Introdução à Segurança da Informação

Controle de Acesso a Recursos Compartilhados

Prof. Dr. Daniel Caetano

2021 - 1

Compreendendo o problema

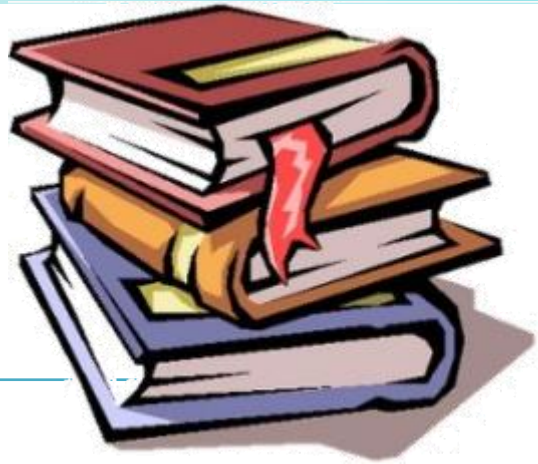
- **Situação:** Funcionário é demitido por justa causa após ter deixado seu computador desbloqueado e outra pessoa ter usado sua senha para cometer ilícitos.

Você costuma deixar seu computador/celular desbloqueado?

Objetivos

- Conhecer alguns dos aspectos administrativos da segurança
- Compreender os mecanismos de controle de acesso a recursos compartilhados
- Compreender os fundamentos da poítica de senhas
- Tomar contato com as estratégias de cópia de segurança (backup)

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 7)
Minha Biblioteca	Windows Server 2012: Guia de Bolso. Cap. 8 e 12.
Material Didático	Gestão de Segurança da Informação, Caps 5
Material Adicional	http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf (TCU)

Retomando:

Controle de Acesso

Retomando: Controle de Acesso

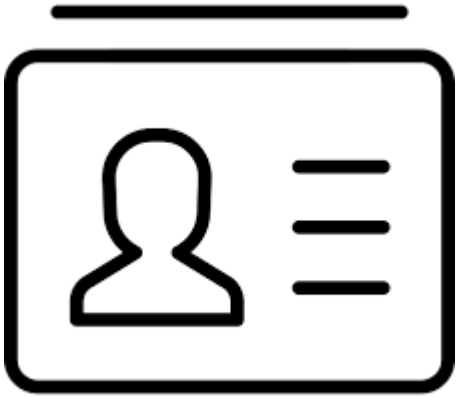
- Segurança pressupõe controle de acesso
  - Físico x lógico
- Envolve
  - Recurso x usuário: quem pode o quê

- Regra de ouro: tudo proibido...
  - ...a menos que expressamente permitido.
  - Registrar tudo que todos fazem
    - Auditoria
    - **Responsabilização**

Retomando: Controle de Acesso

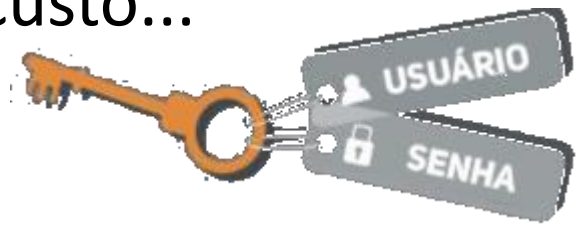
- **Logon/Login**: dois processos básicos
  - Identificação**:** qual é o usuário e suas permissões
  - Autenticação**:** comprovar a identidade

- Resumindo
  - **Identificação** + **Algo que usuário sabe ou tem**



Retomando: Dificuldades

- Processo precisa ser resistente à “invasão”:
  - Cartões: podem ser perdidos
  - UserIDs: podem ser fornecidos facilmente
  - Senhas: anotações, senhas fracas, força bruta...
  - Biometria: falsos negativos, custo...



- Estratégias
  - Controlar quem acessa o quê (limitar acesso)
  - Exigências na criação de senhas
  - Manter cópia de segurança dos dados.

