

Segurança em Servidores WEB

- Introdução
- Princípios de Segurança
- Objetivos
- Fluxo de informações
- Classificação das informações
- Critérios de classificação
- Funções e responsabilidades
- Ameaças
- Como evitar as ameaças?

Introdução

- Uma grande preocupação da evolução da arquitetura de servidores web é como lidar com segurança e armazenamento de informações nesse ambiente.
- A facilidade da comunicação tornou as empresas mais vulneráveis, o ambiente passou a ser mais heterogêneo e mais distribuído, difícil de ser controlado.

Introdução

- Os ataques e invasões acontecem a todos instantes, acarretando:
 - perda de tempo,
 - queda de produtividade,
 - perda significativa de dinheiro,
 - horas de trabalho,
 - devastação da credibilidade ou oportunidades,
 - empresa não habilitada em competir...

Princípios da Segurança

A segurança da informação é o bem mais valioso de uma organização, ela busca reduzir no máximo possível:

- os riscos de vazamento de informações;
- fraudes em arquivos;
- bancos de dados;
- erros humanos e operacionais;
- roubo de informações;

ou qualquer outra ameaça que possa prejudicá-la.

Princípios da Segurança

CONFIDENCIALIDADE ou PRIVACIDADE

- Significa proteger informações contra sua revelação para alguém não autorizado, leitura e/ou cópia não autorizada;
- A informação deve ser protegida independente da mídia que a contenha;
- Deve-se cuidar não apenas da proteção da informação como um todo, mas também das partes da informação que podem ser utilizadas para interferir em um todo.

Princípios da Segurança

INTEGRIDADE DOS DADOS

- Evitar que dados sejam apagados ou alterados sem a permissão do responsável pela administração do servidor.

DISPONIBILIDADE

- Garantir o funcionamento do serviço de informação aos usuários autorizados.
- As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos ou serviços (RAID), e sistemas e políticas de backup.

Princípios da Segurança

CONSISTÊNCIA

- Certificar-se de que o sistema atua de acordo com a expectativa do usuário.

ISOLAMENTO OU USO LEGÍTIMO

- Controlar o acesso ao sistema.
- Garantir que somente usuários autorizados possuam acesso ao sistema.

Princípios da Segurança

AUDITORIA

- Proteger os sistemas contra erros e atos cometidos por usuários não 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.

