

Curso de Ciência da Computação**Disciplina: Segurança e Auditoria da Informação - 8º período****Professor: José Maurício S. Pinheiro****AULA 3: Conceitos de Segurança da Informação**

“Informação é o conjunto de dados utilizados para a transferência de uma mensagem entre pessoas ou máquinas em processos de troca de mensagens (processos comunicativos) ou transacionais (transferência de arquivos)”.

1. Definição

Segurança da Informação é a área do conhecimento dedicada à proteção dos ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Para atender essas expectativas de uma corporação, um sistema de segurança da informação deve atender aos objetivos básicos destacados a seguir:

1. **Confidencialidade ou privacidade** – proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação. Este objetivo envolve medidas como controle de acesso e criptografia;
2. **Integridade dos dados** – evitar que dados sejam apagados ou alterados sem a permissão do gestor da informação;
3. **Disponibilidade** – garantir o funcionamento do serviço de informação e acesso aos usuários autorizados. As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos e sistemas e política de backup;
4. **Consistência** – certificar-se de que o sistema atua de acordo com a expectativa dos usuários;
5. **Isolamento ou uso legítimo** – controlar o acesso ao sistema. Garantir que somente usuários autorizados possuam acesso ao sistema;
6. **Auditoria** – proteger os sistemas contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, são utilizadas trilhas de auditorias e logs, que registram o que foi executado no sistema, por quem e quando;
7. **Confiabilidade** – garantir que, mesmo em condições adversas, o sistema atuará conforme esperado;
8. **Legalidade** – a informação deve estar em conformidade com os preceitos da legislação em vigor.

2. Objetivos

As políticas de segurança da informação devem fornecer meios para garantir que as informações de uso restrito não serão acessadas, copiadas ou

codificadas por pessoas não autorizadas. Uma das maneiras de se evitar o acesso indevido a informações confidenciais é através da codificação ou cifragem da informação, conhecida como criptografia, fazendo com que apenas as pessoas às quais estas informações são destinadas, consigam compreendê-las.

A Figura 1 representa um fluxo de informações e quatro ameaças possíveis para a segurança de um sistema de informação:

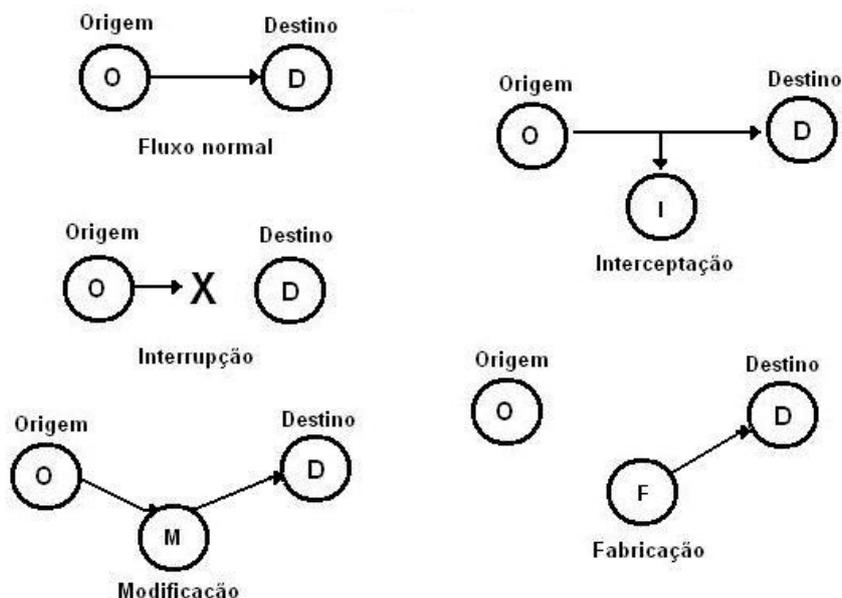


Figura 1 - Exemplos de ataques contra um sistema de informação

- **Interrupção:** Ataque na transmissão da mensagem, onde o fluxo de dados é interrompido, porém pode não ser percebido. Um exemplo pode ser danos de componentes ou clonagem / queda do sistema de comunicação;
- **Interceptação:** Este é um ataque sobre a confidencialidade. Ocorre quando uma pessoa não autorizada tem acesso às informações confidenciais de outra. Um exemplo seria a captura de dados na rede, ou a cópia ilegal de um arquivo;
- **Modificação:** Este é um ataque à integridade da mensagem. Ocorre quando uma pessoa não autorizada, além de interceptar as mensagens, altera o conteúdo da mensagem e envia o conteúdo alterado para o destinatário;
- **Fabricação:** Este é um ataque sobre a autenticidade. Uma pessoa não autorizada insere mensagens no sistema assumindo o perfil de um usuário autorizado.

3. Classificação das informações

A classificação das informações é o processo de identificar e definir níveis e critérios de proteção adequada para as informações, objetivando garantir a

segurança das mesmas. Uma organização precisa ser capaz de identificar os valores de suas informações para garantir sua confidencialidade, integridade e disponibilidades.