Controle de Acesso a Recursos Compartilhados

Política de Acesso Lógico

- Em geral, as permissões de acesso
  - Associadas à função do funcionário
    - Papel do funcionário dentro da empresa
  - Permissões devem ser atribuídas minuciosamente
    - Apenas o necessário...!
    - Revisões periódicas!
      - Remover excessos
    - Ex.: Estagiário

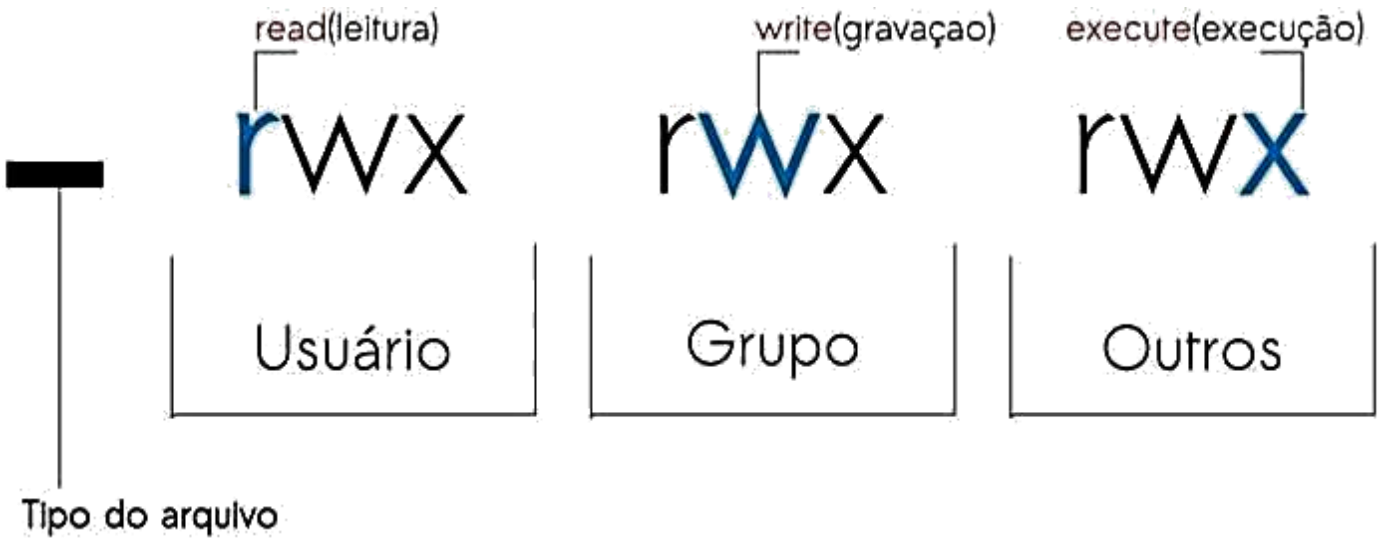
Controle de Acesso de Arquivos

- Além do *login*... existe outro aspecto
  - Proteção de acesso no nível do sistema de arquivos

- Unix/Linux x Windows

Controle de Acesso de Arquivos

- Unix/Linux (todos os sistemas de arquivo)
  - Permissões de execução (x), leitura (r) e escrita (w)
  - Usuário, grupo de usuários e usuários em geral

