UNIVERSIDADE VILA VELHA
ESPÍRITO SANTO

Fundamentos de TC

Segurança da Informação

Prof. Alessandro Bertolani Oliveira

Fundamentos de TC

Segurança da Informação.

UNIVERSIDADE VILA VELHA
ESPÍRITO SANTO

Ideias Importantes:

- Conceito de Fraude.
- Conceitos de Segurança de Dados.
- Formas de Proteção das informações.
- Nível de sensibilidade da Informação.
- Conceitos de Segurança de Informação.
- Pilares da Segurança da Informação.
- Ativos de Informação.
- Ameaças e soluções de Segurança da Informação.
- Mecanismos de Segurança
- Sistema de Gestão da Segurança da Informação (SGSI).
- Lei Geral de Proteção de Dados Pessoais (LGPD).
- Conclusão

De acordo com Prado (2014, p.59), algumas dessas ameaças podem ser identificadas como **Fraude**:

É qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever.

Outros **tipos de ameaças** referem-se:

- ➔ Crimes Eletrônicos (ou cibernéticos),
- ➔ Ameaças Virtuais,
- ➔ Engenharia Social,
- ➔ Terrorismo Digital,
- ➔ Ciberespionagem, dentre outros

Há um conjunto de **normas e leis** estabelecidas no Brasil que buscam proteger os cidadãos e as empresas em seus ativos, sendo algumas delas:

- **Constituição Federal Brasileira**: Assegura a inviolabilidade do direito à privacidade, ao estabelecer que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação”;
- **Marco Civil da Internet** (Lei 12.965/2014):, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- **Lei Geral de Proteção de Dados Pessoais – LGPD** (Lei 13.709/2018): Tenta proteger, de forma efetiva, os direitos do consumidor e do indivíduo quanto a seus interesses comerciais e de dignidade da pessoa humana.

Conceitos de Segurança de Dados e Formas de Proteção – Pontos Importantes:

De acordo com Lyra (2015, p. 12), há uma escala de cinco níveis de sensibilidade a ser atribuída a cada conjunto de informações:

- **Nível 1 – Informação pública** – Informação que foi obtida sem ônus, de fontes públicas, ou que foi produzida internamente pela empresa, mas que tem interesse público. Essas informações não precisam de controle de acesso e de distribuição.
- **Nível 2 – Informação restrita** - Informação que foi adquirida de terceiros com cláusula de sigilo, mas que outras empresas também podem adquirir, ou que foi produzida pela empresa e que tem interesse restrito a ela. Essas informações, se vazadas, podem comprometer a **imagem da organização, mas não sua operação.**

Conceitos de Segurança de Dados e Formas de Proteção – Pontos Importantes:

De acordo com Lyra (2015, p. 12), há uma escala de cinco níveis de sensibilidade a ser atribuída a cada conjunto de informações:

- **Nível 3 – Informação sigilosa** - Informação que foi obtida, com exclusividade de terceiros, ou que foi produzida pela empresa e que trata de decisões, processos ou produtos críticos para a sua operação.
  - Essas informações, se vazadas ou danificadas, podem gerar decisões erradas e prejudiciais para a operação da empresa ou inviabilizar o lançamento de um novo produto ou serviço.

Conceitos de Segurança de Dados e Formas de Proteção – Pontos Importantes:

De acordo com Lyra (2015, p. 12), há uma escala de cinco níveis de sensibilidade a ser atribuída a cada conjunto de informações:

- **Nível 3 – Informação sigilosa** - Informação que foi obtida, com exclusividade de terceiros, ou que foi produzida pela empresa e que trata de decisões, processos ou produtos críticos para a sua operação.
  - ✔ Essas informações, se vazadas ou danificadas, podem gerar decisões erradas e prejudiciais para a operação da empresa ou inviabilizar o lançamento de um novo produto ou serviço.

Conceitos de Segurança de Dados e Formas de Proteção – Pontos Importantes:

De acordo com Lyra (2015, p. 12), há uma escala de cinco níveis de sensibilidade a ser atribuída a cada conjunto de informações:

- **Nível 4 – informação secreta** –Informação referente a detalhes de produtos e serviços que estão em processo de desenvolvimento ou decisões sobre significativas alterações do **valor patrimonial da empresa**.
  - ✔ Essas informações, se vazadas ou danificadas, podem comprometer o protagonismo no lançamento de um novo produto ou ainda permitir que concorrentes o lancem antes da empresa.

