

**UNI
METRO
CAMP**

wyden

Introdução à Segurança da Informação - ARA0064

Prof. José Luiz Alonso Silva, MsC

E-mail: jose.lsilva@unimetrocamp.edu.br

4.2 - Controle de Acesso, Vírus e Backups

**UNI
METRO
CAMP**
wyden

Temas da Aula

- Controle de Acesso
- Backups

Temas de Aprendizagem

- | | |
|---|-------------------|
| 1. PRINCÍPIOS DA SEGURANÇA E O CICLO DE VIDA DA INFORMAÇÃO | |
| 1.1 SEGURANÇA DA INFORMAÇÃO | |
| 1.2 SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO | |
| 2. AMEAÇAS E VULNERABILIDADES À SEGURANÇA DE INFORMAÇÃO | |
| 2.1 TIPOS DE AMEAÇAS E VULNERABILIDADES | |
| 2.2 ATAQUES CIBERNÉTICOS | |
| 3. NORMAS DE SEGURANÇA DA INFORMAÇÃO | |
| 3.1 FINALIDADES E BENEFÍCIOS DAS NORMAS | |
| 3.2 APLICAÇÃO DAS NORMAS | |
| 4. BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO | |
| 4.1 SENHAS, TREINAMENTO E PROTEÇÃO | |
| 4.2 CONTROLE DE ACESSO, VÍRUS E BACKUPS | |
| 4.3 CRIPTOGRAFIA DE DADOS E CERTIFICADO DIGITAL | |
| 5. GESTÃO DE RISCO | |
| 5.1 PRESERVAÇÃO DA CONFIDENCIALIDADE, INTEGRIDADE E DISPONILIDADE (CID) | |
| 5.2 ETAPAS DA GESTÃO DE RISCOS | |
| 6. GESTÃO DE CONTINUIDADE DO NEGÓCIO (ATIVIDADE PRÁTICA SUPERVISIONADA) | |
| 6.1 PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN) | 6.2 ETAPAS DO PCN |
| 6.3 PGCN E BIBLIOTECA ITIL | |

Objetivo da Aula

- Identificar os recursos protegidos pelos sistemas de controle de acesso e os aspectos relacionados à política de vírus e ao gerenciamento de backups



Situação Problema

- Para que serve o controle de acesso?
- Importante Segurança Inform.
- Controlar o que será acessado
 - Hardware ou Software



Controle de Acesso

Elemento essencial de segurança

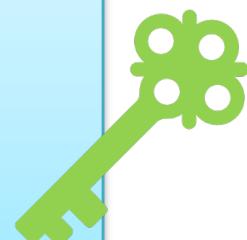
Determina quem tem permissão para acessar determinados dados, aplicativos e recursos e em que circunstâncias



Controle de Acesso

Uso de políticas, procedimentos, dispositivos, hardware e software, métodos qualificados de identificação e sistemas de bloqueios

Busca controlar e gerenciar o trânsito de pessoas, objetos e informações, num determinado espaço físico ou lógico



Elementos Chaves

Sujeito

- Entidade que solicita o Acesso
- Usuários, processos

Objeto

- Peça da informação acessada
- Arquivos, sistemas, bancos dados

Técnicas

- Como promover o controle
- Sistemas, equipamentos, biometria

Fluxo do Controle de Acesso

Identificar um usuário com base em suas credenciais

Autenticar o usuário

Autorizar do nível de acesso apropriado

Realizar auditoria

Fluxo de Controle de Acesso

- Identificação e Autenticação
- Primeira Etapa do Processo
 - Responsáveis por confirmar quem são os sujeitos que acessam os objetos
 - Mecanismos que permitam que o sujeito identifique quem ele é
 - Ex. Username , UserID, Login, pin

Fluxo de Controle de Acesso

- Autenticação é a confirmação da Identidade
- Tecnologias
 - Conhecimento: algo que o usuário saiba (senha)
 - Posse: algo que ele tem (tokens, *smartcards*, certificados digitais)
 - Características: traço físicos
- Autenticação forte
 - Deve ser multifator, 2 ou mais tecnologias (biometria)

