falha da principal
- Poder de processamento alto
  - Ex.: manter serviços 100% funcionais
- Recomendado para...
  - Serviços intolerantes a falhas

Ambiente Alternativo – Resumo

Cold Site

- Pouco ou nenhum equipamento
- Se conectividade de rede significativa
- Ativação manual
- Sem sincronia de dados
- Alta chance de perda de dados
- Custo baixo

Recuperação em **semanas/dias**

Warm Site

- Equipamento parcialmente redundante
- Conectividade de rede ativa
- Ativação automática em caso de falha
- Sincronia de dados diária ou semanal
- Pequena perda de dados
- Custo mediano

Recuperação em **dias/horas**

Hot Site

- Equipamento totalmente redundante
- Conectividade de rede ativa de alta performance
- Sempre ativo
- Sincronia em tempo real (ou quase)
- Nenhuma perda de dados
- Custo elevado

Recuperação em **horas/minutos**

Todos: Complexidades + Custos

Ambiente Alternativo – Tempo x Custo

Contratação de Terceiros

Contratação de Terceiros

- Dois grandes campos
  - Segurança interna dos sistemas e dados
    - Configurações, classificações, gestão de segurança...
  - Segurança da infraestrutura computacional
    - Equipamentos, armazenamento etc.

Contratação – Sistemas

- Para segurança interna permanente
  - Delicada no caso de sistemas e dados
    - Possibilidade de exposição
- Para apoio à segurança interna
  - Comum em diversos momentos
    - Consultoria para análise de risco
    - Testes de segurança (invasão)
    - Consultoria para certificação.

Contratação – Infraestrutura

- Segurança de infraestrutura...
  - Difícil manter internamente
  - Custo elevado, desperdício etc...
    - Estoque de peças que podem nunca ser usadas
    - Não há como garantir que não faltará peças.

Contratação – Infraestrutura

- Comumente contratada para
  - Ambientes alternativos (*Cold Site* e *Warm Site*)
  - Ambiente de backup (*Storages*)
  - Manutenção/Suporte de equipamentos
    - *Storages* e Processamento
  - Com o advento do "*as a service*" (nuvem)
    - Ambiente alternativo (*Hot Site* inclusive)
    - Ambiente principal
    - Além dos anteriores.

Contratação – Infraestrutura

- Ambientes alternativos (Cold e Warm Site)
  - Dificuldades associadas
    - Definir o que vai estar ativo e o que não
    - Manutenção de ambiente alternativo
    - Pagamento mesmo que não seja usado
    - Se há operação, mesclar dados com sistema principal

  - Cuidados na contratação
    - SLA: tempo para entrar em operação
      - Como comunicar?
    - Custo não pode ser excessivo considerando baixo uso
    - Segurança da permanência
      - Não adianta nada se quando precisar estiver fora!

Contratação – Infraestrutura

- Ambiente de backup (*Storages*)
  - Dificuldades associadas
    - Definir a priori o quê guardar (política de backup)
    - Espaço e desempenho adequados
    - Estratégias de recuperação (parcial x completa)
  - Cuidados na contratação
    - SLA: tempo para acesso para restauração
      - Liberação x Download dos dados
    - Custo x política de espaço e uso
    - Segurança da informação
      - Não podem perder!

