A **segurança da informação** está relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

Características básicas:

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Autenticidade.

Políticas de segurança:
Consiste em um conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

ASPECTOS JURÍDICOS - CLT (Consolidação das Leis do Trabalho)

Art. 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador:

a) ato de improbidade;
b) incontinência de conduta ou mau procedimento;
c) negociação habitual por conta própria ou alheia sem permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço;
g) violação de segredo da empresa;

Políticas de Segurança – Elaboração

1. **Planejamento, levantando o perfil da empresa:**
   Analisar o que deve ser protegido, tanto interno como externamente.
2. **Aprovação da política de segurança pela diretoria:**
   Garantir que a diretoria apóie a implantação da política.

Políticas de Segurança – Elaboração

3. **Análise interna e externa dos recursos a serem protegidos:**
   Estudar o que deve ser protegido, verificando o atual programa de segurança da empresa, se houver, enumerando as deficiências e fatores de risco.

Políticas de Segurança – Elaboração

4. **Elaboração das normas e proibições, tanto física, lógica e humana:**
   Nesta etapa devemos criar as normas relativas à utilização de programas, utilização da internet, ***uso de smartphones e tablets,*** acessos físicos e lógicos, bloqueios de sites, utilização do e-mail, utilização dos recursos tecnológicos, etc.

Políticas de Segurança – Elaboração

5. **Aprovação pelo Recursos Humanos:**

   As normas e procedimentos devem ser lidas e aprovadas pelo departamento de Recursos Humanos, no que tange a leis trabalhistas e manual interno dos funcionários da organização.

Políticas de Segurança – Elaboração

6. **Aplicação e Treinamento da Equipe:**
   Elaborar um treinamento prático com recursos didáticos, para apresentar a política de segurança da informação, recolhendo declaração de comprometimento dos funcionários. A política deve ficar sempre disponível para todos os colaboradores da organização.

Políticas de Segurança – Elaboração

7. **Avaliação Periódica :**

   A política de segurança da informação deve ser sempre revista, nunca pode ficar ultrapassada.

Políticas de Segurança – Elaboração

8. **Feedback:**

   A organização deverá designar um colaborador específico para ficar monitorando a política, a fim de buscar informações ou incoerências, que venham a alterar o sistema, tais como vulnerabilidades, mudanças em processos gerenciais ou infra-estrutura.

Políticas de Segurança – Elaboração

9. **Atenção à novas tecnologias:**

   O setor de TI deve estar sempre atendo à novas tecnologias e demandas externas, para poder analisar e atualizar constantemente.

Criptografia

Segurança física: Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, algo que possa danificar a parte física da segurança, acesso indevido de estranhos, forma inadequada de tratamento e manuseio do veículo.

Segurança lógica

Atenta contra ameaças ocasionadas por **vírus,** acessos remotos à rede, *backup* desatualizados, violação de **senhas**, etc. Segurança lógica é a forma como um sistema é protegido no nível de sistema operacional e de aplicação.

Políticas de Senhas

Senha com data para expiração Adota-se um padrão definido onde a senha possui prazo de validade com 30 ou 45 dias, obrigando o colaborador ou usuário a renovar sua senha.

Políticas de Senhas

Inibir a repetição Adota-se através de regras predefinidas que uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos, p. ex: senha anterior “123senha” nova senha deve ter 60% dos caracteres diferentes como “456seuse”, neste caso foram repetidos somente os caracteres “s” “e” os demais diferentes.

Políticas de Senhas

Recomenda-se ainda utilizar senhas com **Case Sensitive** e utilização de caracteres especiais como: @ # $ % & *

Golpes na Internet:

Ataques na Internet:

Códigos maliciosos (*Malware*):

Spam:

Privacidade:

Criptografia

QUESTÃO 14

Em relação à Segurança da Informação, a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes é o princípio da

(A) autenticidade.
(B) integridade.
(C) criptografia.
(D) disponibilidade.
(E) confiabilidade.

Criptografia

QUESTÃO 14

Em relação à Segurança da Informação, a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes é o princípio da

(A) autenticidade.
(B) integridade.
(C) criptografia.
(D) disponibilidade.
(E) confiabilidade.

Certificado digital

Um **certificado digital** é um arquivo de computador que contém um conjunto de informações referentes a entidade para o qual o certificado foi emitido (seja uma empresa, pessoa física ou computador) mais a **chave pública** referente a **chave privada** que se acredita ser de posse unicamente da entidade especificada no certificado.

Certificado digital