João Bosco **Beraldo** - 014 9726-4389

jberaldo@bcinfo.com.br

José F. F. de **Camargo** - 14 8112-1001

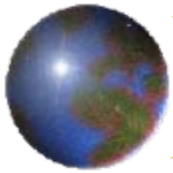
jffcamargo@bcinfo.com.br

BCInfo – Consultoria e Informática

14 **3882-8276**

WWW.BCINFO.COM.BR

Segurança da Informação



Segurança da Informação

Princípios básicos de segurança

Arquitetura de segurança

Mecanismos de segurança

Uma visão geral do contexto

O Sistema Brasileiro de Pagamentos

Princípios Básicos da Segurança da Informação

INTEGRIDADE

CONFIDENCIALIDADE

DISPONIBILIDADE

Princípios Básicos da Segurança da Informação

INTEGRIDADE

Princípio da proteção da informação ou dos bens contra a criação ou modificação não autorizada

- Perda de Integridade pode estar relacionada com erro humano, ações intencionais ou contingências.
- A perda da integridade de uma informação pode torná-la sem valor, ou mesmo perigosa.
- As conseqüências de se utilizar dados incorretos pode ser desastrosa

Princípios Básicos da Segurança da Informação

CONFIDENCIALIDADE

Princípio que trata sobre a disponibilidade de informações apenas a pessoas autorizadas

- Controles devem ser implementados para garantir que o acesso à informação seja sempre restrito àquelas pessoas que necessitam efetivamente tê-lo.
- Muitos crimes cibernéticos acontecem através da quebra de sigilo e do roubo da informação.

OBS: Temos que considerar o “ser confidencial” e o “manter-se confidencial”.

- Para ser confidencial deve ter uma classificação que determine as medidas de segurança necessárias quando estiver sendo tratada.
- Manter-se confidencial significa que o meio utilizado para tratar a informação permite proteção adequada

Princípios Básicos da Segurança da Informação

DISPONIBILIDADE

Princípio que trata sobre prevenir que a informação ou o recurso esteja disponível quando requerido

- Aplica-se não só à informação em si mas também aos canais eletrônicos, equipamentos de rede e outros elementos da estrutura tecnológica.
- Não conseguir acesso a um recurso desejado é chamado de “denial of service”, técnica utilizada por “hacker’s”.
- Os ataques intencionais contra a infra-estrutura tecnológica podem ter a finalidade de tornar os dados indisponíveis assim como de roubar informações.
- Quando o problema acontece com o público interno pode-se não ter perda significativa de imagem mas, se for com público externo haverá um reflexo negativo para a imagem da instituição.

Arquitetura de segurança

Conjunto de normas, procedimentos, ações, recursos e soluções para atender às preocupações de segurança

Deve-se considerar os aspectos técnicos, humanos e organizacionais.

Para se obter um alcance amplo e corporativo deve-se aplicar uma metodologia que considere o ciclo de vida da segurança e os objetivos do negócio.

Arquitetura de segurança

Ciclo de Vida

O ciclo de vida tem 4 fases:

Avaliar
Projetar
Implementar
Acompanhar

Arquitetura de segurança

Ciclo de Vida – Avaliar

Na fase avaliar, o objetivo é identificar riscos e vulnerabilidades considerando os objetivos do negócio e as características dos recursos tecnológicos.

O produto será uma mapeamento para a identificação dos riscos tecnológicos e dos negócios.

Arquitetura de segurança

Ciclo de Vida – Avaliar

Pode-se utilizar diversas técnicas na identificação de riscos ou no diagnóstico de vulnerabilidades tais como:

- Teste de penetração e intrusão
- Análise de vulnerabilidades
- Diagnósticos de segurança
- Revisão de riscos operacionais
- Revisão de continuidade do negócio

Arquitetura de segurança

Ciclo de Vida – Projetar

Nesta fase o objetivo é definir e elaborar padrões, ações e soluções de segurança que minimizem os riscos e aprimorem o nível de segurança e controle tomando como base o mapeamento de riscos identificados na fase anterior.

Arquitetura de segurança
Ciclo de Vida – Projetar

Resultados da fase Projetar:
Projetos relacionados com:

- Desenvolvimento da estratégia de segurança
- Adoção de metodologia de gerenciamento de riscos
- Arquitetura de segurança
- Planos e Políticas de segurança da informação
- Metodologia da Classificação de dados
- Estabelecer normas, procedimentos e padrões de segurança
- Programas de treinamento
- Estabelecimento de níveis de acordo de serviços

Arquitetura de segurança

Ciclo de Vida – Implementar

Tem como objetivo tornar efetivo o que foi projetado.

