

Segurança da Informação e Segurança em Redes de Computadores **Segurança Física e Lógica**

Prof. Dr. Kelton Costa
kelton.costa@gmail.com
kelton.costa@unesp.br

Segurança Física

- O principal objetivo da implantação de controles de segurança física, é restringir o acesso às áreas críticas da organização, prevenindo os acessos não autorizados que podem acarretar danos a equipamentos, acessos indevidos à informação, roubos de equipamentos, entre outros.

Segurança Física

- Os controles de acesso físico devem ser implementados em conjunto com os controles de acesso lógico.
- A falta de implementação desses dois controles em conjunto, seria o mesmo que restringir o acesso as informações através de senhas, mas deixar os servidores desprotegidos fisicamente, vulneráveis a roubo, por exemplo.

- **Localização**

- A localização do CPD ou Data Center é um fator de grande importância, pois é ela que vai determinar as vulnerabilidades do CPD a fatores ambientais, e vulnerabilidades quanto ao acesso.
- Antes da escolha do local onde o CPD é implantado, deve-se observar, se o mesmo estará vulnerável aos seguintes itens:
 - inundações;
 - impacto de escombros;
 - excesso de calor;
 - excesso de poeira;
 - excesso de umidade;
 - excesso de radiação;
 - magnetismo;
 - vandalismo;
 - exposição a gases nocivos.

- **Localização**

- Deve-se observar ainda se há proximidade de caixas d'água, materiais inflamáveis e se o CPD ficará próximo a entrada da empresa ou da fábrica.
- A proximidade do CPD à entrada, determina a facilidade de acesso por pessoas não autorizadas, e também o grau de dificuldade de acesso de pessoas autorizadas em dias de greve, paralisações e manifestações.

- **Controle de acesso**

- O acesso ao CPD deve ser restrito ao pessoal autorizado, para tanto as portas devem permanecer trancadas, e devem ser implementados controles de acesso, que registrem quem entrou no CPD, horário e permanência.

- Algumas opções de controle de acesso, são:

- crachás eletrônicos;
- dispositivos biométricos;
- trancas manuais usadas em conjunto com outros controles, como por exemplo lista de permanência.



- **Acesso de prestadores de serviços**

- O acesso de prestadores de serviços, ou de qualquer pessoa que não esteja autorizada a acessar e permanecer no CPD, deve ser controlado e registrado, essas pessoas sempre devem estar acompanhadas de um funcionário do CPD.

- **Monitoramento**

- O uso de câmeras de monitoramento, é importante para se monitorar o que acontece dentro e fora, próximo as entradas do CPD.
- Esse tipo de monitoramento é utilizado para inibir possíveis ações não autorizadas, tentativas de burla dos controles de acesso, e também é utilizado para auxiliar na detecção de responsáveis.

- **Cabeamento**

- A estrutura do cabeamento do CPD é importante para evitar panes e problemas com a comunicação da rede da organização, portanto devem ser tomados certos cuidados ao se estruturar o cabeamento. Ex. recomendável utilizar piso falso em todo o CPD.



- **Portas e janelas**

- As janelas do CPD devem estar protegidas por grades, e as portas além de estarem trancadas, devem ser do tipo corta-fogo, para evitar que em caso de incêndio, o fogo se propague rapidamente.



- **Controles ambientais**

- Os equipamentos de informática devem estar protegidos contra fatores ambientais, como calor, umidade, poeira, fogo, etc.
- No CPD devem ser implantados os seguintes equipamentos de controle ambiental:
 - ar condicionado;
 - termômetros;
 - controle de umidade;
 - detector de fogo e fumaça;
 - extintor de incêndio

A quantidade de cada equipamento varia de acordo com o tamanho da sala, porém são indispensáveis em um CPD. É recomendável que exista também um extintor de incêndio fora do CPD, próximo a porta de entrada.

- **No Break**

O uso de um no break é indispensável para garantir o processamento das informações em caso de interrupção no fornecimento de energia.