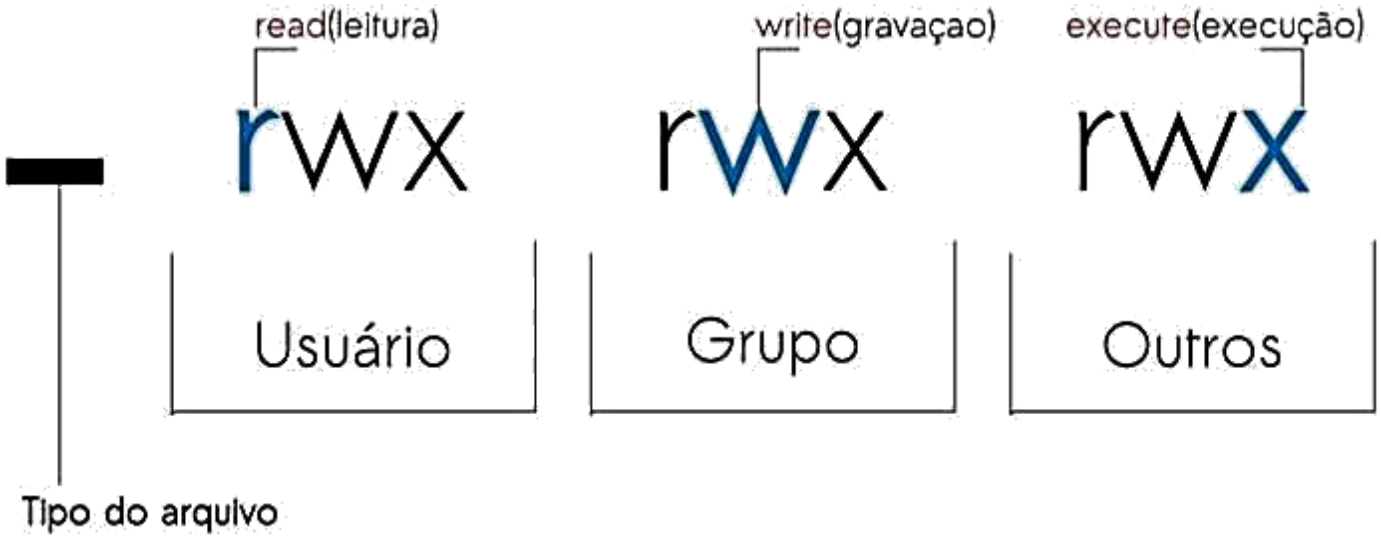


Controle de Acesso de Arquivos

- Unix/Linux
  - Permissões de execução (x), leitura (r) e escrita (w)
  - Usuário, grupo de usuários e usuários em geral

Controle de Acesso de Arquivos

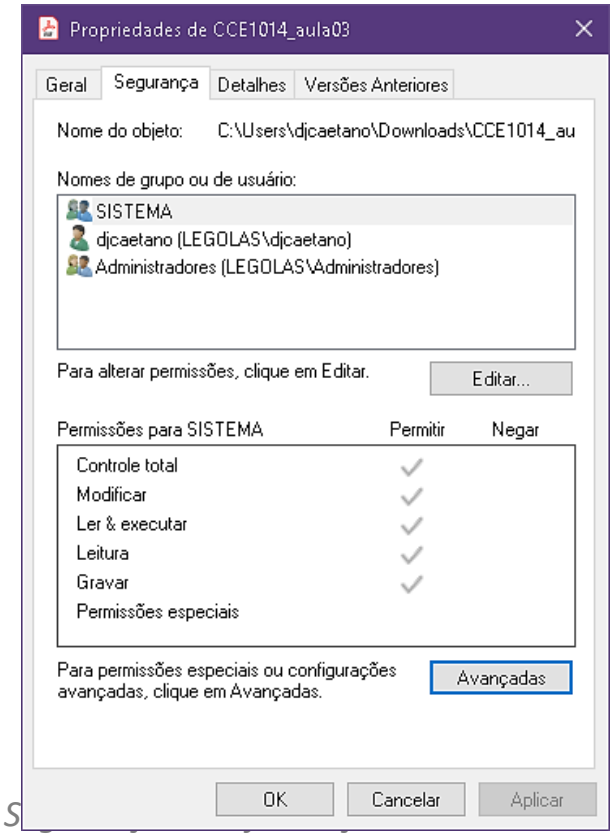
- Unix/Linux
  - Permissões de execução (x), leitura (r) e escrita (w)
  - Usuário, grupo de usuários e usuários em geral

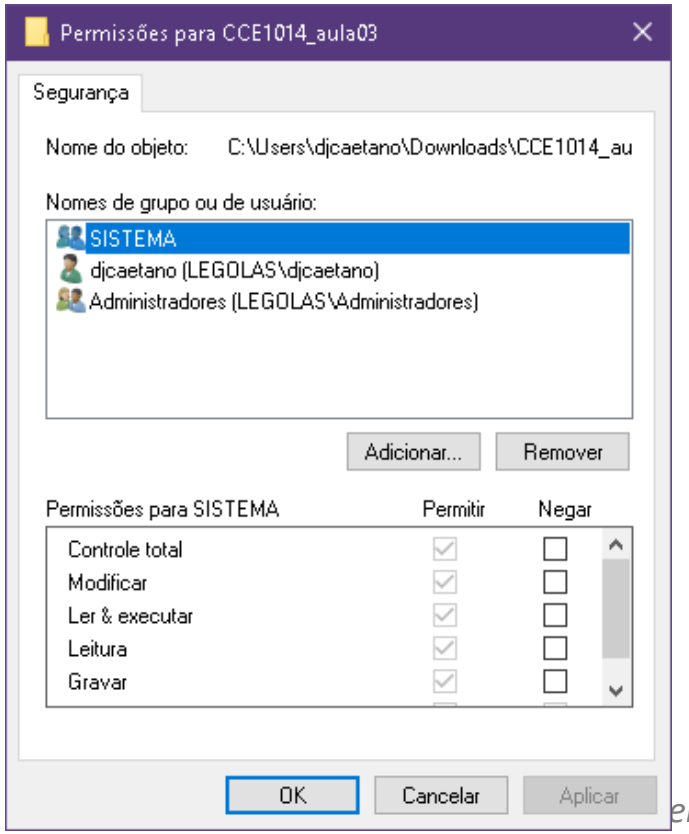


  - Root sempre tem acesso a tudo.
    - Proteger! Nunca *login* remoto!