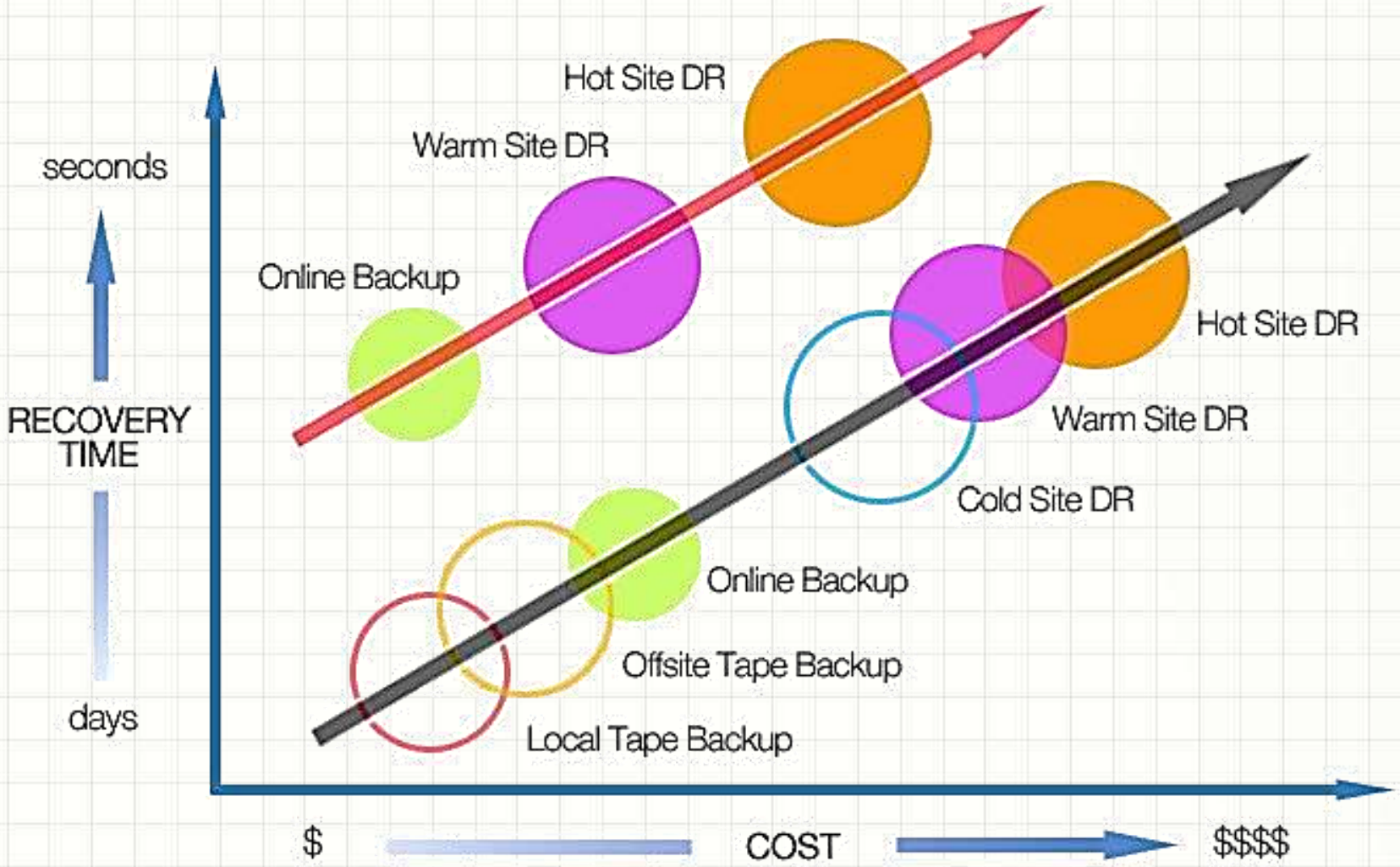
Contratação – Infraestrutura

- Manutenção/Suporte de equipamentos
  - Dificuldades associadas
    - Definir os requisitos de cada equipamento
    - Definir o período de contratação (x substituição)
  - Cuidados na contratação
    - SLA: tempo de resposta e correção de dano
      - Conserto x reposição por novo
    - Custo x duração do contrato
      - Períodos mais longos x curtos
        - » Mudança parque x valor sobe
    - Segurança do negócio
      - Empresa deve arcar com combinado

Contratação – Infraestrutura

- Sistemas e Serviços em Nuvem
  - Dificuldades associadas
    - O que é necessário contratar?
    - Quais dados, externamente?
      - Quais cuidados com os dados?
  - Cuidados na contratação
    - SLA: tempo de resolução de problemas
      - Término do contrato: tempo para migração
    - Custo do contrato: uso fixo + uso variável
    - Segurança do negócio e informação
      - Empresa deve arcar com combinado
      - Necessário garantir a segurança dos dados