Objetivo

Objetivo Controle de Acesso

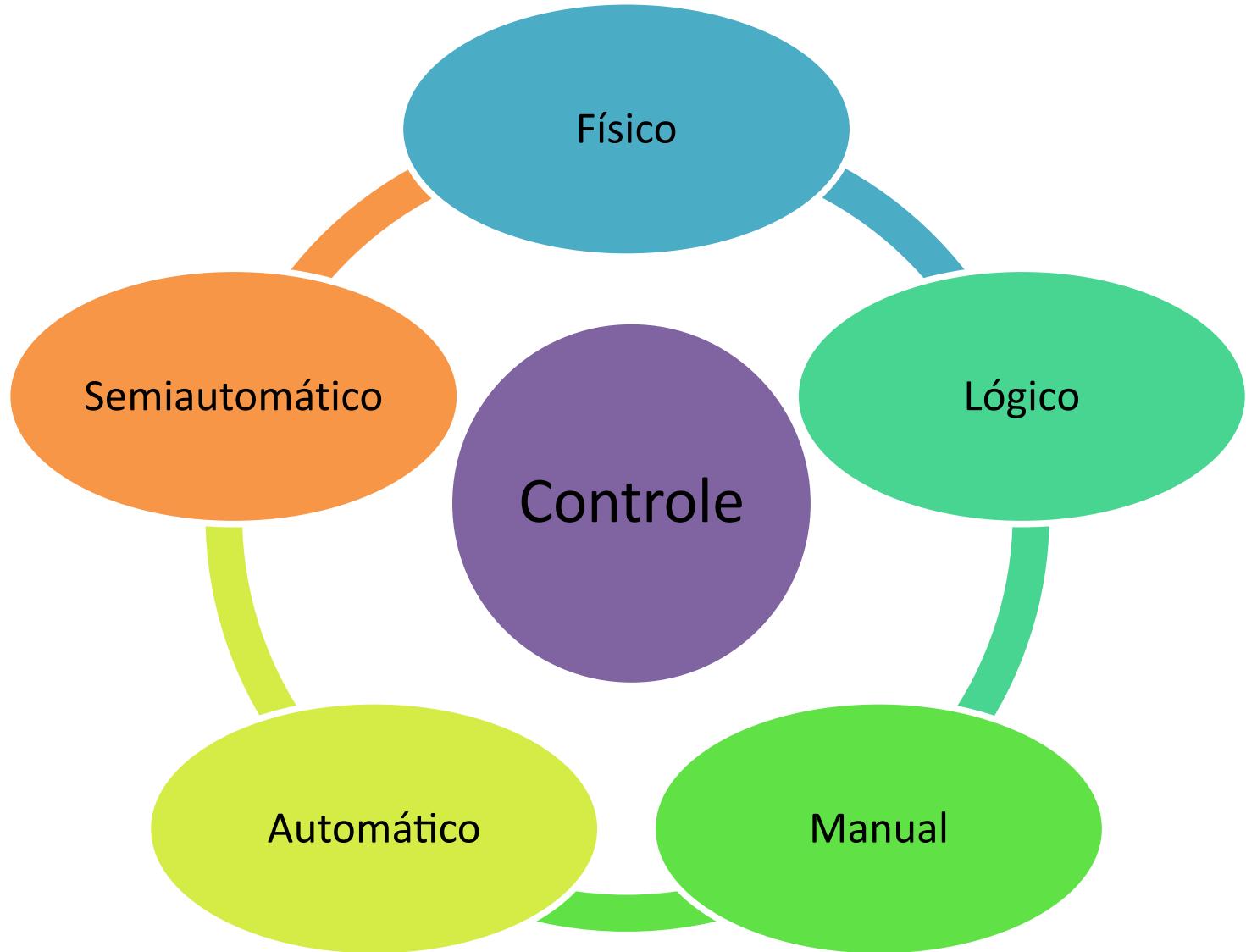
Proteger de acessos não autorizados

Gerenciar permissão de Acesso

Permitir rastreabilidade de acesso

Proteger Ativos Organizacionais

Controlar o Acesso



Função e Funcionamento

Controle de Acesso

Quanto ao Funcionamento

Manuais operados exclusivamente pela ação humana

Semiautomáticos integram pessoas com a tecnologia

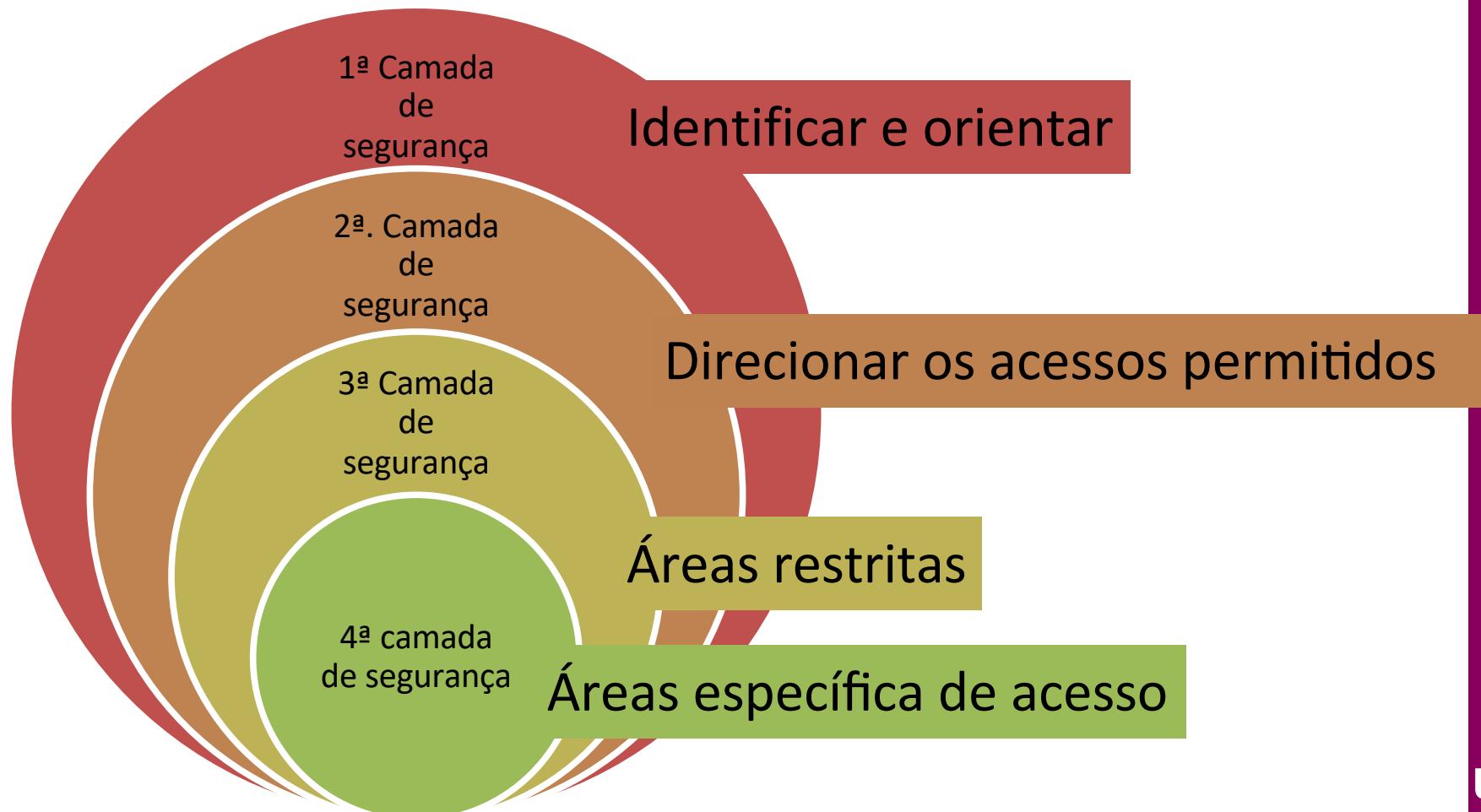
Automáticos não dependem diretamente da ação humana, operam com tecnologia