Controle de Acesso de Arquivos

- *Windows/Active Directory*
  - ACL – *Access Control Lists* (Local x Centralizada)
    - Melhor controle, gestão + complexa e menor velocidade





Controle de Acesso de Arquivos

- *Windows/Active Directory*
  - ACL – *Access Control Lists* (Local x Centralizada)
    - Melhor controle, gestão + complexa e menor velocidade
- Sistemas de arquivos que suportam:
  - NTFS (para recursos locais e de rede)
  - HPFS386 (para recursos de rede – legado*)
- Sistemas de arquivos que não suportam
  - FAT (qualquer um, do FAT12 ao FAT64)
  - HPFS (legado*)

Proteção com Controle de Acesso

- O que proteger?
  - Aplicativos;
  - Arquivos de dados;
  - Utilitários e S.O.;
  - Arquivos de senha;
  - Arquivos de log.

Proteção com Controle de Acesso

- Aplicativos
  - Código fonte e objetos compilados
  - Por quê?
    - Inserir as mais variadas brechas de segurança
    - Modificar o comportamento de maneira inadequada
      - Ex.: “arredondamentos” em código financeiro.

Proteção com Controle de Acesso

- Arquivos de Dados
  - Tanto arquivos propriamente ditos...
    - ...quanto em banco de dados
  - Por quê?
    - Dados de operação da empresa
    - Dados estratégicos
    - Dados de clientes...

Proteção com Controle de Acesso

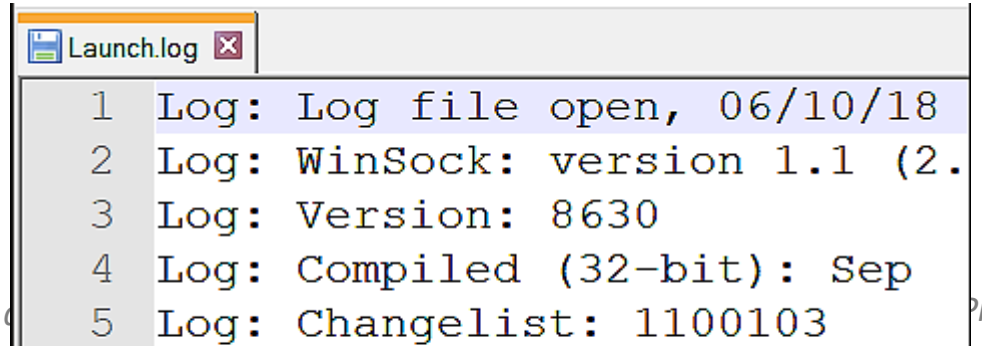
- Utilitários e Sistema Operacional
  - Acesso restrito, principalmente aos mais críticos
    - Compiladores, manutenção, monitoração, diagnóstico...
  - Por quê?
    - Maiores alvos, permitem expor configurações e falhas
    - Permite abrir brechas graves e "invisíveis".

Proteção com Controle de Acesso

- Arquivos de Senha
  - Tanto do sistema operacional quanto aplicativos
  - Por quê?
    - Prejudicam completamente o controle!
    - Usuário que tenha acesso pode ser passar por outros!.