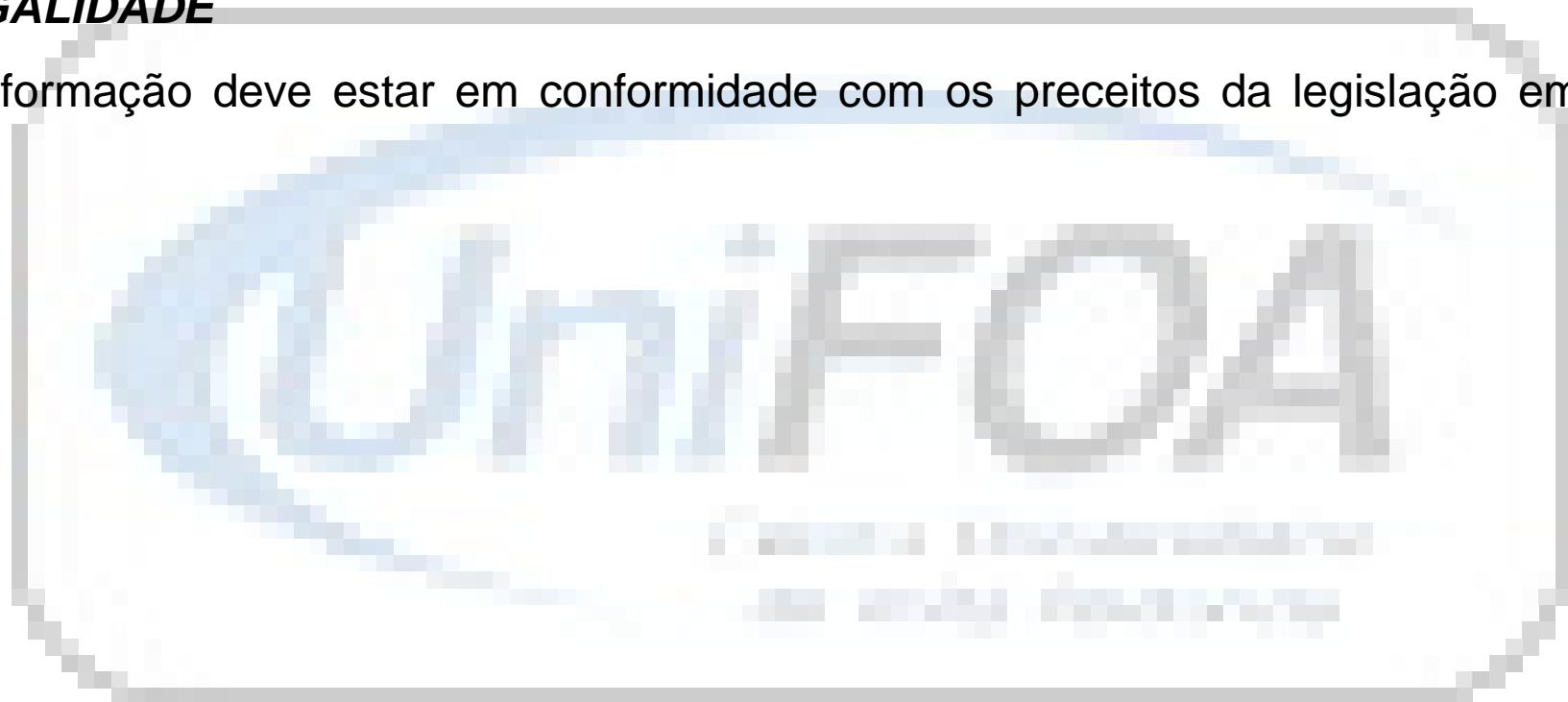
CONFIABILIDADE

- Garantir que, mesmo em condições adversas, o sistema atuará conforme esperado.

Princípios da Segurança

LEGALIDADE

- A informação deve estar em conformidade com os preceitos da legislação em vigor.

