



Estácio

Introdução à Segurança da Informação

Prof. Dr. José Augusto de Sena Quaresma
Jq.quaresma12@gmail.com

Agenda

- Apresentação do docente
- Apresentação dos alunos
- Apresentação da disciplina
- Composição das atividades
- Conceitos básicos



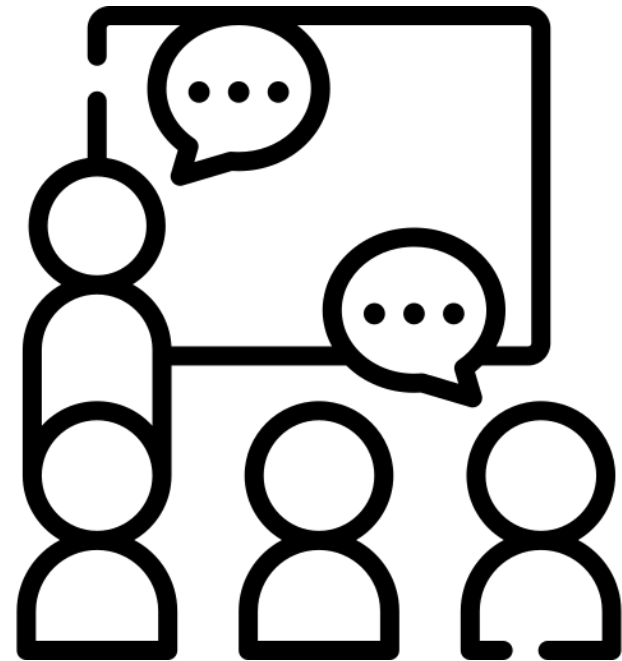
José Augusto Quaresma

- Professor da Estácio
- Teach Lead – Cielo
- Certificado Implementador MPS.BR
- Bacharel em Sistemas de Informação
- Especialista em Gestão da Tecnologia da Informação
- Mestre em Ensino
- Doutor em Ciência da Computação



Apresentação dos alunos

- Nome
- O que espera da disciplina?
- O que espera do curso ?



Apresentação da disciplina

- Ementa
- Objetivos
- Procedimentos de ensino e aprendizagem
- Conteúdos ministrados
- Procedimentos de avaliação
- Bibliografia básica
- Bibliografia Complementar



Ementa

- Princípios da segurança e o ciclo de vida da informação
- Ameaças e vulnerabilidades à segurança de informação
- Normas de segurança da informação
- Boas práticas em segurança da informação
- Gestão de risco
- Gestão de continuidade do negócio (crédito digital)



Objetivos

- Identificar os elementos da segurança da informação, conforme conceitos, princípios e normas, bem como referências do CERT.br, para ambientar se à área da segurança, e destacar sua importância;
- Definir formas de preservar a informação, utilizando técnicas de controle de acesso e proteção, para minimizar a ocorrência de incidentes de segurança;
- Examinar boas práticas, baseado em políticas de segurança da informação, para destacar a importância dos fatores humanos e estimular a conduta profissional que vise a manutenção de um ambiente de trabalho seguro e produtivo.



Conteúdo

- 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



Conteúdo

- 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 disponibilidade (cid)
 - 5.2 etapas da gestão de riscos
- 6. Gestão de continuidade do negócio
 - 6.1 plano de continuidade de negócios (PCN)
 - 6.2 Etapas do PCN
 - 6.3 PGCN e biblioteca ITIL

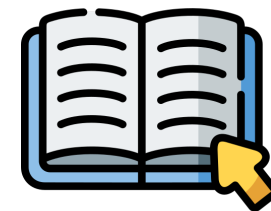


Procedimentos de ensino e aprendizagem

- Aula teórica e prática com participação dos alunos
- Lista de exercício
- Sala de aula invertida (apresentações)
- Projetos práticos
- Avaliando aprendizagem