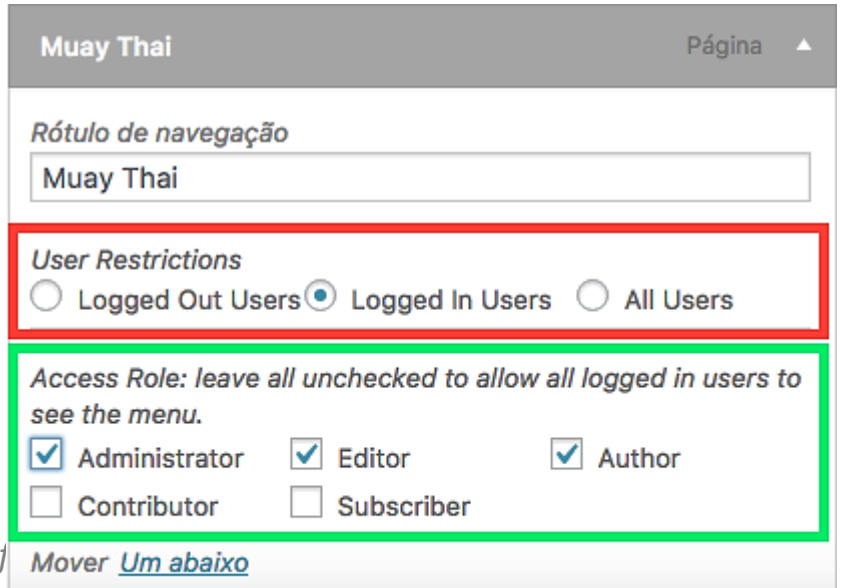
Proteção com Controle de Acesso

- Arquivos de Log
  - De acesso e operações...
    - De sistema e das aplicações!
  - Por quê?
    - É pelos logs que fazemos auditoria
      - Identificar tentativas e sucessos de ataques
    - Se eles forem alterados/apagados...
      - Ficamos sem pistas!



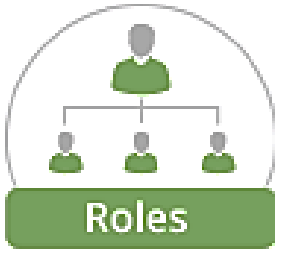
O que mais Restringir?

- Além do acesso a arquivos...
  - (Permissões do sistema de arquivos e ACLs)
- Restringir funções nas aplicações
  - Opções não autorizadas não devem nem aparecer
  - Ocultar dados que não devem ser exibidos.



Administração de Usuários

- Desativar usuários inativos
  - Demitidos, transferidos etc.
  - Em férias?.
- Todo funcionário inativado...
  - Deve ser inativado em todos os sistemas
- Não apague os dados do usuário
  - Apenas desative-os
  - Não forneça acesso livre a esses dados.



Política de Senhas

Senhas Seguras

- São a forma mais tradicional de autenticação
  - Solução de menor curso
  - Segurança tão grande quanto:
    - Qualidade da senha
    - Política de troca de senhas
    - Cuidados e atenção do usuário
      - "Senha é pessoal e intransferível"

- Por que esses cuidados são tão importantes?

Senhas: Quebrando-as

- Existem 2 formas básicas de se obter senhas
  - Engenharia Social **Com jeitinho**
    - Conseguir que a pessoa a forneça
    - Encontrar a mesma registrada em local não seguro
    - Senhas óbvias (informações facilmente encontradas).
  - Força Bruta **Na marra**
    - Testar usuários/senhas até encontrá-los
    - Palavras comuns
    - Senhas simples (usando apenas letras, por exemplo).
- Vejamos regras e orientações para dificultar...

Senhas: Regras

- As seguintes regras devem ser seguidas
  - Manter a confidencialidade das senhas
  - Nunca compartilhar senhas
  - Evitar registrar as senhas em papel
    - Se precisar registrar, use um software adequado
    - Ex.: KeePass, mSecure, LastPass, DashLane....

LastPass •••|

Senhas: Regras

- As seguintes regras devem ser seguidas
  - Selecionar senhas de boa qualidade
    - Muito curtas: ruim
    - Muito longas: ruim
    - De 6 a 8 caracteres.
  - Alterar quando houver indício de anormalidade
  - Alterar as senhas em intervalos regulares
    - Usuários com acesso privilegiado: intervalos menores.

Senhas: Regras

- Informe sempre aos usuários
  - Evitar reutilizar senhas já usadas no passado
  - Obrigar mudar senhas temporárias no 1º acesso
  - Não incluir senhas em processos automáticos
    - Macros, navegador etc.
    - Repositórios de código!.
  - Evitar usar a mesma senha para vários sistemas
    - Se usar do tipo Single Sign-On, use uma complexa
    - Ex.: Google, Facebook etc..

Senhas: Orientações

- Algumas orientações podem ser passadas
  - E muitas delas podem virar regras também!
- Evitar senhas facilmente identificáveis
  - Nome do usuário ou user id (mesmo embaralhado)
  - Nomes (familiares, amigos, lugares etc).
  - Nome do sistema operacional ou da máquina
  - Números de telefone ou documentos
  - Datas.