Ambiente Alternativo – Nuvem



Incidentes e Desastres: Alguns Procedimentos

Incidentes e Desastres

- Nem todo incidente...
  - ...se torna um desastre.
- Tentativas de ataques detectadas
  - Demandam um tipo de ação
- Ataques realizados com sucesso
  - Demandam outro tipo de ação

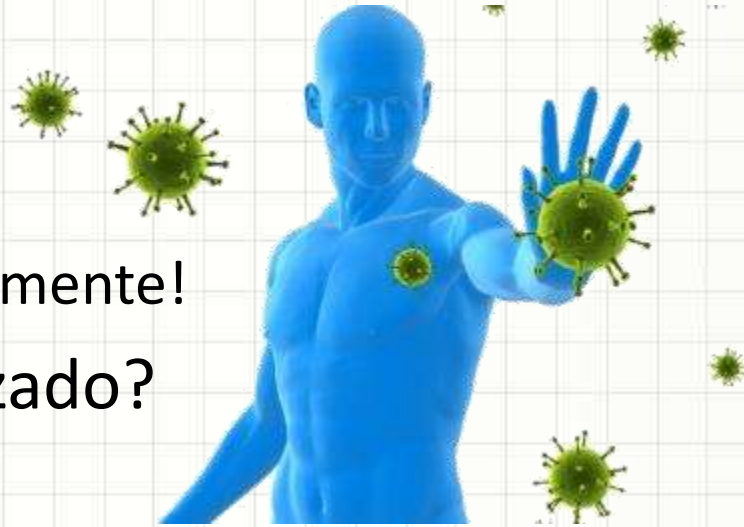
- Serão dadas algumas dicas...
  - Que podem exigir adaptação no seu ambiente!

Tentativas de Ataques

- Tentativa: ainda não causou desastre
  - Recomenda-se ação tão rápida quanto possível
  - Mas... importante! Mantenha a calma!

Tentativas de Ataques

- Primeiro passo
  - Certificar-se de que as defesas do sistema estão ok
- O que verificar?
  - Firewall está ativo?
    - Se não estiver, suba imediatamente!
  - Antivírus está ativo e atualizado?
    - Se não estiver, atualize.
  - Verifique as portas abertas com o NMAP
    - As portas abertas são as que deveriam?
  - Há uso de SSH é a máquina tem acesso público?
    - Verifique se o SSHGuard está funcional.



Tentativas de Ataques

- Segundo passo
  - Auditoria: identificar os tipos de ataques
- O que verificar em termos de log?
  - Log de sistema (Ex.: syslog)
  - Log de falha de acesso (Ex.: lastb)
  - Logs de aplicações (Ex.: apache, postfix etc)

Tentativas de Ataques

- Terceiro passo
  - Auditoria: identificar se houve sucesso no ataque
- O que verificar em termos do sistema?
  - Execute uma verificação dos arquivos
    - Rkhunter, Lynis etc. (cfg prévia); Antivirus com LiveCD
  - Usuários do sistema (Ex.: passwd)
    - Verifique se não apareceu nenhum indevido!
  - Processos/Serviços automáticos (Ex.: crontab)
    - Para todos os usuários!
  - Verifique os processos em execução (Ex.: top, htop)
    - Tem algum processo estranho?
  - Verifique as conexões ativas (Ex.: netstat -punta)
    - Tem conexões estranhas?

Tentativas de Ataques

- Quarto passo
  - Ações corretivas
- Não houve invasão, mas há método no ataque?
  - Certifique-se de que todo o possível foi feito
    - Configure proteções, instale programas de proteção...
    - Pesquise!.
- Argh! Tem coisa estranha na máquina!
  - Parta para a próxima seção...
    - Procedimentos para desastre!.

Desastre Identificado

- Houve desastre: há comprometimento
  - Primeira ação imediata: desligue a rede
    - Pode ser tirando o cabo, mesmo
    - Se não for possível, desabilite as interfaces de rede.
  - Agora respire fundo e mantenha a calma
  - Sangue frio é importante nesse momento

Desastre Identificado

- Primeiro passo
  - Verificação no restante do sistema
- O que verificar?