- **Backup**

- O backup é um elemento fundamental na recuperação dos dados e retomada do processamento das informações. Para garantir que esse recurso esteja disponível quando necessário é recomendado que seja criado um site backup.
- Site backup é uma sala que possui as mesmas características do CPD utilizado na organização, contendo os mesmos tipos de equipamentos, com as mesmas configurações, em suma é uma cópia do atual CPD, que estará sempre disponível para assumir, se necessário, todas as operações e funções do CPD original.

- **Backup**

- O site backup deve estar localizado fora da empresa, pois se a sua ativação for decorrência de um desastre, ele não será afetado. Nele devem conter os últimos backups feitos, mantendo as informações atualizadas.
- Independente do uso do site backup, as fitas de backup devem ser armazenadas em local externo a organização em cofres anti-chamas, deve ser mantida ainda uma cópia do backup atual no CPD em cofre apropriado, para a rápida recuperação dos dados.

Definição da metodologia de backup

- O backup dos sistemas críticos devem estar preferencialmente separados dos outros backups para facilitar a sua restauração.
- Os cuidados tomados com essas fitas, devem ser os mesmos utilizados na política de backup utilizada pela organização, sendo observados os seguintes itens:
 - local onde serão armazenadas as fitas de backup;
 - uso de cofres;
 - controle da ordem cronológica de baixa dos backups;
 - controle da vida útil das fitas de backup;
 - simulações periódicas da restauração dos backups.

Definição da metodologia de backup - 9 tipos

1. Backup Completo

- O backup completo cria uma cópia de todos os dados presentes em um servidor para outro local. São todos os dados mesmo, sem nenhuma seleção.
- Tipo de backup que leva mais tempo para a restauração
- Principal vantagem do backup completo é que uma cópia de todos os dados do negócio estará disponível e em um único local.

Definição da metodologia de backup - 9 tipos

2. Backup Incremental

- Realiza cópia de segurança dos dados que foram alterados desde a última operação de backup.
- O sistema geralmente faz essa seleção por meio do acompanhamento da data e hora da modificação combinada com a data de hora do backup anterior.

Definição da metodologia de backup - 9 tipos

3. Backup Diferencial

- Uma operação de backup diferencial copiando todos os dados alterados desde o backup completo anterior.

Definição da metodologia de backup - 9 tipos

4. Backup Espelhado

- Os backups de espelhamento são um espelho da origem da cópia. Isso quer dizer, por exemplo, que quando um arquivo é excluído na origem ele também é excluído no backup.

Definição da metodologia de backup - 9 tipos

5. Backup Local

- Esse tipo de backup é feito de uma origem para um dispositivo físico como um disco externo, HD ou SSD por exemplo.
- Backups locais protegem o conteúdo digital de:
 - falhas no disco rígido;
 - exclusões acidentais;
 - ataques de vírus.

Definição da metodologia de backup - 9 tipos

6. Backup Externo

- Com a mesma ideia de um backup feito em um dispositivo físico, o backup externo tem uma diferença do backup local:
 - o dispositivo não fica na mesmo endereço que a origem dos arquivos.
- Exemplos de backup externo incluem levar a mídia de backup ou a unidade de disco rígido para casa.
- Pode ser aplicado em pequenas empresas

Definição da metodologia de backup - 9 tipos

7. Backup Remoto

- Tipo de backup externo, possível acessar as cópias de segurança mesmo estando a quilômetros de distância.
- Nesses casos os backup não é feito em um dispositivo físico como HD ou SSD externo, mas sim em plataformas que usam a tecnologia e permitem o acessos externo.
- Os backups em nuvem são considerados backups remotos também.