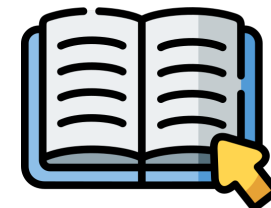


Bibliografia básica



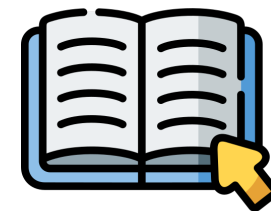
- CABRAL, Carlos.; CAPRINO, Willian. Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados. 1. Rio de Janeiro: Brasport, 2015. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/160689>
- HINTZBERGEN, Jule. et. al. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.. 1. Rio de Janeiro: Brasport, 2018. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044>
- STANEK, William R. Windows Server 2012: Guia de Bolso. 1. Porto Alegre: Bookman, 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788582601693/>

Bibliografia complementar



- BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. Manual de Investigação Cibernética: à luz do Marco Civil da Internet. 1. Rio de Janeiro: Brasport, 2016. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/160741>
- GALVÃO, Michele da Costa. Fundamentos em Segurança da Informação. 1. São Paulo: Pearson, 2015. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525>
- MANOEL, Sérgio da Silva. Governança de Segurança da Informação: como criar oportunidades para o seu negócio. 1. Rio de Janeiro: Brasport, 2014. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/160684>

Bibliografia complementar (continua)



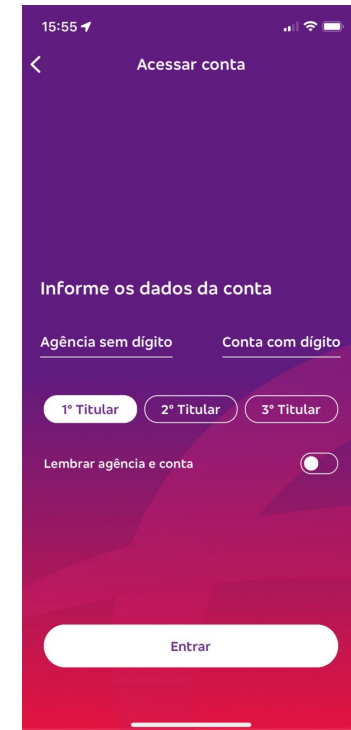
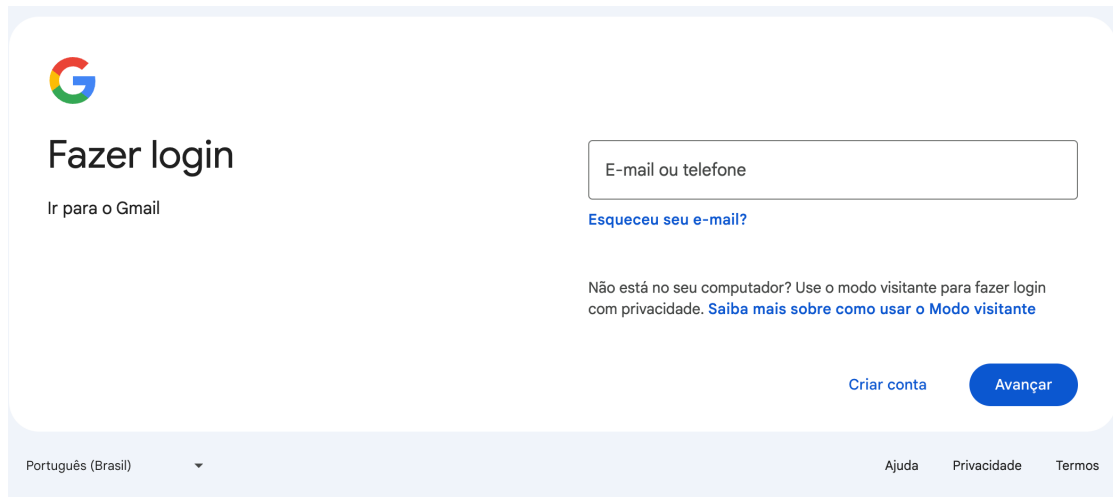
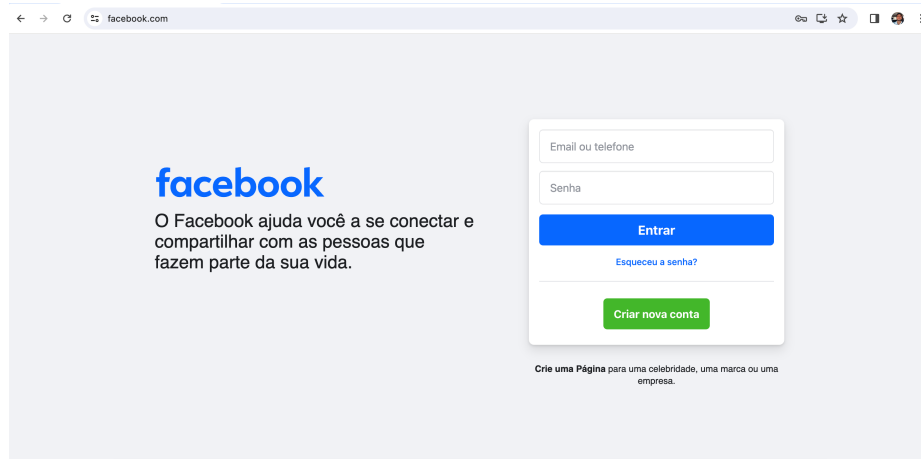
- STALLINGS, William. Criptografia e Segurança de Redes: princípios e práticas. 4. São Paulo: Pearson, 2008.
Disponível em:
<https://plataforma.bvirtual.com.br/Acervo/Publicacao/396>
- VANCIM, Flávia. Gestão de Segurança da Informação. 1. Rio de Janeiro: Seses, 2016. Disponível em:
<https://repositorio2.azurewebsites.net/api/objetos/efetuaDownload/70c5eeeece67944b9b8d4d1b7e9215631>