  - Todas as máquinas ligadas na rede da empresa
    - No mínimo as da mesma sub-rede
  - Busque a mesma falha da máquina atacada
  - Se localizadas falhas, mesmo procedimento
    - Desligá-las da rede
  - Pode ser feita em paralelo com próximos passos
    - Comande a equipe para realizar esse primeiro passo
    - Próximos passos: aplicados em todas as máquinas

Desastre Identificado

- Segundo passo
  - Subir ambiente alternativo
  - Preparar o recuperado
- Qual ambiente alternativo?
  - Se há, o do **cold site**.
  - O do warm ou hot site pode estar comprometido
- Como preparar novo ambiente?
  - Restaurar o backup mais recente
    - Em nova máquina
    - Em ambiente desconectado ou com firewall fechado

Desastre Identificado

- Terceiro passo
  - Auditoria: verificar extensão de dano imediato
- O que verificar?
  - Execute uma verificação dos arquivos
    - Rkhunter, Lynis etc. (cfg prévia); Antivirus com LiveCD
  - Usuários do sistema (Ex.: passwd)
    - Verifique se não apareceu nenhum indevido!
  - Processos/Serviços automáticos (Ex.: crontab)
    - Para todos os usuários!
  - Verifique os processos em execução (Ex.: top, htop)
    - Tem algum processo estranho?

Tentativas de Ataques

- Quarto passo
  - Auditoria: identificar como o ataque teve sucesso
- Como começar?
  - Pesquise o que pode ocasionar o problema
    - Oriente-se pelo resultado do terceiro passo

- O que verificar nos log?
  - Log de sistema (Ex.: syslog)
  - Log de falha de acesso (Ex.: lastb)
  - Logs de aplicações (Ex.: apache, postfix etc)

Tentativas de Ataques

- Quinto passo
  - Ações corretivas...
  - ...na nova máquina
- Procedimento?
  - Com a nova máquina criada no segundo passo
    - Restauração do backup...!
  - Aplique todas a checklist de segurança da empresa
  - Aplique todas as correções para travar
    - Problemas encontrados no terceiro passo
    - Brechas identificadas no quarto passo

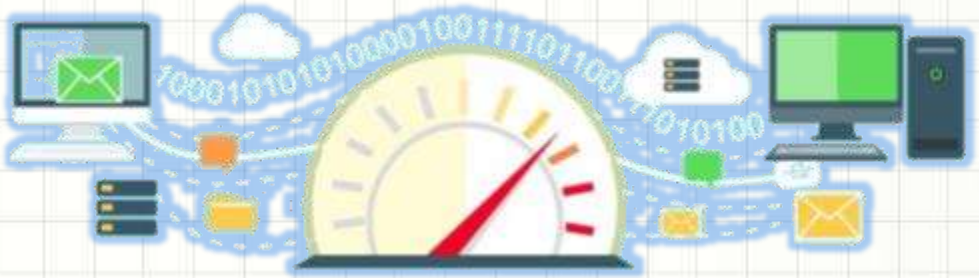
Tentativas de Ataques

- Sexto passo
  - Ajustando novo ambiente

- Procedimento?
  - Verifique se há portas “ouvindo” (netstat –punta)
  - Passe o pente fino na nova configuração do firewall
  - Se for uma VM, faça um snapshot
  - Habilite a nova configuração do firewall
  - Verifique o que está aberto com o NMAP

Tentativas de Ataques

- Sétimo passo
  - Monitoramento e controle
- Máquina antiga...
  - Nunca mais será confiável
  - Auditoria detalhada
  - Desativar a máquina após.
- Máquina nova
  - Monitorar por um tempo
    - Conexões, tráfego
    - Processos



QUESTÕES

Quiz

Ao contratar um serviço de manutenção de equipamentos, o que é **menos** relevante...

https://kahoot.it/

Conclusões

Resumo e Próximos Passos

- Ambientes Alternativos
  - Para recuperação de desastres
- Contratações externas
  - Aspectos e cuidados
- Noções para enfrentamento de ataques

- Continuidade de Negócios
  - O plano de contingência
  - Noções legais

PERGUNTAS?