Senhas: Orientações

- Evitar senhas facilmente identificáveis (cont.)
  - Placas, marcas de carro, etc..
  - Palavras que constam em dicionários
  - Letras ou números repetidos
  - Letras seguidas do teclado
    - ASDF, QWERTY, 123456...
  - Objetos ou locais visíveis da mesa do usuário
    - Livro na estante, loja vista pela janela...
  - Qualquer senha com menos de 6 caracteres.

Senhas: Orientações

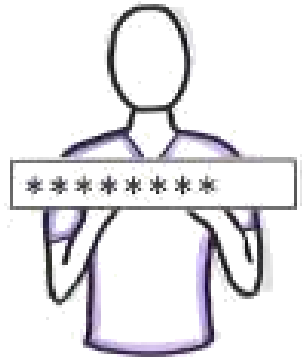
- Dificultar “adivinhação” e “força bruta”
- Boas práticas em senhas
  - Fácil de memorizar por você, mas não por outros
  - Usar, simultaneamente:
    - Números
    - Caracteres especiais.
    - Letras maiúsculas e minúsculas
  - Senhas que possam ser digitadas rapidamente
  - Seguir todas as regras anteriores

Senhas: Distribuição

- Deve ser feita com cuidado e com orientação
  - O usuário precisa saber a importância da senha!.
- Solicitar que usuário assine declaração
  - Tomando ciência da confidencialidade da senha.
- Garantir senha temporária segura
  - E forçar usuário a mudá-la no primeiro acesso
  - Fornecer senha temporária em mãos, se possível
  - Se fornecer link para cadastro de senha...
    - Limitar o tempo para isso (1 hora, por exemplo)
    - Ter certeza que e-mail é do usuário e não foi invadido.

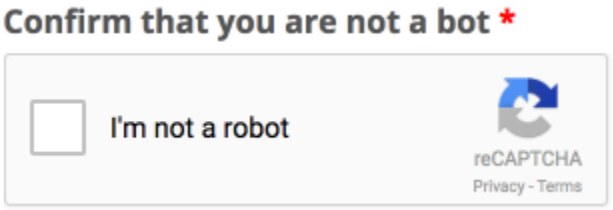
Senhas: Medidas Adicionais

- Uso de sistemas que dificultem quebra
- No cadastro da senha
  - Indicar o nível de segurança da senha
  - Impedir o cadastro de senhas “fracas”
  - Expirar as senhas de tempos em tempos
    - Ex.: 42, 45, 90... dias
  - Evitar reuso de uma das últimas senhas
    - Ex.: 5, 12, 24...
  - Guardar as senhas na forma de hashs.



Senhas: Medidas Adicionais

- Uso de sistemas que dificultem quebra
- Na tela de *login*
  - Bloqueio após erros
    - 3 ou 5 erros (mínimo 30 minutos)
  - SSHGuard
  - Captchas

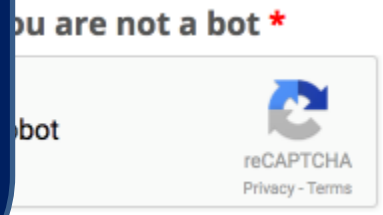


  - Nunca informar que "usuário não existe" ou "senha incorreta", isoladamente, em caso de erro de *login*

Senhas: Medidas Adicionais

- Uso de sistemas que dificultem quebra
- Na t
  - Bl
    -
  - Ss
  - Ca
  - Num ste" ou "senha incorreta", isoladamente, em caso de erro de *login*

Mas... E se as medidas falharem e houver perda ou adulteração de dados/arquivos?



CÓPIAS DE SEGURANÇA

Cópias de Segurança

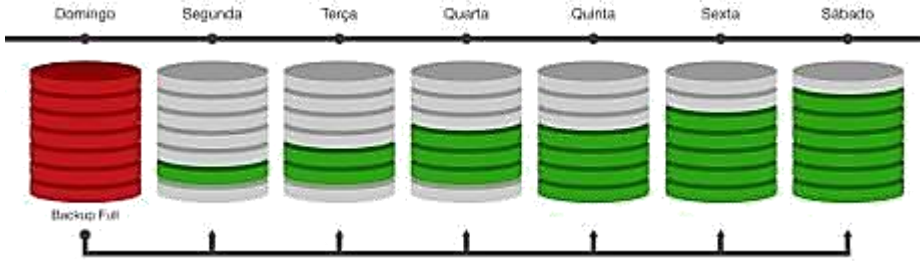
- O que é isso?
  - Cópias de dados e programas relevantes...
  - ...para recuperação em caso de desastres
  - E para proteção legal.
- Também conhecidas como...