Conceitos de Segurança de Dados e Formas de Proteção – Pontos Importantes:

De acordo com Lyra (2015, p. 12), há uma escala de cinco níveis de sensibilidade a ser atribuída a cada conjunto de informações:

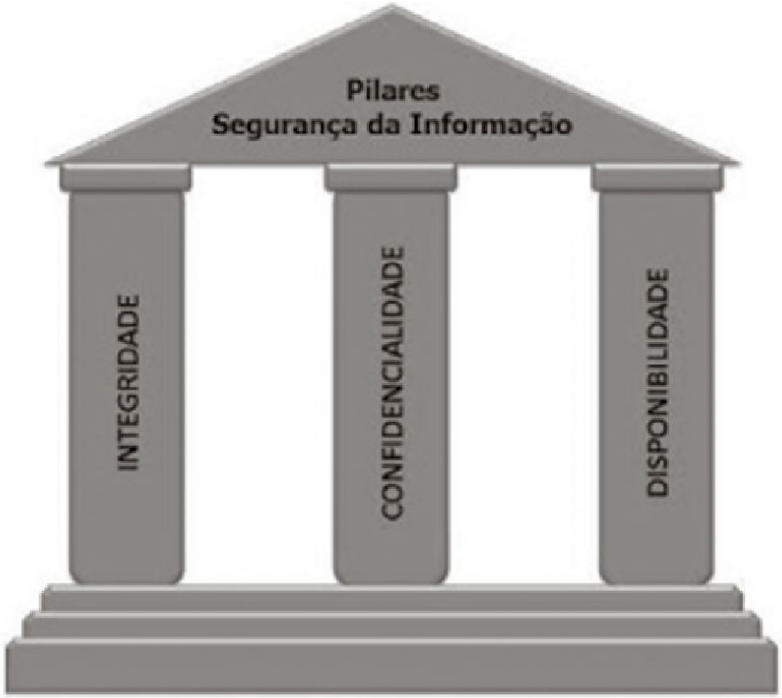
- **Nível 5 – Informações ultrassecretas** – Informações sobre atos e fatos da organização cujo acesso é limitado apenas a mais alta direção executiva e seus acionistas.
  - ✔ Essas informações, se vazadas, podem levar a ações judiciais à empresa ou a seus executivos e acionistas.

Conceitos de Segurança de Dados e Formas de Proteção – Pontos Importantes:

Em Lyra (2015, p. 20), a **Segurança da Informação** é caracterizada pela aplicação adequada de **dispositivos de proteção** sobre um ativo ou um conjunto de ativos visando preservar o valor que este possui para as organizações. A aplicação destas proteções busca preservar a **confidencialidade**, a **integridade** e a **disponibilidade** (CID).

UNIVERSIDADE VILA VELHA ESPÍRITO SANTO

Conceitos de Segurança de Dados e Formas de Proteção – Pontos Importantes:



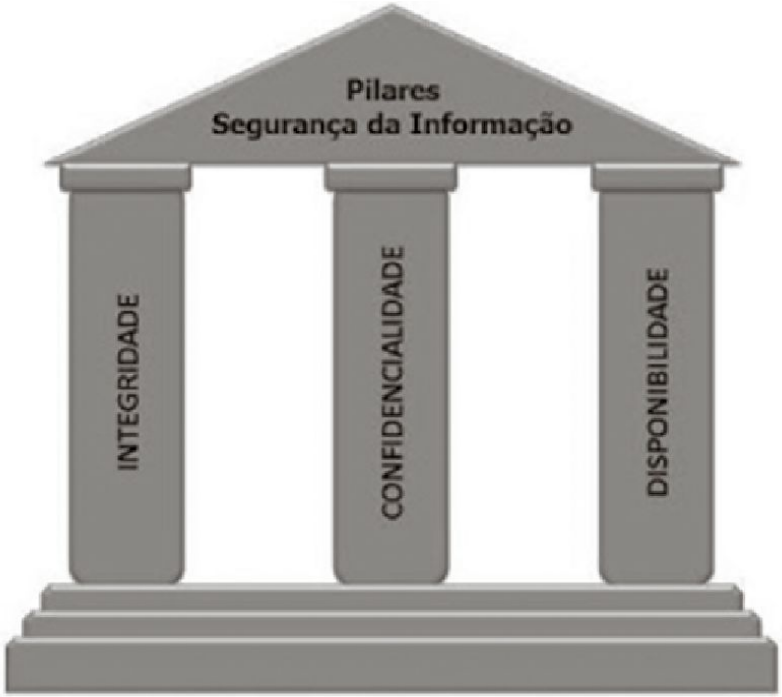
- **Confidencialidade**: é a propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não-autorizados.