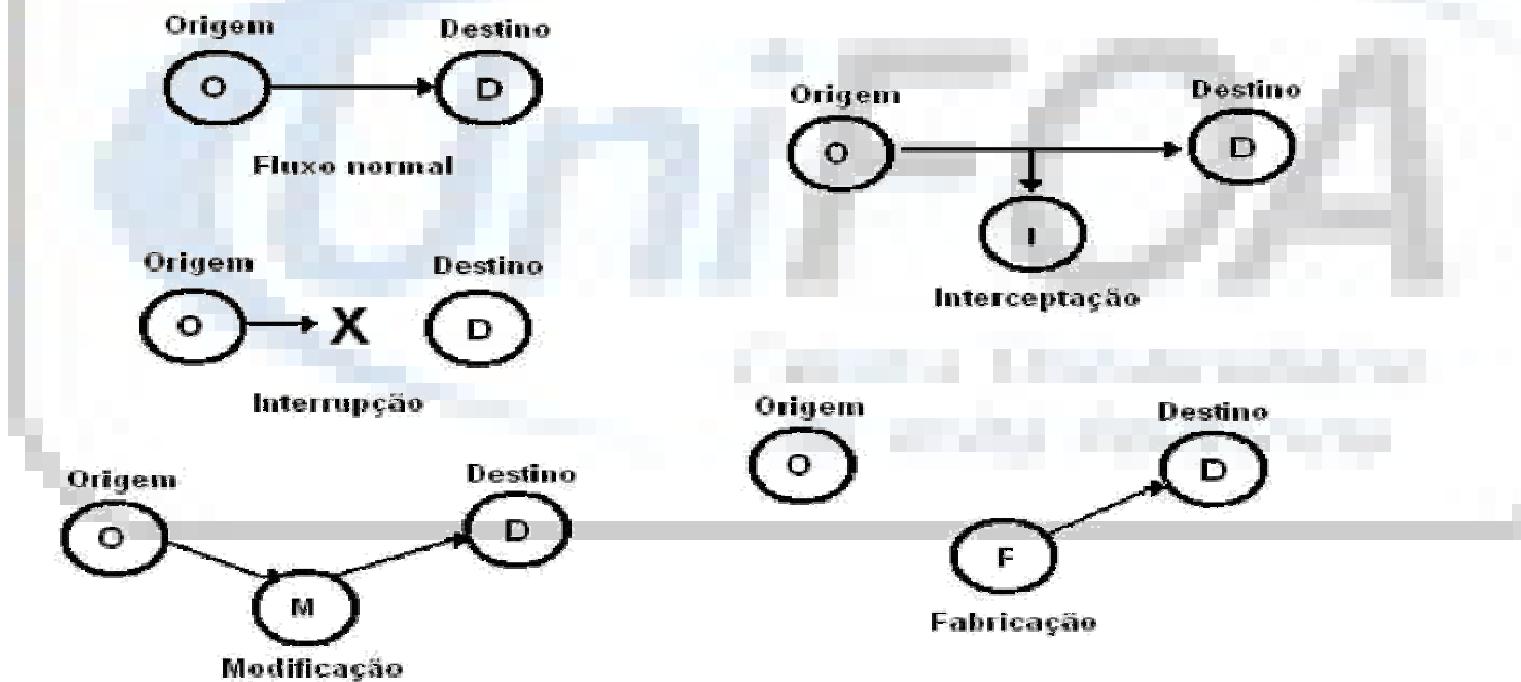


Objetivos

- As políticas de segurança, em relação a arquitetura de servidores Web, 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 é através da codificação ou cifragem da informação, conhecida com **Criptografia**, fazendo com que apenas as pessoas às quais estas informações são destinadas, consigam compreendê-las.

Fluxo de Informações

- Abaixo está representado um fluxo de informações e quatro ameaças possíveis para a segurança de um sistema de informação em servidores Web.

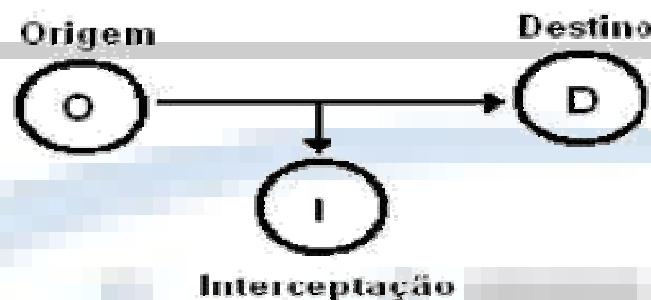


Interrupção



- Ataque na transmissão da mensagem, onde o fluxo de dados é interrompido.
- Um exemplo pode ser a danificação de componentes de hardware ou a queda do sistema de comunicação por sabotagem.

Interceptação



- 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



- 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 ao destinatário.

Fabricação



- É um ataque sobre a autenticidade.
- Uma pessoa não autorizada insere mensagens no sistema assumindo o perfil de um usuário autorizado.

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.
- O objetivo desta classificação está em priorizar recursos, focando os investimentos nas informações mais importantes para a organização.

Classificação das Informações

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 telecomunicações, serviço de energia elétrica, água, etc.

Critérios de Classificação

- Uma informação pode ter seu nível de classificação alterado ou rebaixado, dependendo dos níveis de critério que a informação tiver no momento.
- Definem qual o tratamento de segurança que uma informação receberá, ou seja, quanto será preciso investir para garantir a confidencialidade, integridade e disponibilidade dessa informação, objetivando sempre priorizar recursos.

Confidencialidade

- Classificar a informação levando em consideração a gravidade do impacto ou prejuízo que a revelação não autorizada da mesma trará para a organização.
 - Confidencial – toda informação considerada de alto risco para a empresa, pois sua revelação não autorizada pode trazer graves prejuízos.
 - Restrita – 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.
 - Pública – toda informação considerada de nenhum risco para a empresa e sua revelação não autorizada não traz nenhum prejuízo.