Definição da metodologia de backup - 9 tipos

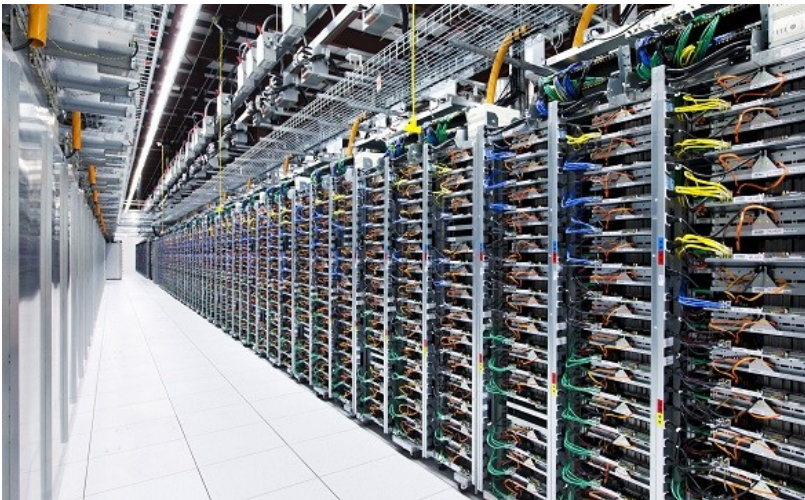
8. Backup em Nuvem

- Tipo de backup mais adotado atualmente por empresas de todos os tamanhos e áreas.
- Geralmente, os backups em nuvem são feitos continuamente. Para isso é preciso que a origem dos dados esteja conectada por uma rede ou conexão com a Internet à plataforma de armazenamento em nuvem.
- Para ter acesso ao backup em nuvem a empresa deve contratar uma plataforma de armazenamento. Ex. Google Drive, Dropbox, etc.

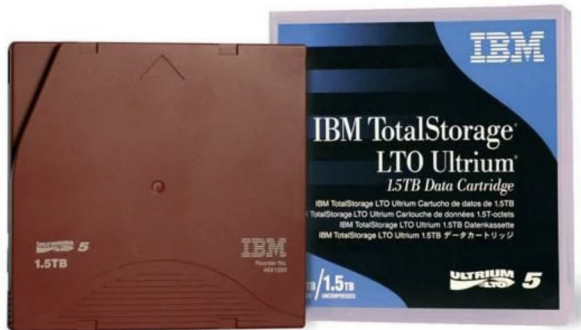
Definição da metodologia de backup - 9 tipos

9. Backup FTP

- Tipo de backup onde o processo de cópia dos arquivos é feito por meio da internet para um servidor FTP.
- O servidor FTP está localizado em um data center comercial, longe dos dados de origem que estão sendo armazenados em backup.



Definição da metodologia de backup - 9 tipos



Segurança Lógica

Autenticação é a capacidade de garantir que um usuário é de fato quem ele diz ser. É uma das funções de segurança mais importantes que um sistema operacional deve fornecer.

Os mecanismos de autenticação podem ser divididos em quatro categorias:

- **Algo que você sabe** - O mecanismo mais utilizado é o onipresente, par formado pelo nome do usuário e sua senha, assim como números PIN usados para acesso a Banco 24 Horas e combinações de cofres.
- **Algo que você tem** - Chaves de carro, cartões de banco 24 horas, e outros dispositivos físicos são mecanismos de autenticação que exigem a posse física de um usuário.
- **Algo que você é** - Impressões digitais, análise de retina e reconhecimento de voz são exemplos de mecanismos biométricos que podem ser usados para fornecer um nível alto de autenticação.
- **Algun lugar onde você está** - Endereços de adaptador de rede, e sistema baseado em Posicionamento Global via Satélite proveem informação de autenticação baseada na localização do usuário.

- Sistemas de autenticação forte geralmente requerem simultaneamente o uso de pelo menos dois destes mecanismos.
 - Por exemplo, o acesso a sua conta bancária em um banco 24 horas requer tanto a posse física do cartão 24 horas como o conhecimento do PIN.
- A confidencialidade da informação usada para autenticar os usuários é extremamente importante. Se você escrever o número do PIN no cartão 24 horas, a autenticação forte está perdida.
- Semelhantemente, se a informação de nome e senha do usuário trafegar abertamente através da rede, é impossível obter-se uma autenticação confiável.