- **Integridade:** pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.

- **Disponibilidade** de informações: pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

UNIVERSIDADE VILA VELHA
ESPÍRITO SANTO

Conceitos de Segurança de Dados – **Outros Pontos Importantes**:



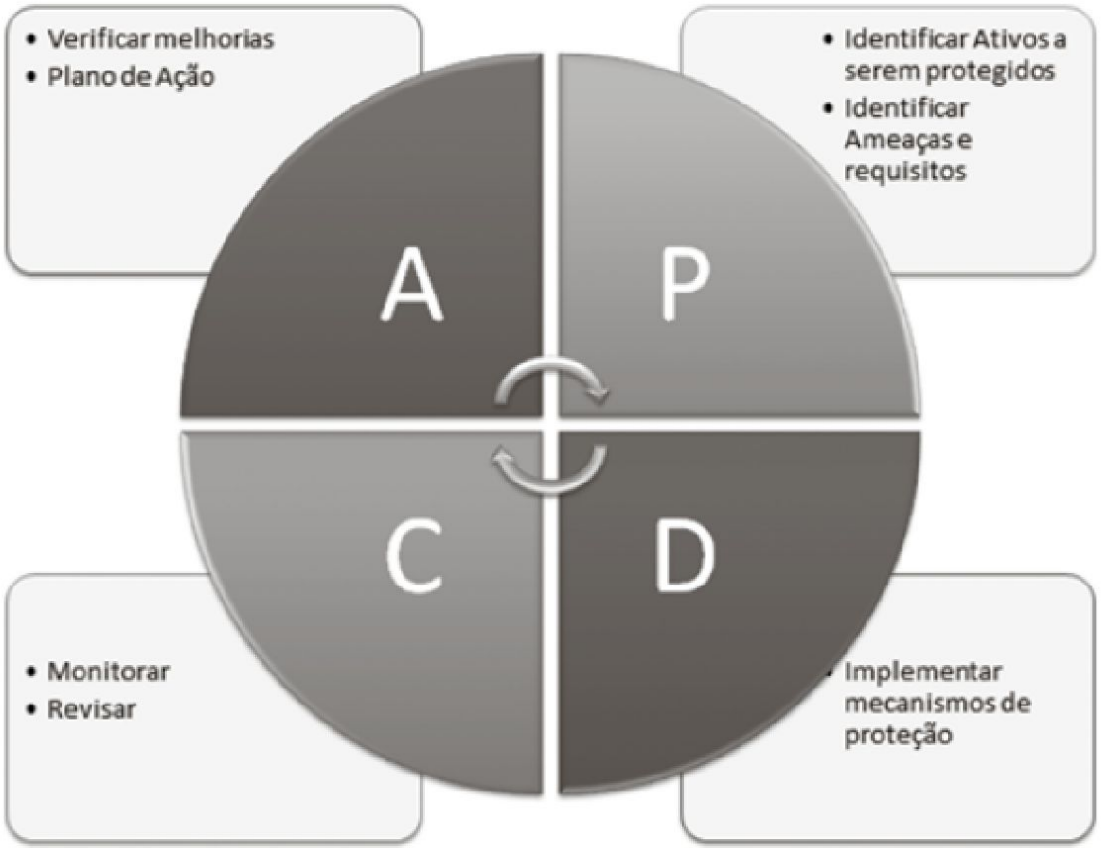
- **Criticidade:** é a classificação da informação de acordo com o **grau de relevância** do ativo de informação.
- **Não-repúdio ou Irretratabilidade**: É a garantia de que uma pessoa não consiga negar a autoria ou envio de uma informação.
- **Proporcionalidade**, em que a organização, em seu poder discricionário (decisão), buscará subsídios na forma da lei, em conceitos, normas e princípios que deverão ser observados em cada caso concreto, dentro do critério de razoabilidade.

Conceitos de Segurança de Dados – Pontos Importantes:

Fatores críticos de sucesso para a garantia da segurança da informação é a correta identificação, controle e constante atualização dos diferentes **tipos de ativos** (inventário).