Quanto a Função

Gerenciamento de acesso ao espaço virtual
Redes e bancos de dados, dispositivos, equipamentos informatizados

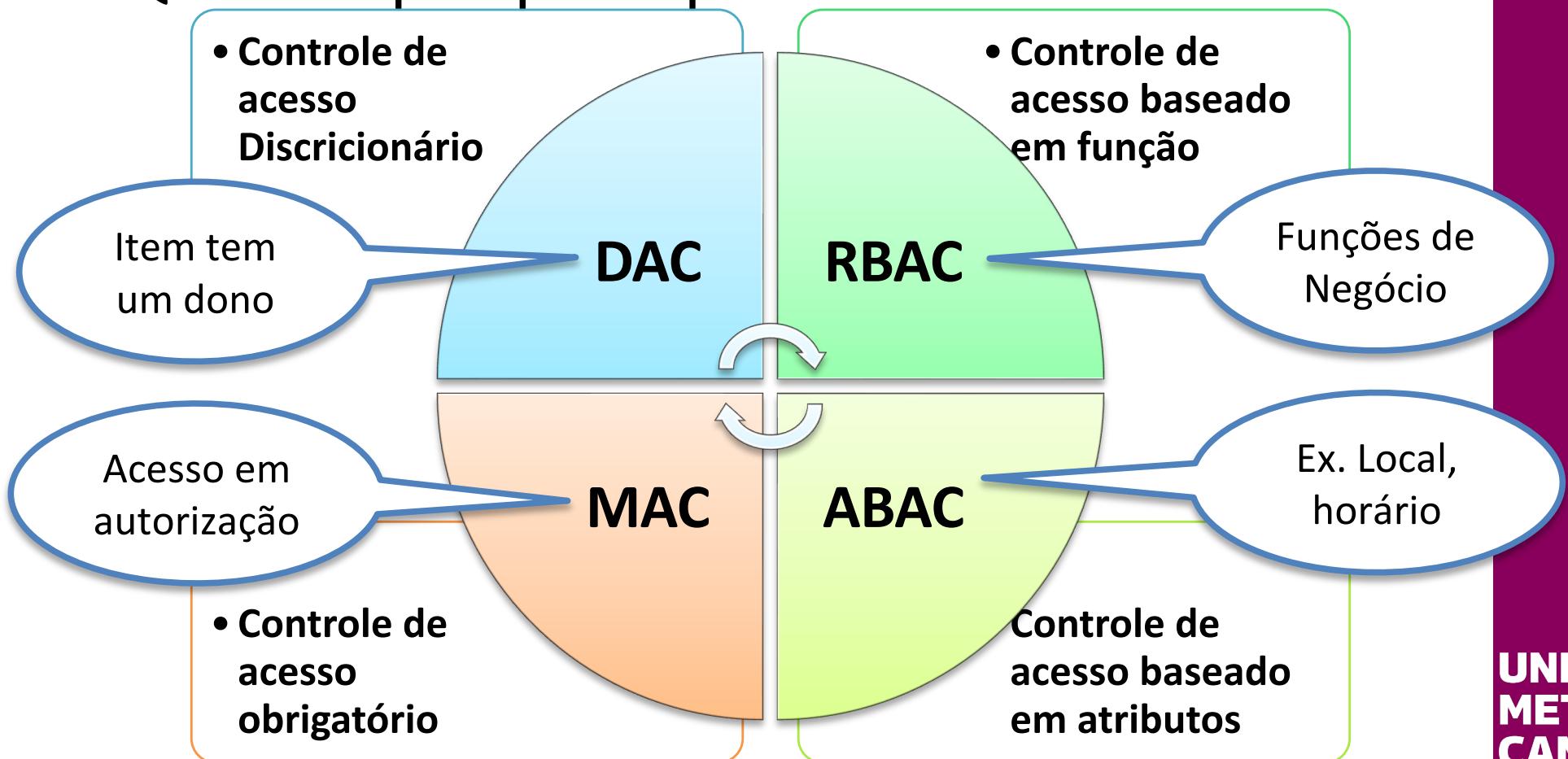
Gerenciamento de acesso espaço físico
Instalações, áreas, salas entre outros

Camadas de Controle de Acesso



Tipos de Controle de Acesso

- Quatro tipos principais



Como Realizar o Controle de Acesso

Uso de
Tecnologias
e/ou
Métodos

Gerenciamento do Acesso a determinados ambientes
ou sistemas

Hardware

Senhas, pins

Software

Cartão de proximidade, tags

Biometria

Código de Barras

MFA – Autenticação Multifator

Antes de liberar o Acesso

Confirmar os requisitos de negócios para que se estabeleça uma identidade

Verificar a identidade de uma entidade antes de atribuir-lhe uma identidade lógica