O objetivo principal dessa classificação está em priorizar recursos, focando os investimentos nas informações mais importantes para a organização. São exemplos de informações:

- **Dados:** base de dados e arquivos, documentação de sistema, informações armazenadas, procedimentos de suporte ou operação;
- **Software:** aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- **Ativos físicos:** equipamentos computacionais (processadores, monitores), equipamentos de comunicação (roteadores, hubs), mídia magnética (fitas, discos), mesas, cadeiras;
- **Serviços:** serviço de operadoras de telecomunicação, serviço de energia elétrica, água, etc.;

4. Desclassificação e reclassificação das informações

Uma informação pode ter seu nível de classificação alterado ou rebaixado, dependendo do nível de confidencialidade, integridade e disponibilidade que a informação tiver no momento. Por exemplo, a informação sobre um novo produto de uma empresa que ainda será lançado comercialmente. Esta informação no momento anterior ao lançamento é considerada confidencial, mas no momento em que este produto é divulgado publicamente, esta informação passa a ser pública.

5. Critérios de classificação das informações

Os critérios de classificação definem qual o tratamento de segurança que uma informação receberá, ou seja, quanto será preciso investir em segurança para garantir a confidencialidade, integridade e disponibilidade dessa informação, objetivando sempre priorizar recursos. Para tanto, podemos classificar as informações quanto a:

- **Confidencialidade** – Classificar a informação levando em consideração a gravidade do impacto ou prejuízo que a revelação não autorizada da mesma trará para a organização. Podem-se definir três níveis de classificação quanto a confidencialidade:
 - **Confidencial** - é toda informação considerada de alto risco para a empresa, pois sua revelação não autorizada pode trazer graves prejuízos. Geralmente estas informações são acessadas pela alta administração (presidência, diretoria, superintendência);
 - **Restrita** – é toda informação considerada de médio e baixo risco para a empresa, pois sua revelação não autorizada pode trazer prejuízos a uma determinada área da empresa. Geralmente estas informações são acessadas pelas áreas envolvidas na geração e

uso destas informações, pelos gestores da área e pela alta administração;

- Pública – é toda informação considerada de nenhum risco para a empresa e sua revelação não autorizada não traz nenhum prejuízo. Estas informações são acessadas por todos os funcionários e pessoas externas à empresa.
- **Integridade** - Classificar a informação levando em consideração a gravidade do impacto ou dos prejuízos que a modificação não autorizada da informação trará. Podem-se definir dois níveis de classificação quanto à integridade:
 - Crítica – é toda informação de alto risco para a empresa. Esta informação não pode ser alterada sem prévia autorização;
 - Não Crítica – é toda informação que, se alterada sem prévia autorização, não representa nenhum risco para a empresa.
- **Disponibilidade** - Classificar as informações levando em consideração a gravidade do impacto ou dos prejuízos que a indisponibilidade da informação trará. Podem-se definir dois níveis de classificação quanto à disponibilidade:
 - Vital - é toda informação de alto risco para a empresa. Esta informação precisa estar sempre disponível;
 - Não Vital - é toda informação que em caso de indisponibilidade não representa nenhum risco para a empresa.
- **Classificação Padrão** - Todas as informações que não forem classificadas deverão entrar no nível padrão de classificação.

6. Funções e Responsabilidades

Em um processo de classificação das informações devemos definir as funções e os responsáveis por cada etapa desta classificação, ou seja, devemos definir quem classifica, armazena, atualiza, etc.

- **Proprietários** - são considerados proprietários da informação os gestores das áreas geradoras das informações, sendo os proprietários responsáveis por classificar, desclassificar, redefinir os níveis de classificação das informações;
- **Custodiante** - é considerada custodiante das informações a área de informática, sendo responsável por guardar e recuperar as informações classificadas e responsáveis por prover e administrar os acessos às informações devidamente solicitados pelos proprietários.

7. Controles para as informações

Devemos definir controles para as informações classificadas como confidenciais, críticas e vitais, estes controles são definidos quanto ao armazenamento, envio e descarte.

7.1. Armazenamento

- **Armazenamento de informações eletrônicas** – As informações eletrônicas classificadas como confidenciais e/ou críticas e/ou vitais deverão ser armazenadas em locais específicos para tal finalidade, onde o mesmo será protegido com controle de acesso e procedimento de backup;
- **Armazenamento de informações impressas** – As informações impressas classificadas como confidenciais e/ou críticas e/ou vitais deverão ser armazenadas em locais protegidos do acesso por pessoas não autorizadas pelo proprietário da informação.

7.2. Envio

- **Envio de informações eletrônicas** – O envio por correio eletrônico de informações eletrônicas classificadas como confidenciais e/ou críticas e/ou vitais deverá ser feito utilizando software de criptografia e assinatura digital, para garantir a confidencialidade, integridade e autenticidade das informações trafegadas;
- **Envio de informações impressas** – O envio de informações impressas classificadas como confidenciais e/ou críticas e/ou vitais deverá ser feito através de envelopes lacrados, contendo o nome do destinatário e um carimbo de “CONFIDENCIAL”.