Tipos de Ativos: Físicos e Lógicos.

Conceitos de Segurança de Dados – Pontos Importantes:



Ciclo de controle PDCA da Segurança da Informação.

Definidos os “Ativos de Informação”, precisamos determinar suas fragilidades, ou **vulnerabilidades**, que, segundo Coutinho (2017), podem ser exploradas por uma ou diversas ameaças que podem ocasionar danos.

As principais ameaças identificadas e catalogadas:

Ataques direcionados:

- ✔ O criminoso, neste caso, estuda a empresa e faz uso de técnicas de engenharia social para induzir os profissionais ao erro, como fazer um depósito em uma conta ou pagar um boleto.
- ✔ diferentemente dos ataques em massa e automatizados, os ataques direcionados utilizam informações específicas de uma organização para executar um ataque.

As principais ameaças identificadas e catalogadas:

Ataques persistentes avançados:

- ✔ As ameaças persistentes avançadas são descritas desta forma, pois, na maioria das vezes, são invasores contratados para atacar uma empresa específica. Essas tentativas de invasão só irão cessar após o objetivo final ser atingido, o que pode, às vezes, demorar meses.
- ✔ também conhecidos como **APT (Advanced Persistent Threats)**, são utilizados para descrever um tipo de ataque direcionado, focado em espionagem via internet.

As principais ameaças identificadas e catalogadas:

Malwares:

- ✔ constituem um software malicioso que têm como objetivo danificar dados ou agir no sistema da vítima sem sua autorização.
- ✔ Ele pode, por exemplo, deletar arquivos ou fazer com que o IP do usuário acesse um determinado site sem que ele saiba — isso é feito em larga escala para derrubar sites de organizações para prejudicá-las..

As principais ameaças identificadas e catalogadas:

Adwares:

- ✔ **Tipo de malware** criado para apresentar **anúncios não solicitados na tela dos usuários** via navegador web, podendo abrir nova abas, alterar a página inicial ou redirecionar para sites não seguros ou impróprios.

Business E-mail Compromise:

- ✔ também conhecido como **fraude do CEO**, o business e-mail compromise é um ataque em que o criminoso **envia uma mensagem** se passando por **um profissional de alto cargo**, como o presidente da empresa.

As principais ameaças identificadas e catalogadas:

Engenharia social:

- ✔ um ataque via engenharia social engana a vítima sem utilização de uma única linha de código ou conhecimento sobre segurança da informação.
- ✔ Os criminosos exploram a psicologia humana, a única fraqueza encontrada em toda e qualquer empresa.
- ✔ Geralmente, o criminoso se passa por alguém confiável e a própria vítima passa seus dados pessoais de livre e espontânea vontade.

As principais ameaças identificadas e catalogadas:

Phishing:

- ✔ É uma prática que visa **roubar dados cadastrais de clientes** por meio de **mensagens iscas, geralmente, por e-mail**.
- ✔ Ao clicar em um **link que supostamente levaria à compra de um produto**, são solicitados os dados do usuário que, posteriormente, são utilizados para outras fraudes.

As principais ameaças identificadas e catalogadas:

Spyware:

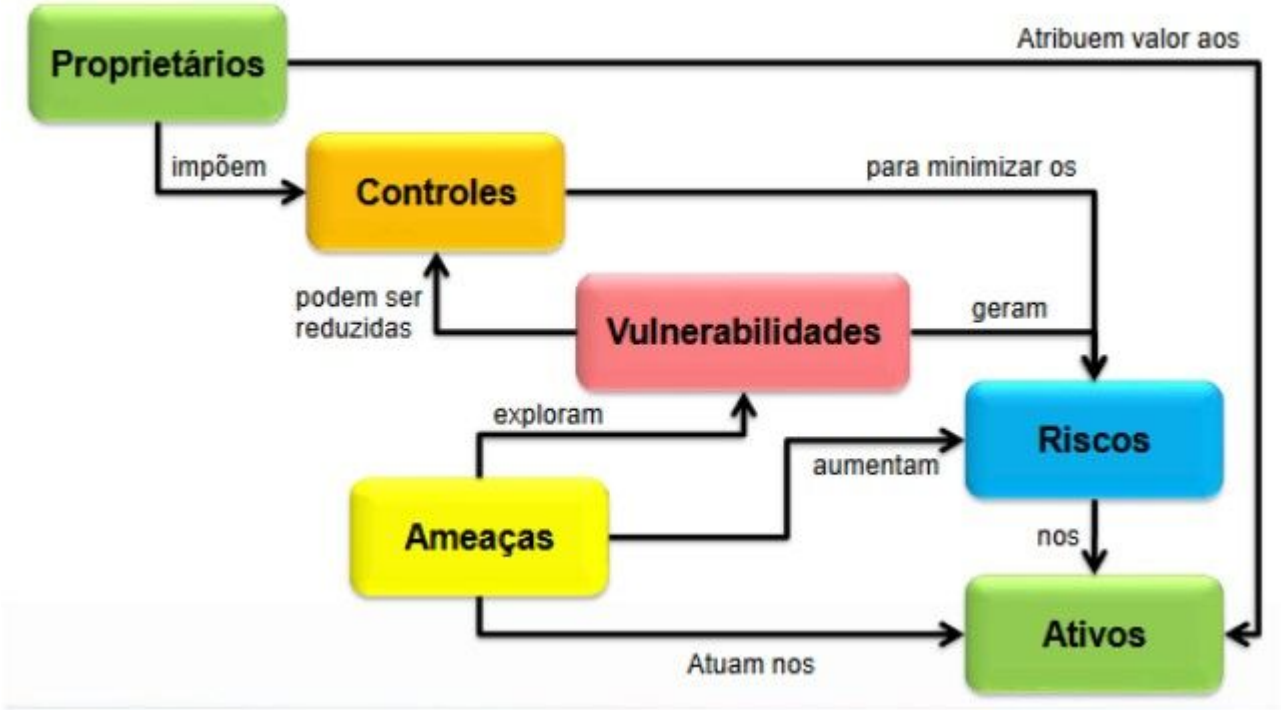
- ✔ ataca computadores ou dispositivos móveis para coletar informações sobre seus usuários.
- ✔ É considerada uma ameaça sorrateira; geralmente, atua abrindo caminho no sistema operacional sem o consentimento da vítima.

As principais ameaças identificadas e catalogadas:

Trojan:

- ✔ também conhecido como Cavalo de Troia, o **trojan é um software** que se passa por um programa legítimo, simulando alguma funcionalidade útil.
- ✔ Esta ameaça **abre uma porta** para que um hacker tenha acesso ao seu computador para **roubar senhas ou qualquer outro tipo de dado sigiloso** que possa ser usado para extorquir a vítima.

As principais ameaças identificadas e catalogadas:



Relação de causa/efeito entre os elementos da Segurança da Informação.

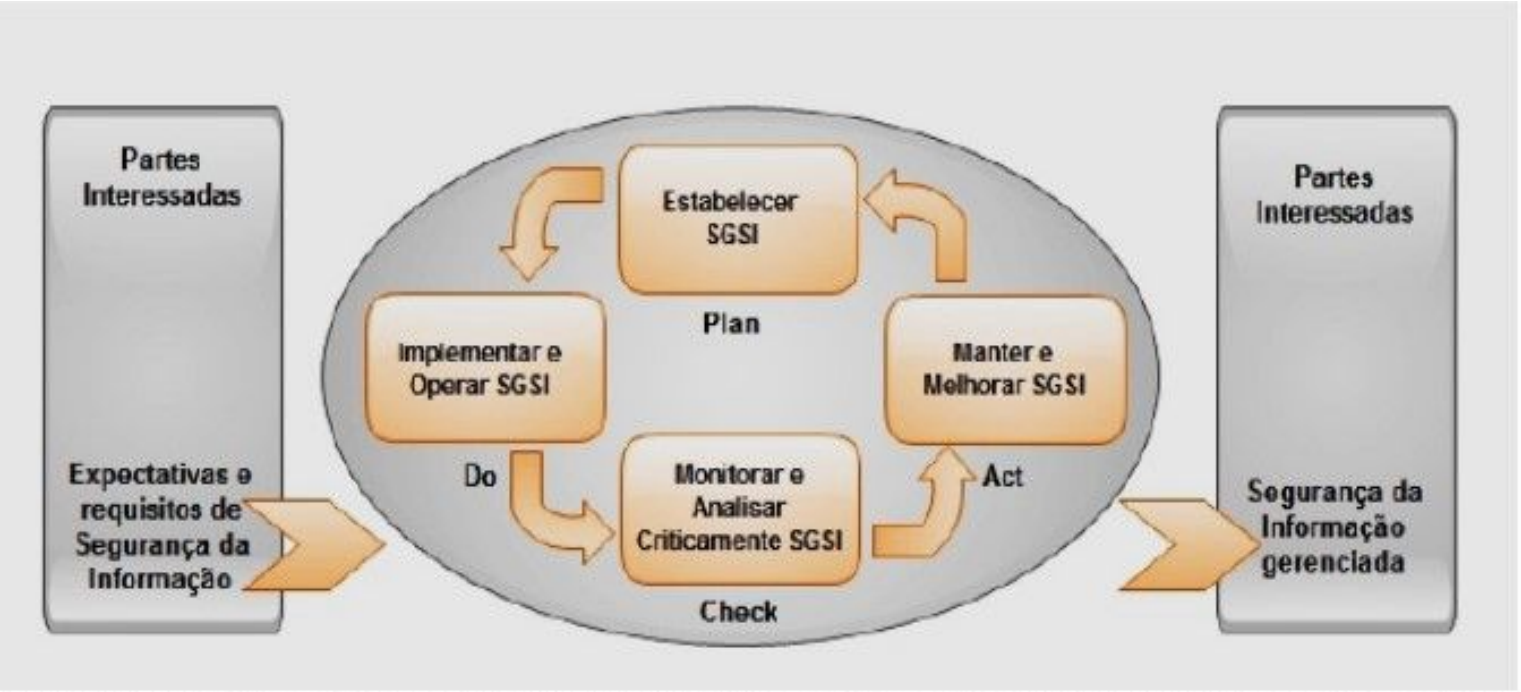
Norma **ISO 27001** é uma norma que define os requisitos para um