Estabelecer uma identidade

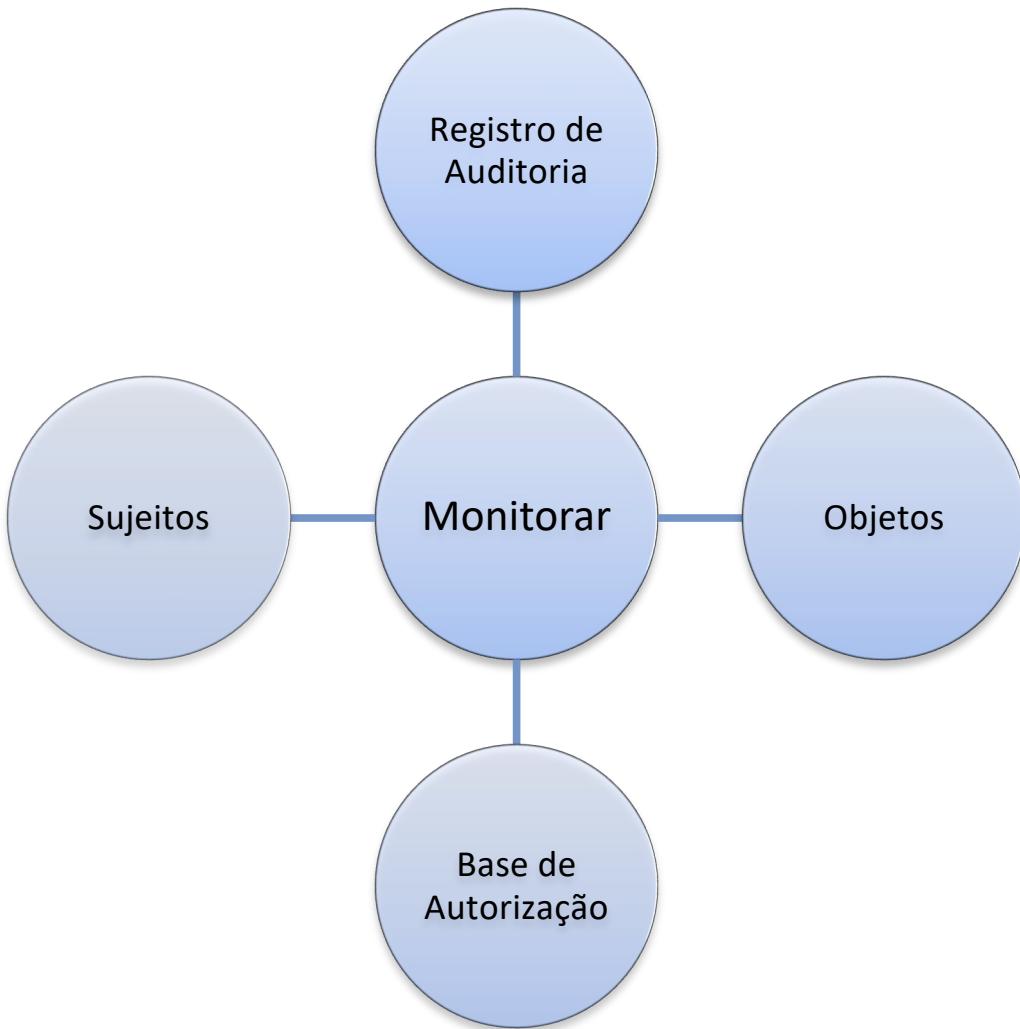
Configurar e ativar a identidade

Conceder ou revogar direitos específicos de acesso à identidade

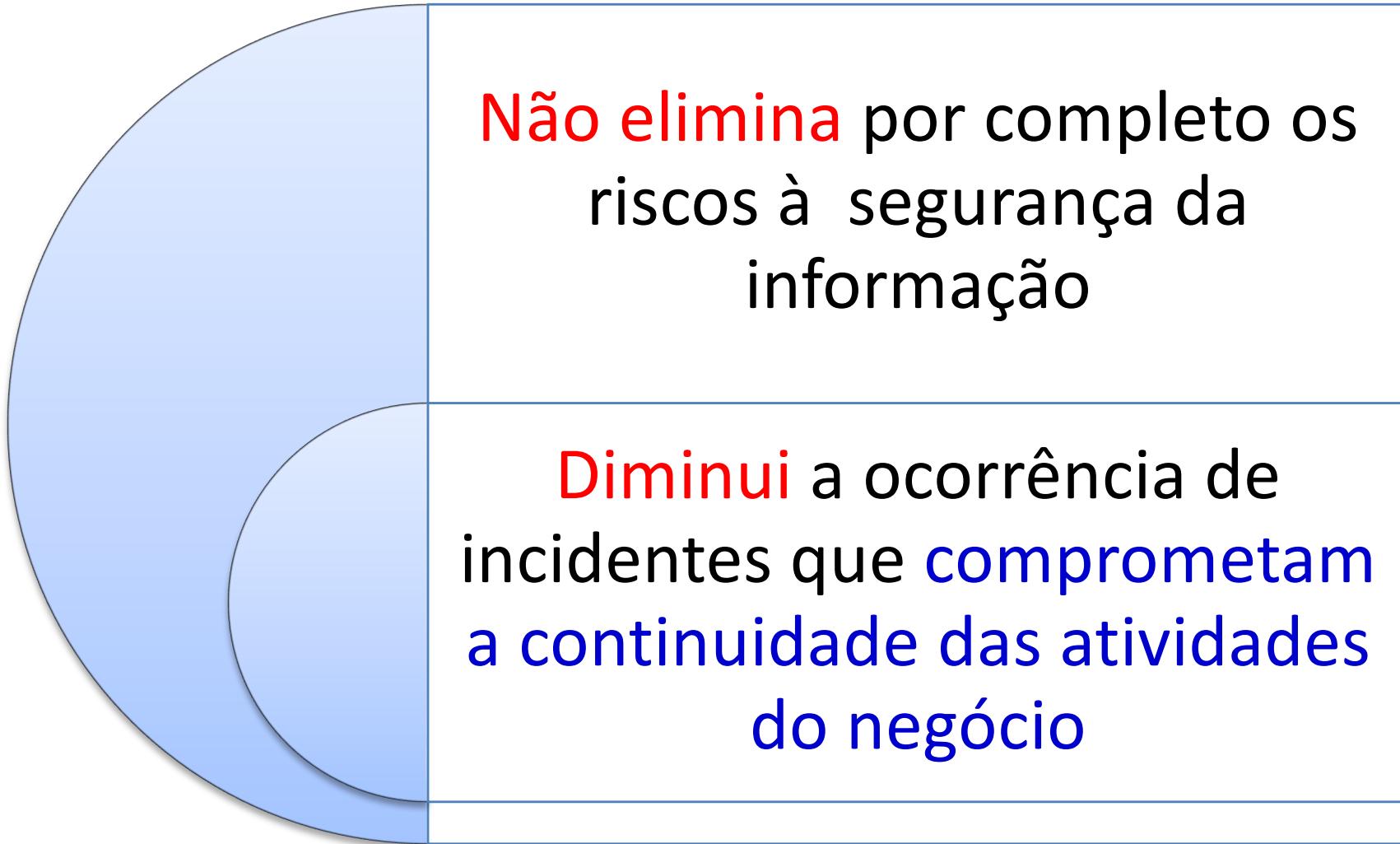
Atividades do Controle de Acesso

- Registro e cancelamento acesso do usuário
- Provisionamento de acesso de usuário
- Gestão de direitos de acesso privilegiado
- Gestão de informações secretas de autenticação
- Revisão dos direitos de acesso de usuário
- Remoção ou ajuste dos direitos de acesso