Nosso grupo no Whatsapp

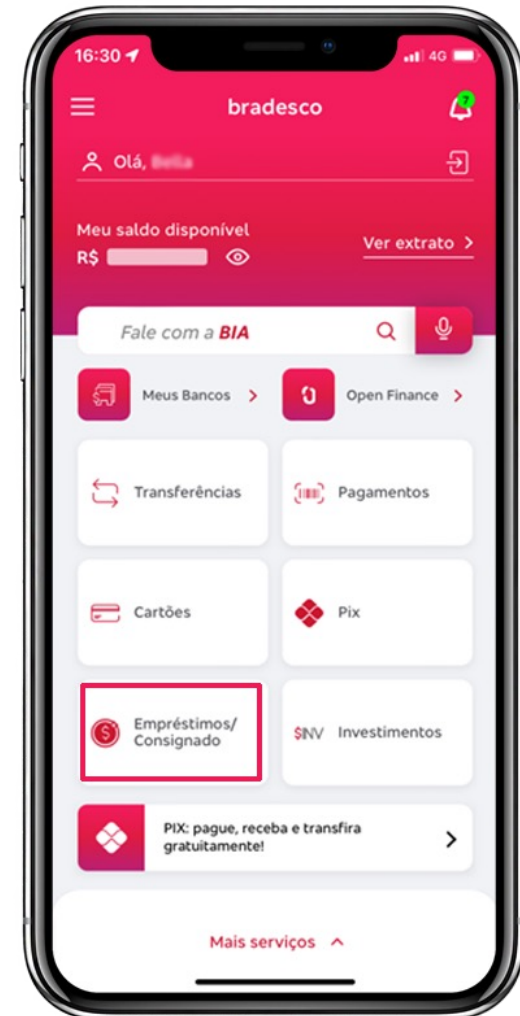
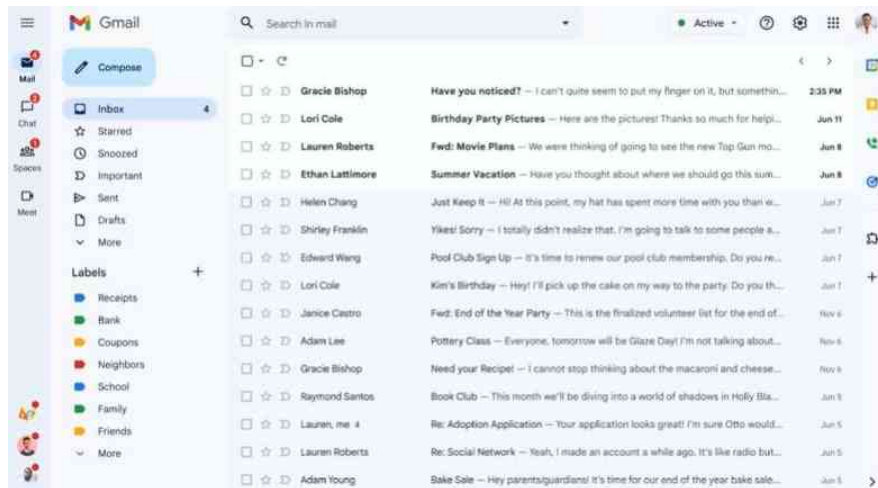
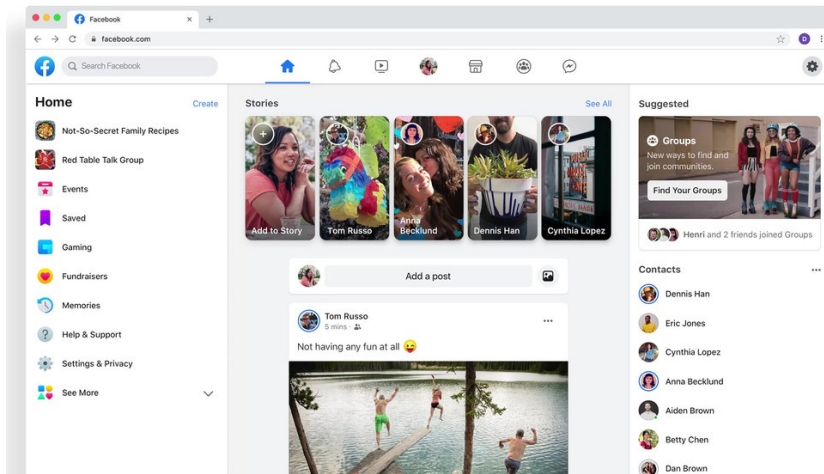


Importância da Segurança da Informação

Importância da Segurança – Login



Importância da Segurança – Acesso



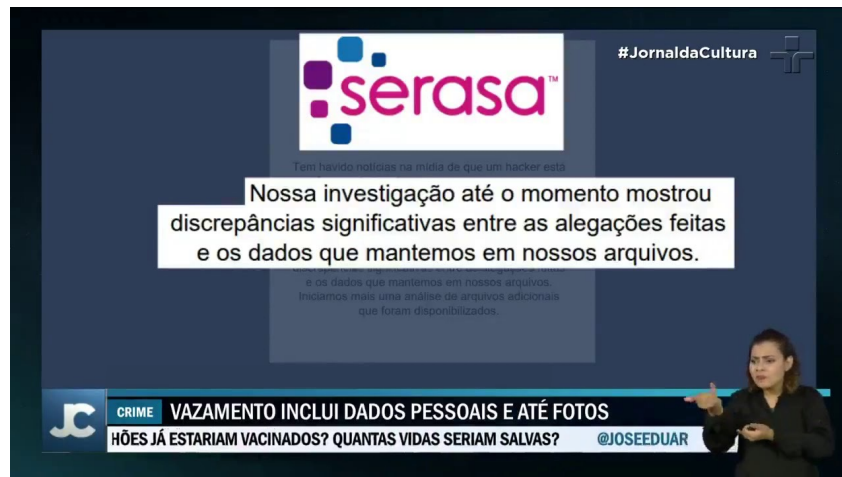
Computação

**Introdução à Segurança
da Informação**

Importância da Segurança – Transações digitais



Importância da Segurança – Vazamento de dados



Importância das informações para as empresas

Importância da informação – Empresa

- O que as empresas precisam?
 - Solucionar um problema
 - Identificar como fazer – Informação
 - Melhorar o que é feito – Manipulação da informação
 - Identificar público alvo