Frequência de *Backup*

- Com que frequência fazemos *backup*?
  - Sempre que possível e não prejudique os negócios.
- Limitações
  - Espaço: cópias ocupam espaço
  - Tempo: *backup* com sistema desligado
  - Desempenho: *backup* com sistema ligado.
- Resumindo: não dá pra copiar tudo sempre
  - Diária, semanal, mensal... Misto
  - Depende da necessidade.

Abrangência do *Backup*

- Tenho que fazer *backup* de tudo?
  - Depende!
- Estratégias comuns:
  - Completa ou completa+diferencial



- O que usualmente protegemos?
  - Arquivos de dados / banco de dados
  - Arquivos de configuração.
- Em sistemas complexos / máquinas virtuais
  - Pode-se fazer *backup* de tudo, completo
    - Deixa-se para o "*storage*" eliminar as redundâncias

Mídias/Armazenamento de *Backup*

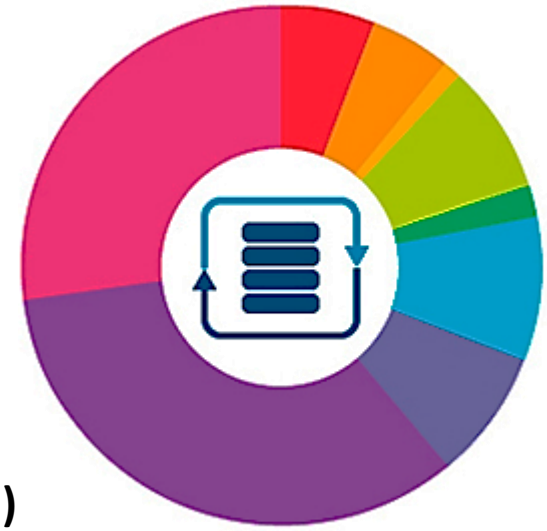
- Em que meio guardar esses dados?
  - Diversos: fitas DAT, DVDs, BluRays, *storage*...
- Escolha:
  - Tipo de ameaça aos dados
  - Quantidade de dados
  - Tempo de vida do dado
  - Frequência da recuperação
  - Tempo de recuperação.

Localidades de *Backup*

- Onde guardar esses dados?
  - De preferência, não na mesma máquina da origem!
    - Embora mesmo essa seja melhor que nenhuma!
- Idealmente:
  - Localidade externa
  - Distante o suficiente para evitar “desastre duplo”
  - Perto o suficiente para não prejudicar recuperação
    - Quando necessária.... Qual o prazo?
  - Segurança física e lógica na localidade externa
    - Controle ambiental.

Testes de Restauração

- Os ambientes mudam...
  - Conteúdo do *backup*: revisar com frequência
  - Além da documentação, como saber?.
- Testes de restauração
  - Simulação de desastre
  - Restabelecer estado anterior
    - Completa x arquivos específicos



Frequência de Necessidade de Recuperação (GFI Software)

6%	Every day	8%	Once a week	9%	Once every 2 - 3 months
5%	2 - 4 times a week	2%	Every 2 weeks	34%	Once every 4 - 6 months
1%	5 - 6 times a week	9%	Once a month	27%	Less than once every 6 months

ATIVIDADE

Atividade

- Grupos – 15 minutos
  - Conforme canais do Teams
- Considere uma empresa com 5 funcionários e 3 setores, com um servidor de arquivos
- Definam:
  - O nome da empresa
  - Os setores
  - Grupos de usuários
  - Nomes dos funcionários
    - UserID, função, setor
    - Grupos
  - Estrutura de pastas
    - Quais grupos podem fazer o quê em cada pasta

ENCERRAMENTO

Resumo e Próximos Passos

- Política de controle de acesso a recursos
  - Unix x Windows
- Política de senhas
  - Treinamento!
- Estratégias de cópia de segurança
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/seguranca

- Criptografia e certificados digitais
  - Garantindo a confidencialidade nas transmissões

PERGUNTAS?