Atividades do Controle de Acesso



Restrição de Acesso



Backup

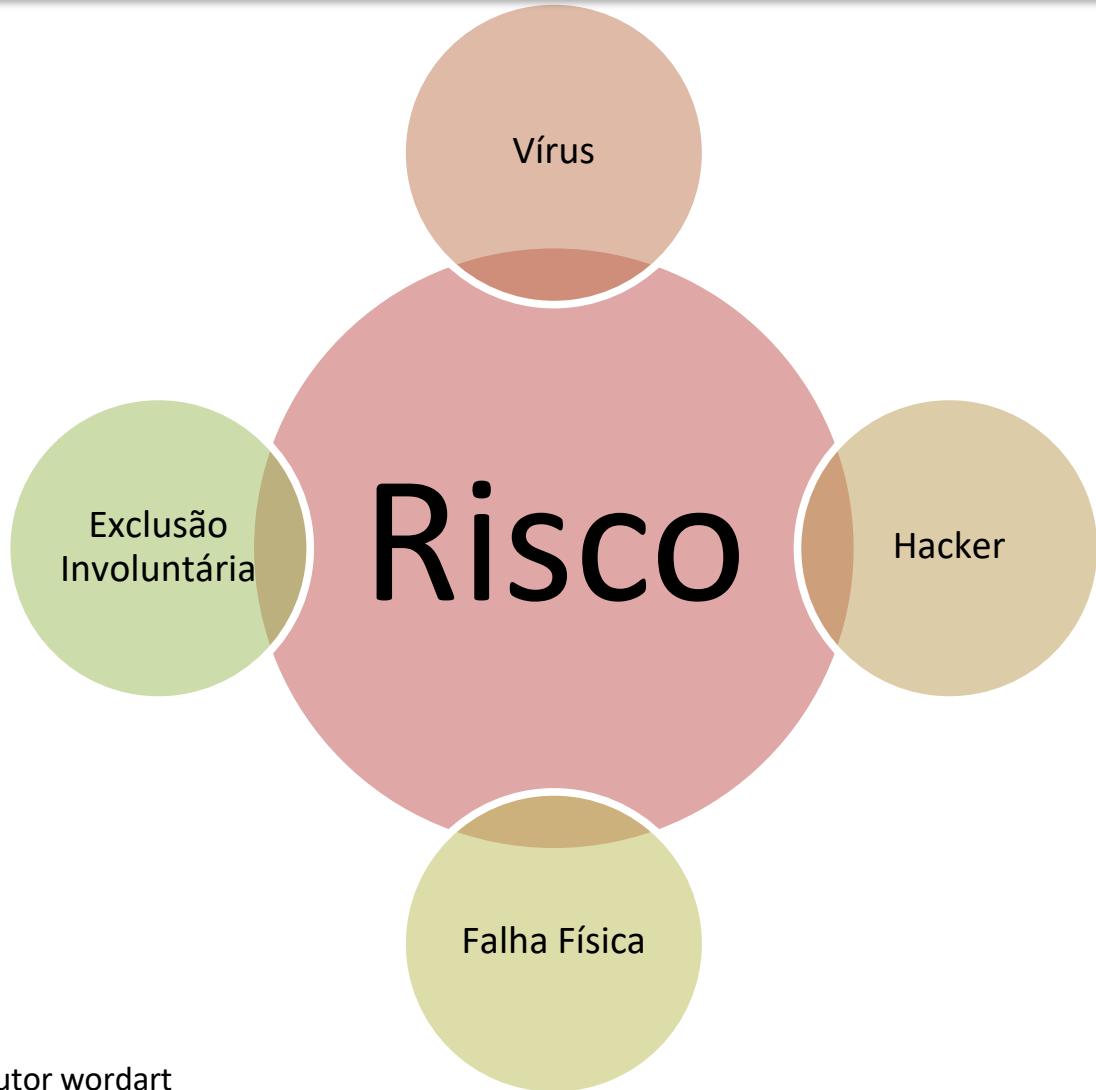
cópia de
segurança

- Ato de copiar arquivos, pastas ou discos inteiros (físicos ou virtuais) para sistemas de armazenamento secundários