- A informação é essencial para a continuidade dos negócios



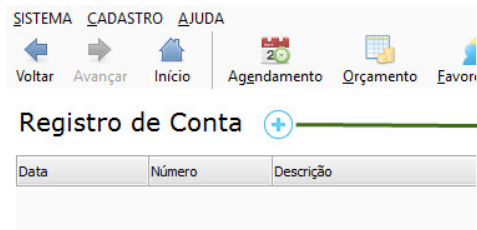
Importância da informação – Empresa (cont...)

- Informação é um ativo para a empresa
 - Devem ser protegidas
 - Permite a continuidade do negócio
 - Maximiza o retorno de investimento/ oportunidades
 - Minimiza transtornos
- Informação está em constante risco
 - Proteção dos negócios
 - Lei geral de proteção de dados

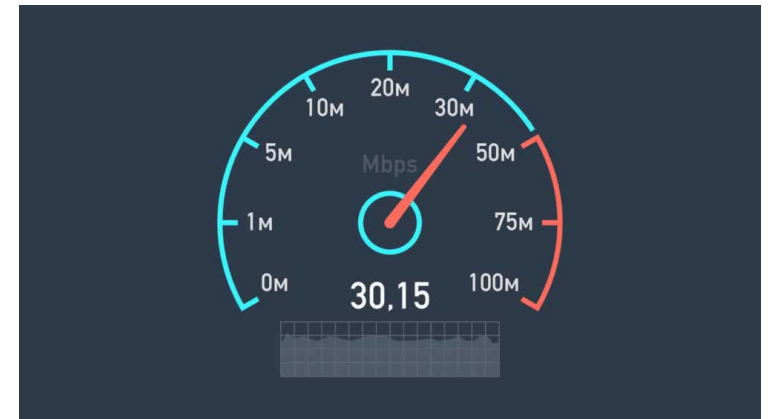
Conceitos iniciais

Conceitos – Dado

- É um evento registrado
- Um dado é fácil de se representar, manipular e transportar.



Clique no botão *Novo* (+) da tela *Registro de Conta*, para abrir o cadastro da transação.



Conceitos – Informação

- Um agrupamento de dados em um determinado contexto
- A informação tem significado e solicita uma transmissão mais elaborada.



Acesso à Informação

[illegible]

- O conhecimento são informações inter-relacionados e não identifica como usar
- A transmissão passa a ser mais complexa

[illegible][illegible]