7.3. Descarte

- **Descarte de informações eletrônicas** – O descarte de mídias com informações eletrônicas classificadas como confidenciais e/ou críticas e/ou vitais deverá ser feito pela área de informática. As mídias eletrônicas contendo informações a serem descartadas deverão ser encaminhadas à área de informática pelo proprietário da informação;
- **Descarte de informações impressas** – O descarte de informações impressas classificadas como confidenciais e/ou críticas e/ou vitais deverá ser feito através de trituradores de papéis.

8. Etapas para o processo de classificação das informações

As etapas que devem ser cumpridas para a correta classificação das informações são as seguintes:

- Elaboração de uma política de classificação;
- Levantamento das informações;
- Classificação das informações levantadas;
- Implementação da política;
- Revisão periódica da classificação

9. A política da segurança da informação

A política da segurança da informação é um mecanismo preventivo de proteção dos dados e processos de uma organização e que define também um padrão de segurança que deve ser seguido pelo pessoal técnico, gerência e pelos demais usuários (internos e externos) do sistema de informação. Pode ser usada ainda para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais. Uma de suas preocupações é estabelecer os métodos de proteção, controle e monitoramento dos recursos de informação. É importante que a política de segurança defina as responsabilidades das funções relacionadas à segurança e discrimine as principais ameaças, riscos e impactos envolvidos.

Uma interessante ferramenta para implantação de políticas de informação é o Ciclo PDCA, uma ferramenta gerencial que possibilita a melhoria contínua de processos e a solução de problemas.

Conforme sugere a Norma ABNT NBR 27001, uma organização deve identificar e gerenciar os processos envolvidos em sistemas de gestão e segurança da informação, bem como reconhecer suas interações. A Norma adota o PDCA (Plan, Do, Check, Act) para estruturar todos os processos envolvidos.



Figura 2 - Ciclo PDCA

A política de segurança da informação deve integrar-se às metas de negócio da organização e ao plano das políticas de informatização, influenciando todos os projetos de informatização da empresa tais como o desenvolvimento de novos sistemas, planos de contingências, planejamento de capacidade, dentre outros. É importante lembrar que a política não envolve apenas a área de tecnologia da informação, mas a organização como um todo.

Como toda política institucional, deve ser aprovada pela alta gerência e divulgada a todos os funcionários e usuários de serviços de informática. A partir de então, todos os controles devem ser baseados nessa política de segurança.

10. Gerenciamento de Recursos de Informação

A segurança de uma rede de computadores é parte integrante do Gerenciamento de Recursos de Informação de uma empresa e deve preocupar-se com a aplicação das proteções (técnicas e administrativas) para minimizar as vulnerabilidades e anular falhas potenciais como:

- **Vulnerabilidades:** pontos suscetíveis a ataques, causados por uma brecha do software ou hardware, má configuração e administração ou ambos. Podemos citar como exemplo a análise do ambiente de uma sala de servidores de conectividade e Internet com a seguinte descrição: A Sala dos Servidores não possui controle de acesso físico;
- **Ameaças:** problemas que podem atacar as vulnerabilidades. Normalmente são agrupadas em três categorias: pessoais (omissão ou intenção criminal), de componentes (falha de um equipamento) e de eventos (fogo, inundação). Seguindo o exemplo da Sala dos Servidores, podemos identificar a ameaça da seguinte forma: Fraudes, Sabotagens, Roubo de Informações, Paralisação dos Serviços.

11. Objetivos do Gerenciamento

A segurança de redes de computadores, dentro do conceito de Gerenciamento de Recursos, visa atender aos seguintes objetivos gerais:

- **Confidencialidade ou sigilo:** proteger contra a revelação acidental ou deliberada de informações críticas. É a garantia de que somente as pessoas ou organizações envolvidas na comunicação possam ler e utilizar as informações transmitidas de forma eletrônica pela rede;
- **Integridade:** proteger contra corrupção deliberada ou acidental de informações garantindo que o conteúdo de uma mensagem ou resultado de uma consulta não será alterado durante seu tráfego;
- **Disponibilidade:** proteger contra ações que causem a indisponibilidade de informações críticas aos usuários quando necessitarem;
- **Autenticação:** garantia de identificação das pessoas ou organizações envolvidas na comunicação;
- **Não-Repúdio (Não recusa):** garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá negar sua autoria posteriormente.

12. Questionário

1. Defina “informação”.
2. Quais são as categorias das ameaças para redes de computadores?
3. Um sistema de segurança da informação visa atender alguns objetivos gerais. Comente sobre um deles.
4. O que significa classificar informações?
5. Dentro dos critérios de classificação das informações, como podemos definir os níveis de confidencialidade?
6. O que é uma informação vital?
7. Enumere as possíveis ameaças para a segurança de um sistema de informação.
8. O que é a política de segurança da informação? Onde pode ser usada?
9. Quais as principais ameaças que devem ser tratadas pela política de segurança da informação?
10. Na classificação das informações devemos definir as funções e os responsáveis por cada etapa desta classificação. Quem é considerada custodiante?