Integridade

- Classificar a informação levando em consideração a gravidade do impacto ou dos prejuízos que a modificação não autorizada da informação trará.
 - Crítica – toda informação de alto risco para a empresa. Não pode ser alterada sem prévia autorização.
 - Não-Crítica – 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.
 - Vital – toda informação de alto risco para a empresa. Esta informação precisa estar sempre disponível.
 - Não-Vital – 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.

Funções e Responsabilidades

- Proprietários da Informação – gestores das áreas geradoras das informações, sendo os proprietários, responsáveis por classificar, desclassificar, redefinir os níveis de classificação das informações, dentro da arquitetura dos servidores Web específicos.
- Custodiantes – são os responsáveis por guardar e recuperar as informações classificadas e por prover e administrar os acessos às informações devidamente solicitadas pelos proprietários.

Ameaças

- Ameaças à Integridade – ameaças ambientais (fogo, água, terremoto, etc), erros humanos, fraudes, falhas no processamento.
- Ameaças de Indisponibilidade – falhas em sistemas ou nos diversos ambientes computacionais.
- Ameaças de divulgação da informação – divulgação de informações premeditada ou acidental.
- Ameaças por alterações não autorizadas – alteração premeditada ou acidental do conteúdo das informações do sistema.

Prevenção

- Proteção de Hardware – chamado de segurança física, impede acessos físicos não autorizados à infra-estrutura da rede, prevenindo roubos de dados, desligamento de equipamentos e demais danos possíveis quando se está fisicamente no local.
- Proteção de arquivos e dados – providenciado por autenticação (onde é verificada a identidade do usuário), controle de acesso (só são disponibilizadas as transações pertinentes ao usuário) e antivírus (garante a proteção do sistema contra programas maliciosos).
- Proteção de perímetro – ferramentas de firewall cuidam deste aspecto, mantendo a rede protegida contra invasões de usuários não autorizados.

Detecção

- Alertas – sistemas de detecção de intrusos (IDS) alertam os administradores e responsáveis pela segurança da rede sobre qualquer sinal de invasão ou mudança suspeita no comportamento da rede que possa significar um padrão de ataque. Os avisos podem ser via mail, mensagem no terminal do administrador do servidor, etc.
- Auditoria – periodicamente deve-se analisar os componentes críticos do sistema a procura de mudanças suspeitas. Pode ser realizado por ferramentas que procuram, por exemplo, modificações no tamanho dos arquivos de senhas, usuários nativos, etc.

Recuperação

- Cópia de Segurança de Dados (Backup) – manter sempre atualizados e testados os arquivos de segurança de dados em mídia confiável e separado dos servidores.
- Aplicações de Backup – ferramentas que proporcionam a recuperação rápida e confiável dos dados mais atualizados em caso de perda dos dados originais do sistema.
- Backup de Hardware – servidor reserva, no-break reserva, linha de dados/comunicação reserva. Podem ser justificados levando-se em conta o custo de uma parada de sistema e determinando-se a importância da informática para a organização.

Exercícios

1. Os ataques e invasões acontecem a todos instantes em um sistema com arquitetura vulnerável. O que estes ataques poderão acarretar?

2. A segurança da informação é o bem mais valioso de uma organização. Quais são os riscos que ela busca reduzir?

3. Identifique as características dos seguintes princípios de segurança:
 1. Confidencialidade
 2. Integridade
 3. Disponibilidade
 4. Consistência
 5. Isolamento
 6. Auditoria
 7. Confiabilidade
 8. Legalidade

4. Quais os objetivos das políticas de segurança de servidores? Quais são as maneiras de se evitar o acesso indevido?

5. Identifique e represente graficamente, em um fluxo de informações, as quatro ameaças possíveis para a segurança de um sistema de informação em servidores Web.

Exercícios

6. Qual o objetivo da classificação das informações em servidores? Exemplifique.
7. Uma informação pode ter seu nível de classificação alterado ou rebaixado, dependendo dos níveis de critério que a informação tiver no momento. Sabendo disso, descreva os critérios de classificação.
8. Identifique os dois responsáveis na administração dos servidores Web e defina suas funções.
9. Cite as ameaças que podem incidir em sistemas que utilizam uma arquitetura de servidores específica.
10. Definas as seguintes características:
 1. Prevenção
 2. Detecção
 3. Recuperação