Conceitos – Sabedoria

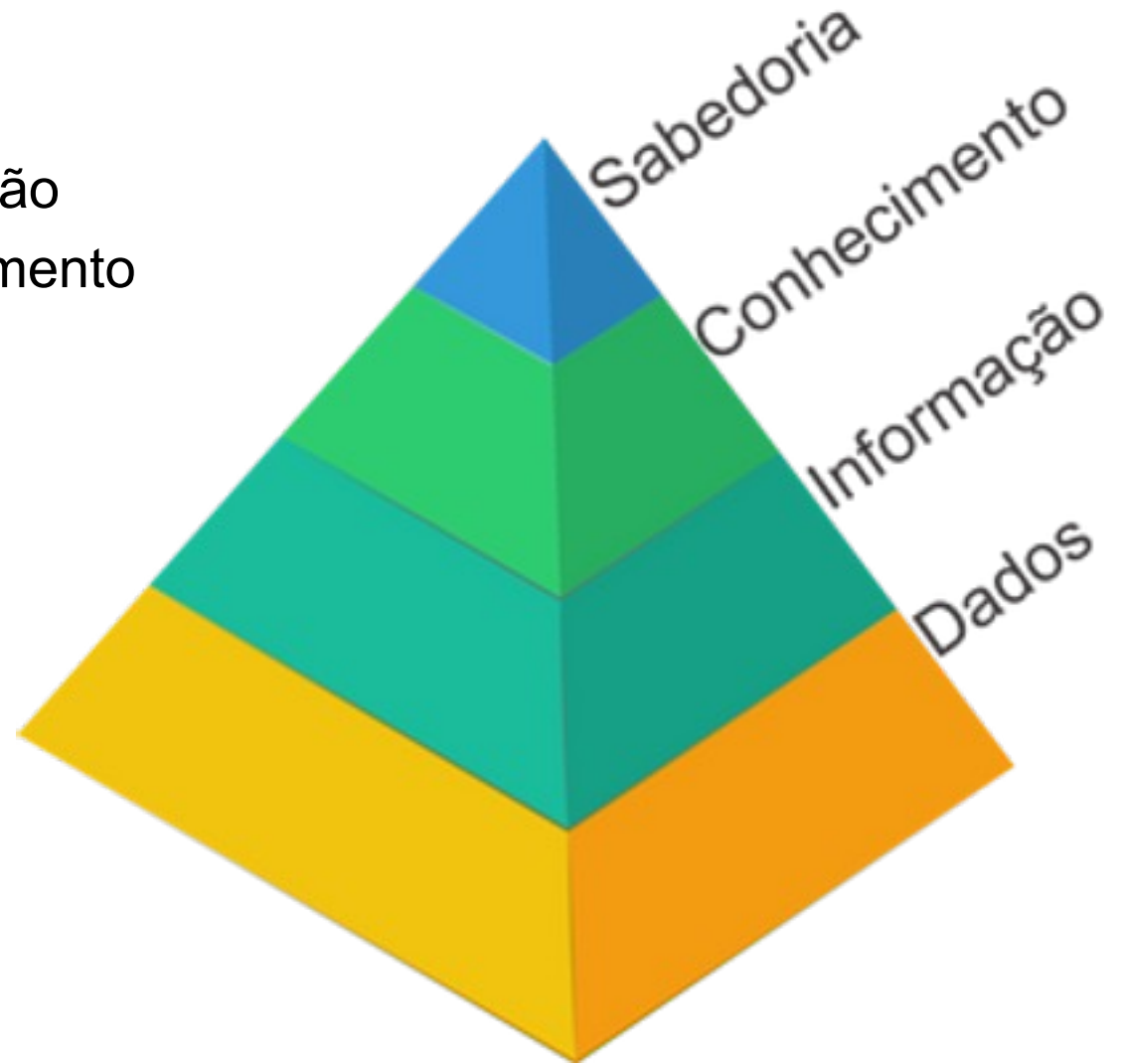
- A sabedoria aprimora o conhecimento trazendo o entendimento de uso
- A transmissão passa a ser mais complexa e exige prática.



Conceitos – Hierarquia DIKW

➤ DIKM:

- Data – Dado
- Information – Informação
- Knowledge – Conhecimento
- Wisdom – Sabedoria



Conceitos – Hierarquia DIKW



Fonte: https://www.researchgate.net/figure/Figura-4-Sequencia-hierarquica-dado-informacao-conhecimento-inteligencia_fig3_308296178