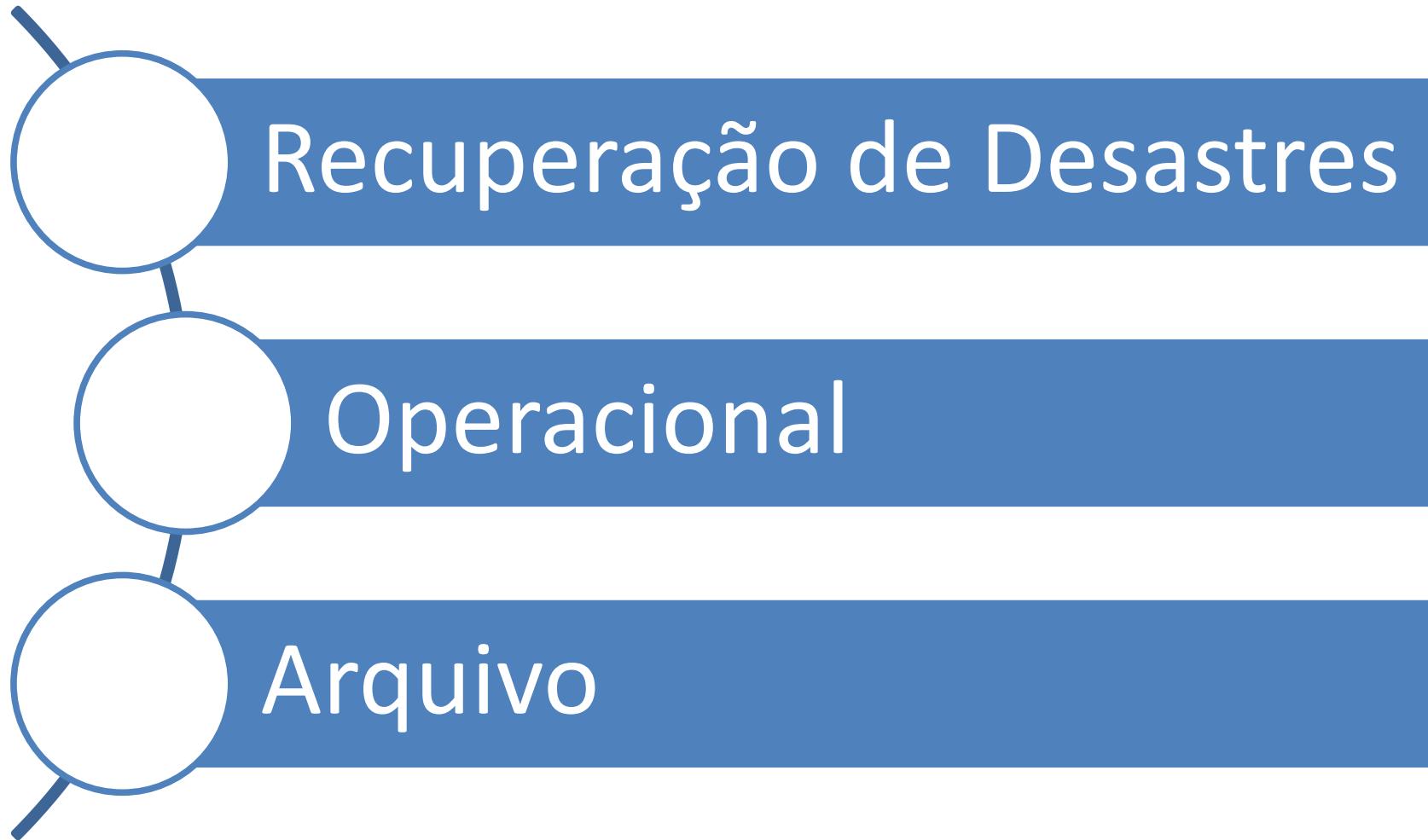
Preservação dos dados em
caso de qualquer
problema