Sistema de Gestão da Segurança da Informação (SGSI):

"O SGSI é descrito como um sistema parte do sistema de gestão global da organização, com base em uma abordagem de risco do negócio, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação. O SGSI inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos"

Norma **ISO 27001** é uma norma que define os requisitos para um

Sistema de Gestão da Segurança da Informação (SGSI):



Processos principais da norma ISO 27001.

Lei Geral de Proteção de Dados Pessoais (LGPD) – Pontos importantes:

- ✔ Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado;
- ✔ O objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- ✔ Deve adotar **medidas de segurança da informação** aptas a proteger os dados pessoais de **acessos não autorizados** e de **situações acidentais ou ilícitas**.
- ✔ A LGPD estabelece o **Data Protection Officer** - DPO (Encarregado), que é a pessoa física ou jurídica cuja responsabilidade é atribuída à empresa para exercer as atividades previstas na LGPD.

Mecanismos de Segurança são – Pontos importantes:

Criptografia:

- ✔ um conhecido meio de converter os dados em um formato que seja impossível decifrá-lo.
- ✔ Imagine que para assegurar que os dados, em idioma português, não sejam compreendidos por meros falantes da língua, as informações sejam convertidas para o hebraico.
- ✔ O raciocínio é muito similar a isso, porém, criptografar é impedir completamente a interpretação das informações, e elas só voltam ao estado inteligível quando uma chave (senha) for inserida aos dados.

Mecanismos de Segurança são – Pontos importantes:

Assinatura digital:

✔ com a assinatura digital é garantida a integridade dos dados por meio de criptografia, ou seja, seu acesso pode ser irrestrito e seu conteúdo não pode ser modificado.

Mecanismos de Segurança são – Pontos importantes:

***Honeypot*:**

- ✔ trata-se de um software que age como um **antivírus em tempo real**, cuja função é proteger os dados de invasores, aplicações maliciosas e estranhas ao sistema.
- ✔ A diferença é que, em vez de mantê-lo em quarentena (vírus ou verme), por exemplo, o *honeyspot* ludibria esse invasor, **fazendo-o acreditar que está tendo acesso real às informações**.

Certificação:

- ✔ uma certificação é como um atestado de autenticidade de um arquivo, uma garantia de que o mesmo é válido.

Conclusão:

Esta unidade abordou um tema de alta relevância a todo **profissional de Tecnologia da Informação**, que é a **Segurança da Informação**.

Por fim, vimos que há normas e padrões de reconhecimento mundial que nos permitem adotar essas práticas de proteção de forma sistematizada, especialmente, as normas **ISO 27001 e 27002**.

No Brasil, entendemos como as normas e leis estão sendo criadas e implementadas com **foco em segurança de dados pessoais** quando discutimos a **LGPD**.