Ciclo de vida da informação

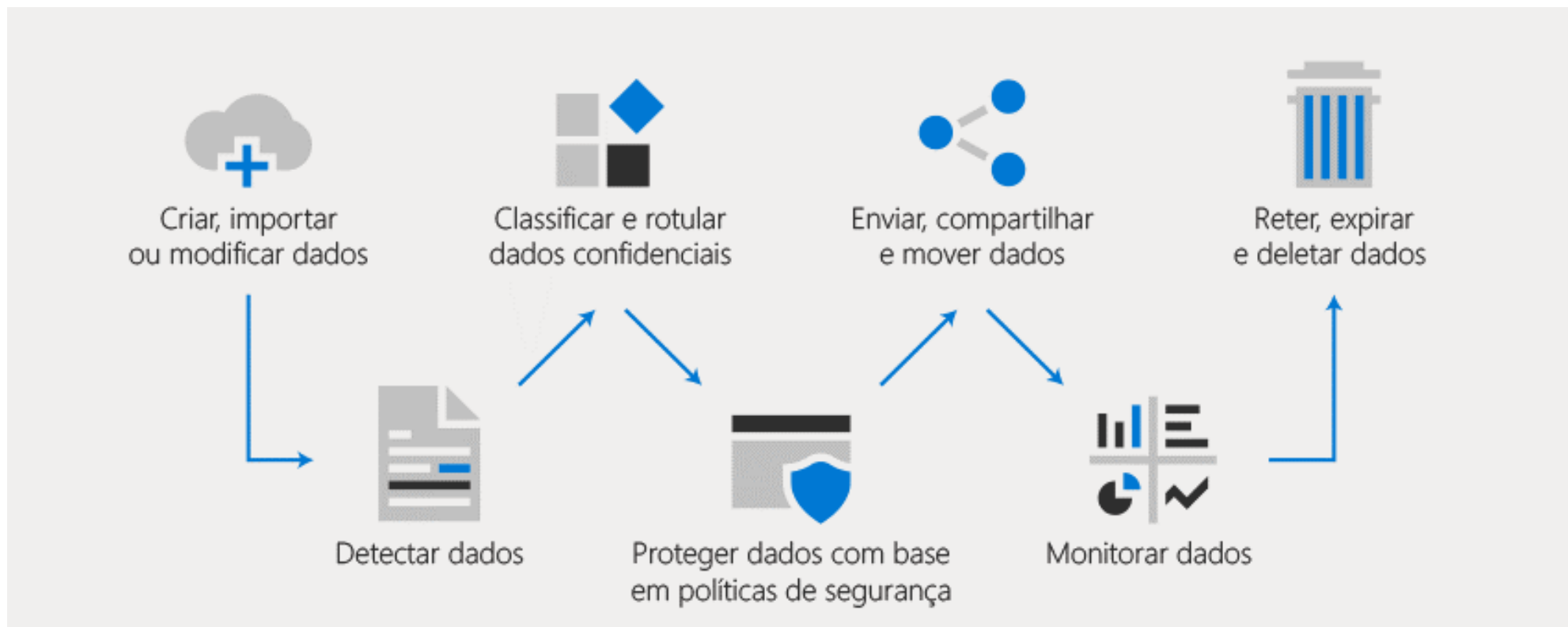
Ciclo de vida da informação

- A informação não é eterna



Ciclo de vida da informação - Empresarial

- É necessário fazer e mapear o ciclo de vida da informação adotado dentro da empresa



Fonte: <https://safe compliance.com.br>

Princípios da Segurança da Informação

Equação da Segurança da informação

- A segurança da informação é inversamente proporcional a praticidade.