- **Senhas**

- Senha de acesso é o método mais utilizado, pelas empresas para a autenticação de usuários. Para garantir o seu uso adequado, deve ser definida uma política de senhas, em que sejam criadas regras para a criação, troca e uso das mesmas.
- As regras definidas devem ser divulgadas a todos os funcionários e colaboradores da organização.
- Itens que devem ser abordados em uma política de senhas:
 - a senha sempre deve ser “criada expirada”, forçando a sua alteração no primeiro logon;
 - as contas de usuários demitidos, prestadores de serviço, ou usuários de teste devem ser imediatamente bloqueadas quando não forem mais utilizadas;

- **Senhas**

- os usuários devem poder alterar a própria senha e devem fazê-lo caso suspeitem que a sua senha foi "descoberta";
- o tamanho mínimo da senha deverá ser de 7 caracteres;
- a periodicidade da troca deve ser preferencialmente mensal. Caso não seja possível, deve ser feita no máximo trimestralmente;
- a senha deve ser composta de uma combinação de caracteres maiúsculos e minúsculos, sinais e números, que deve ser fácil de lembrar, porém difícil de ser descoberta;
- a senha não deve ser baseada em informações pessoais, como próprio nome, nome de familiares, bichos de estimação, nome de time de futebol, placa do automóvel, nome da empresa ou departamento, etc;
- não deve ser constituída de combinações óbvias de teclado, tais como 12345, asdfg;
- não deve existir senhas genéricas, a senha é pessoal e não deve ser compartilhada.

Auditoria

- Do ponto de vista da segurança, auditar é a capacidade de reconstruir um evento relacionado à segurança para auxiliar o exame das causas e efeitos de tal evento.
- Informações de log de sistema podem ser usadas para determinar se uma violação de política aconteceu ou se uma atividade suspeita é causa para alarme.
- Produtos sofisticados para detecção de intrusão usam trilhas de auditoria do sistema operacional como uma base para a sua análise.
- Trilhas de auditoria também fornecem a possibilidade de localizar a fonte de um incidente de segurança complexo e fornecem a evidência necessária para qualquer ação que pode ser requerida.

Integridade

- Integridade é a habilidade para assegurar que o conteúdo de um objeto não seja alterado por uma entidade sem autorização.
- Controles de acesso previnem mudanças sem autorização e são uma forma de proteção de integridade.
- A integridade representa um papel essencial em correio eletrônico e sistemas de comércio onde a garantia de que o conteúdo de uma mensagem está correto é mais importante que manter a mensagem confidencial.

Integridade

- Em um sistema de computador, a integridade se aplica tanto aos dados em armazenamento (arquivos de sistema, executáveis) e para dados em movimento (mensagens, transações).

Confidencialidade

Informações sensíveis podem existir em vários formatos em um sistema de computador:

- Armazenadas em um disco rígido ou outro armazenamento permanente;
- Armazenadas em memória volátil ou outro armazenamento temporário;
- Trafegando em uma rede;
- Trafegando em um sistema.

A confidencialidade é a garantia que a informação só esteja disponível aos usuários autorizados, independentemente de quem possui o recipiente que contém a informação.

Confidencialidade

- A implementação mais comum de confidencialidade é o uso de criptografia.
- Há outros modos de implementar confidencialidade: segurança física, acordos de não revelação, acordos de parceria comercial, etc.
- Os mecanismos de confidencialidade fornecidos pelos sistemas operacionais podem ser avaliados baseados na:
 - Força do mecanismo de proteção (tipicamente um algoritmo de criptografia).
 - Transparência do mecanismo de proteção.
 - Integração do mecanismo com outros controles de segurança do sistema.
 - Impacto do mecanismo na operação do sistema.