Backup

Recuperar dados apagados e/ou corrompidos

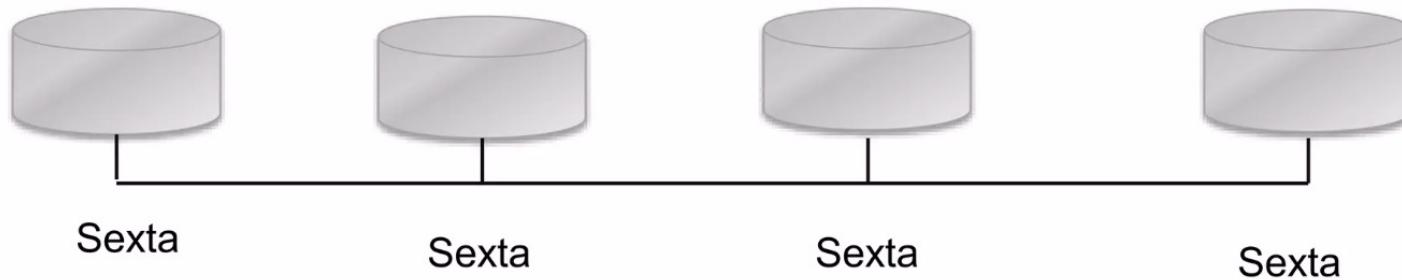


Objetivo do Backup



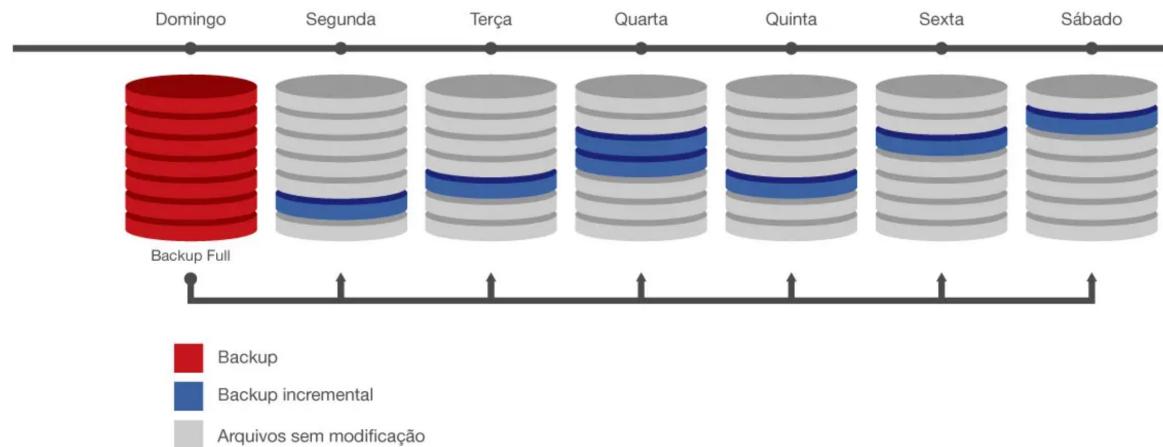
Tipos de Backup

- Completo
 - Periodicamente



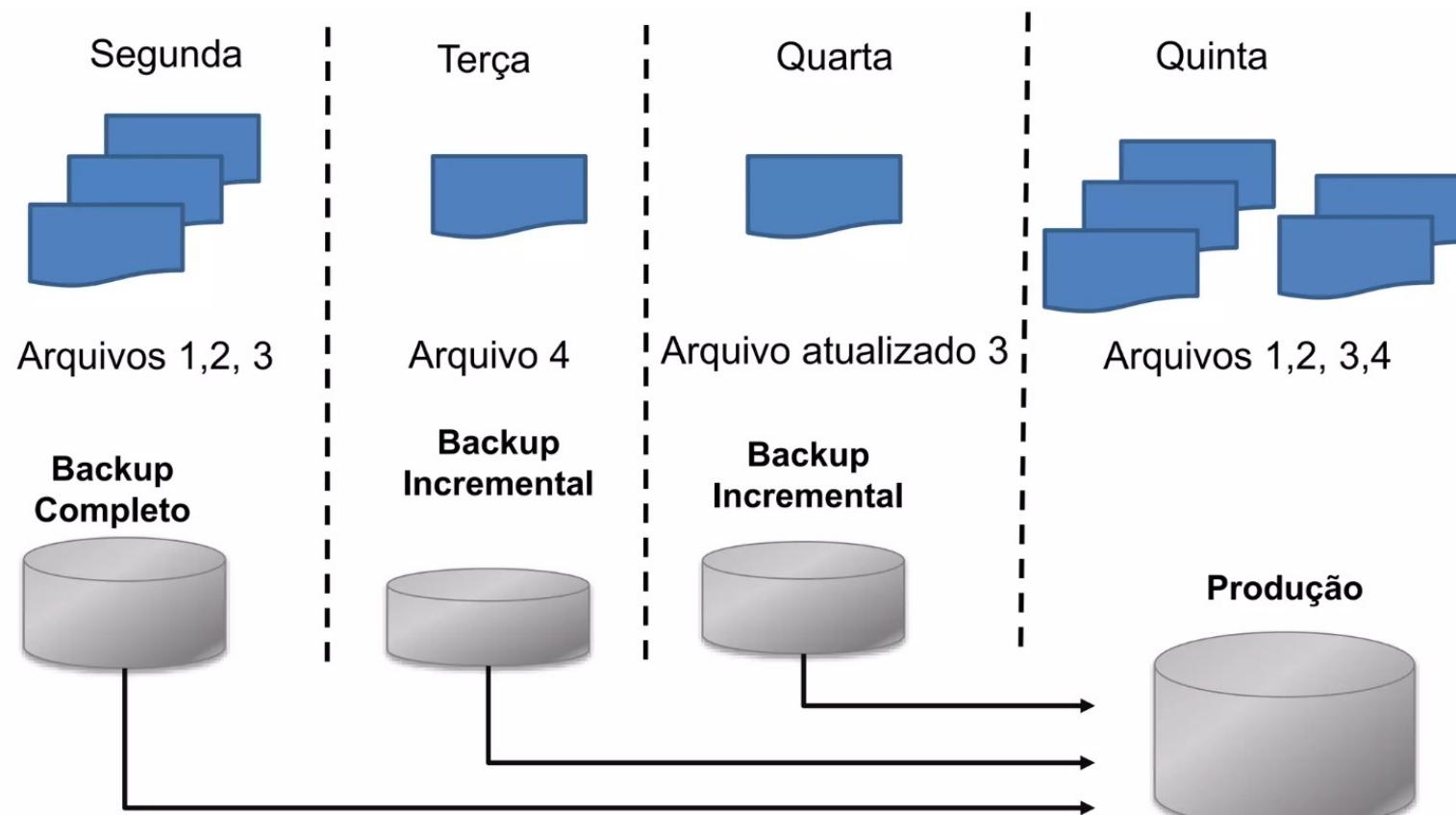
Tipos de Backup

- Incremental
 - Processo gera apenas um fragmento
 - Cada operação, é menor que a cópia completa de tudo que existe desde o último **backup completo**



Tipos de Backup

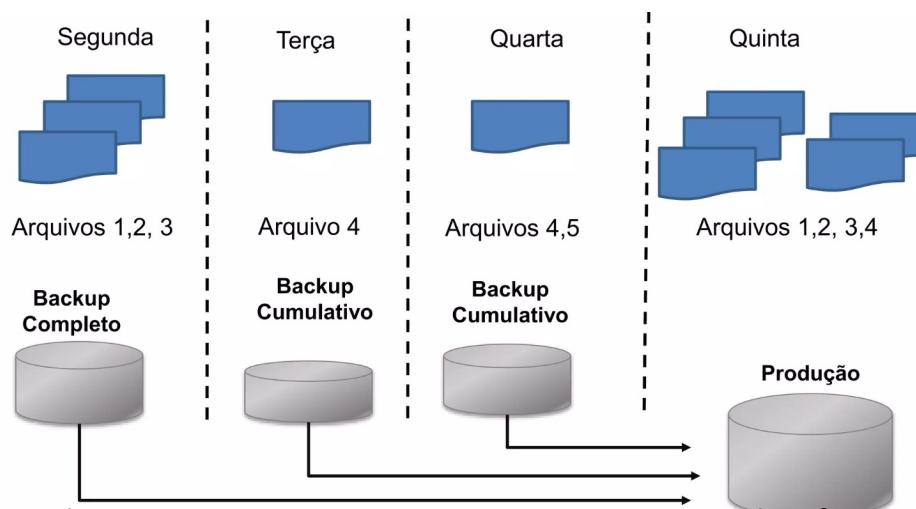
- Incremental e/ou cumulativo



Fonte: SOMASUNDARAM 2011

Tipos de Backup

- Diferenciais
 - Copia os dados alterados desde último backup completo
 - Similar ao incremental, pois ambos fazem cópia dos dados alterados