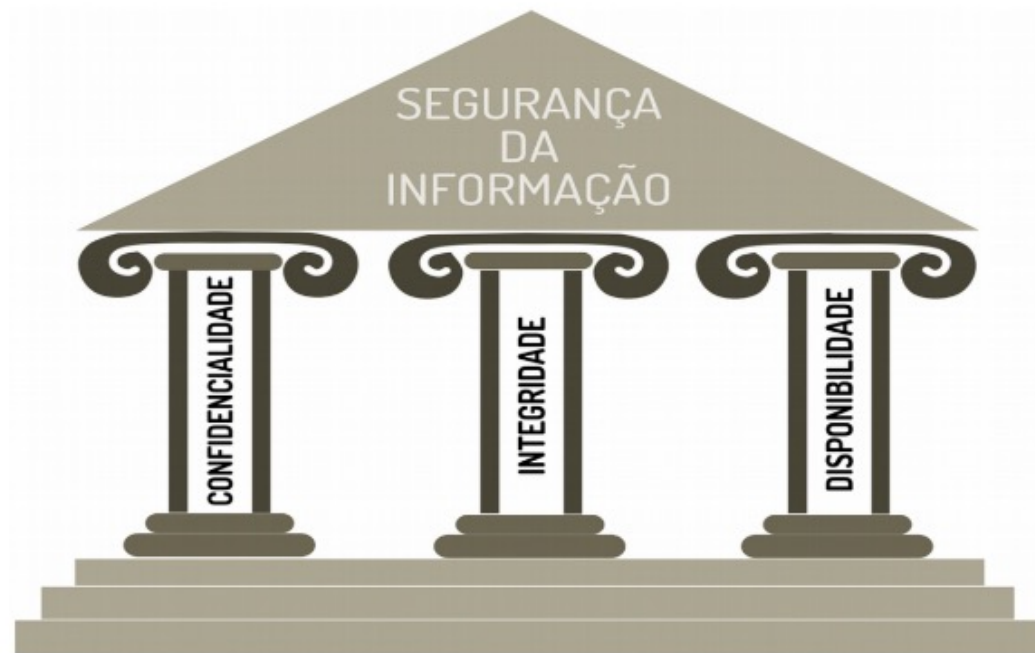
$$Praticidade = \frac{1}{Segurança}$$

- Quanto mais segurança menos praticidade
- Quanto mais praticidade menos segurança
- E agora, como agir nas empresas ?



Princípios fundamentais

- Confidencialidade
- Integridade
- Disponibilidade



Confidencialidade

- Só quem acessa é quem pode acessar
- Classificação das Informações
 - Públicas
 - Publicação ou perda não tem consequências prejudiciais
 - Internas
 - Publicação ou perda não tem consequências sérias
 - Confidenciais
 - Publicação ou perda pode acarretar problemas significativos, com perdas financeiras, de clientes ou de credibilidade
 - Secretas
 - Publicação ou perda pode ser desastrosa para os negócios

Integridade

- Informação sem adulterações espúrias
- Garantias
 - A informação não foi perdida
 - A informação não foi alterada indevidamente

Disponibilidade

- Sempre acessível
- Pontos relevantes
 - Disponível em tempo hábil
 - Indisponibilidade = perda de informação
 - Apenas para aqueles têm acesso

Hexagrama Parkeriano

- Proposto pelo prof. Donn B. Parker
- Confidencialidade
 - Posse
- Disponibilidade
 - Utilidade
- Integridade
 - Autenticidade



Posse

- Controlar quem pode ter acesso
 - Quem guarda/controla esses dados
- Dados vazados
 - Se não forem usados/analisados...
 - Não houve quebra de confidencialidade
 - Houve, porém quebra na “posse”
 - Os dados estão em posse de quem não devia

Autenticidade

- Identidade do autor é a enunciada?
- Em conjunto com confidencialidade
 - O leitor é quem diz ser?
- Em conjunto com integridade
 - O autor da mensagem é quem diz ser?

Utilidade

- Os dados permanecem úteis?
- Dados criptografados com perda de chave
 - Podem estar disponíveis
 - Podem estar íntegros
 - Podem se manter confidenciais
 - Podem estar em posse de pessoa adequada
 - Podem ser autênticos...
 - Mas são inúteis!

Atividade

Atividade – em grupo – Fase 01 (Projeto)

- Pesquise na internet casos reais de falhas de segurança em empresas, especialmente de tecnologia ou financeiras.
- Escolha dois casos e discuta em equipe primeiramente quais princípios básicos de segurança foram violados e depois aprimore para o Hexagrama Parkeriano.
- O trabalho pode ser entregue de maneira escrita ou em apresentação para a turma.

Referencias

- CABRAL, Carlos.; CAPRINO, Willian. Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados. 1. Rio de Janeiro: Brasport, 2015. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/160689>
- HINTZBERGEN, Jule. et. al. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.. 1. Rio de Janeiro: Brasport, 2018. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044>
- Notas de aula do professor Dr. Daniel Caetano.