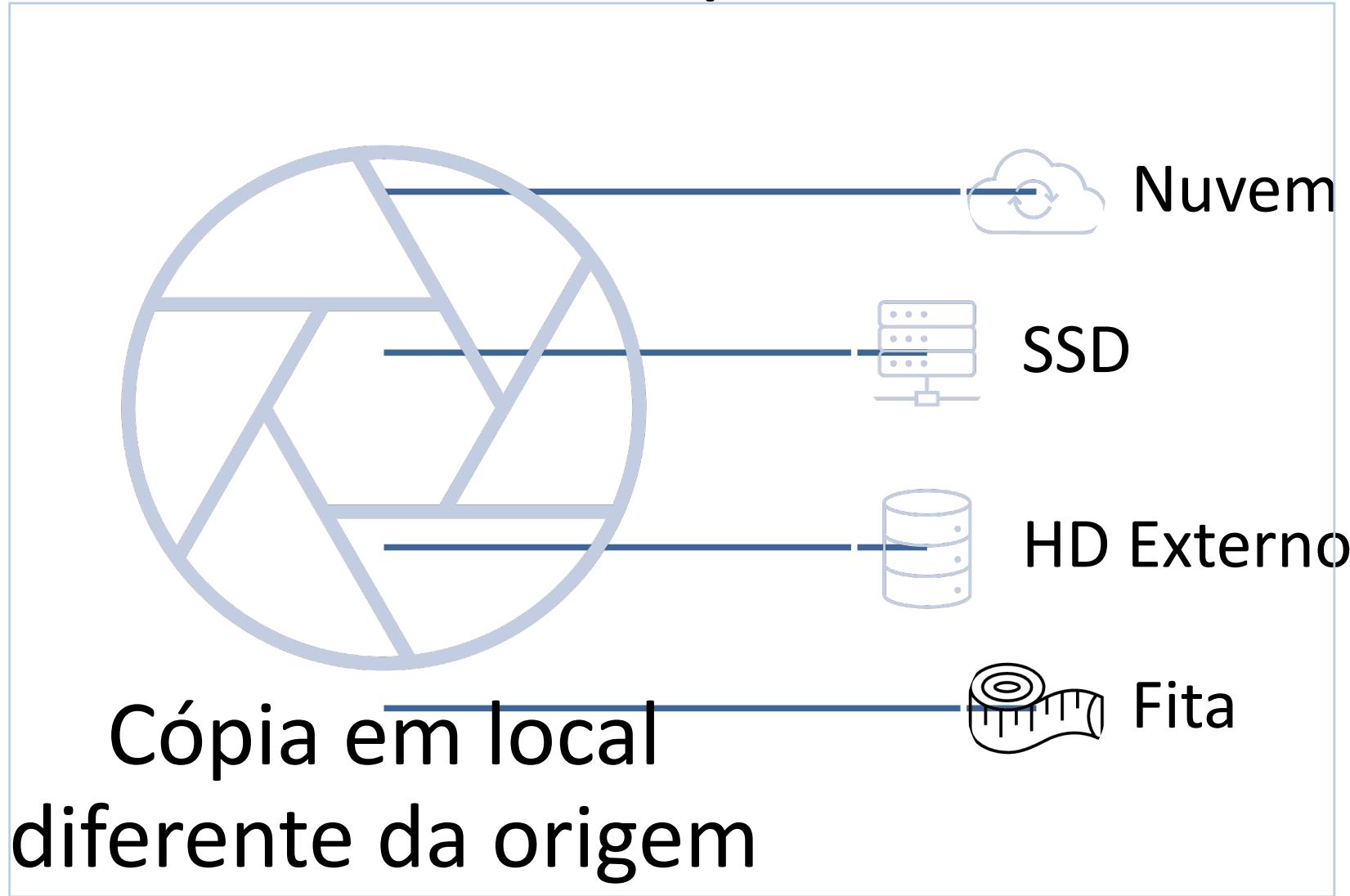


Tipos de Backup

- Vantagens e Desvantagens

Tipo de backup	Vantagem	Desvantagem
Completo	Menor tempo para recuperar os dados	Levam mais tempo para ser executado.
Incrementais	Backup será realizado mais rápido	Recuperação dos dados envolve um procedimento mais complexo
Diferencial	Restauração rápida	Backups mais demorados e maiores

Backup



Backup

Formas de Realizar

Manual

Automático

Pessoas

Cópia
Manual

Sem
Interferência
Pessoas

Software
executa

Backup

- *Restore* (Restauração)

Reativar todos os dados
salvos no backup

Backup

Política de Backup

- Dados a serem guardados
- Frequência
- Tipo (Manual ou automático)
- Controle de versão
- Ciclo de vida (quanto tempo)
- Restauração

Backup

Estabeleça uma Rotina
de Backup

Duvidas, considerações ...



Referências

- BAARS, Hans. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.** Rio de Janeiro ? RJ ? Editora Brasport, 2018. Capítulo 10 e 13. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044>
- GALVÃO, Michele da Costa, Agnaldo Aragon. **Fundamentos em Segurança da Informação.** Rio de Janeiro ? RJ: Editora Pearson, 2015. Capítulo 4. Disponível em: <<https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525>>

Referências

- MANDARINI, M.; **Segurança Corporativa Estratégica.** 1. Ed. Manole. Barueri, 2005
- URPURA, Philip P. ***Security and Loss Prevention.*** 3ed. Newton, Massachusetts. Butterworth Heinemann, 1998

Atividade aula 9

- Pesquise sobre ferramentas de Backup e Restore
 1. Nome do produto
 2. Link do produto
 3. Principais características



- Mínimo de 3 e máximo de 6 integrantes
- Responder no Forms: <https://forms.office.com/r/v7xEiWff7v>

Para Próxima Aula

Assista aos vídeos

- Segurança da Informação Confidencialidade, Integridade e Disponibilidade:
<https://www.youtube.com/watch?v=3vhz3IFjl7M>
- INFORMÁTICA Princípios da SEGURANÇA DA INFORMAÇÃO | REVISÃO rápida com Mapa Mental Explicado:
<https://www.youtube.com/watch?v=T3CkJMZCrL8>
- Não repúdio Segurança da Informação Dicionário de Informática:
https://www.youtube.com/watch?v=Nzb_qGPj

**UNI
METRO
CAMP**
wyden