A atenção maior recai sobre os projetos de mudança nos negócios ou na plataforma tecnológica.

Deve-se considerar fortemente a adoção de tarefas dedicadas ao gerenciamento do projeto.

Muitos projetos falham e não atingem os seus objetivos por falhas no cumprimento de cronogramas e de orçamentos sem observar os caminhos críticos das atividades.

Arquitetura de segurança

Ciclo de Vida – Acompanhar

Esta fase tem como objetivo manter a segurança da informação em funcionamento.

Administrar a segurança dos recursos tecnológicos.

Proporcionar feedback e capacitação.

Avaliar a capacitação das áreas envolvidas preenchendo as lacunas ou falhas identificadas.

Mecanismos de Segurança

Considerando-se:

- Os princípios básicos e o plano de segurança implementado
- O crescimento dos negócios e da infra-estrutura tecnológica;
- Crescimento dos canais externos e internos;
- Disponibilidade de tecnologias a custos viáveis

Cabe então a contínua manutenção da segurança.

Mecanismos de Segurança

Principais dispositivos e técnicas de uma arquitetura de segurança:

- Controle de acesso
- Criptografia
- Firewall
- Virtual Private Network
- Assinatura Digital
- Certificados Digitais e Public Key Infraestructure – PKI
- Secure Eletronic Transaction – SET
- Monitoramento

- **Continuidade Operacional**
- **Plano de continuidade do negócio**

Mecanismos de Segurança

Controle de acesso

Assegura a confidencialidade, integridade, disponibilidade e uso legítimo das informações e recursos.

Autorização

Processo para conceder ou negar direitos a usuários ou sistemas por meio das ACL's (Listas de Controle de Acesso) definindo quais atividades podem ser realizadas.

Devem ser constantemente gerenciadas concedendo ou revogando as permissões de acesso e estabelecer controles rígidos para garantir a revisão freqüente dos perfis de acesso.

Mecanismos de Segurança

Controle de acesso

Autenticação

É o meio para obter a certeza de que o usuário é realmente quem está afirmando ser.

É um serviço essencial de segurança pois um serviço confiável assegura o controle de acesso, quem está autorizado a acessar a informação, permite trilhas de auditoria e assegura legitimidade do acesso.

Mecanismos de Segurança

Controle de acesso

Autenticação

Identificação Positiva

Depende de uma senha ou de um PIN

Identificação Proprietária

O usuário utiliza algo como um cartão magnético, um token ou um smart card.

Identificação Biométrica

Envolve processos automatizados de reconhecimento de características físicas intrínsecas a cada indivíduo.

Mecanismos de Segurança

Criptografia

Ciência que se dedica a transcrever dados em cifras ou códigos.

- As técnicas de criptografia empregam formas de codificação reversíveis e irreversíveis.
- As reversíveis dependem de uma chave e de um algoritmo hash. Esta chave são strings que permitem ao software encriptar/decriptar dados
- Os métodos irreversíveis são conseguidos a partir de funções hash. O processo não requer chaves. É pouco provável que alguém que não tenha o algoritmo, possa decriptar a informação

Mecanismos de Segurança

Criptografia

- **Criptografia Simétrica**

  Utiliza-se de uma chave única para encriptar/decriptar
- **Criptografia Assimétrica**

  Usa uma chave publica para encriptar e uma chave privada para decriptar.
- **Algoritmos Hash**

  Função matemática que transforma uma string em um valor. O destinatário autentica aplicando o mesmo algoritmo
- **Criptografia Híbrida**

  Combinação das técnicas acima

Mecanismos de Segurança

Firewall

Dispositivo de defesa que reforça o cumprimento das políticas de controle de acesso entre redes permitindo somente tráfego de informação autorizada.

Todo o tráfego de informação é examinado em tempo real obedecendo a regra:

“O que não foi expressamente permitido é proibido”

É uma ferramenta importante nos processos de monitoramento e auditoria de uma rede e também pode ser parte da solução de detecção de intrusos e rastreamento de ataques.

Mecanismos de Segurança

Firewall

- Filtro de pacotes
- Network Address Translation – NAT
- Application Level Proxies
- Virtual Private Network – VPN
- Monitoramento em tempo real

Mecanismos de Segurança

Virtual Private Network

VPN ou Rede Privada Virtual permite uma troca segura de informações através da rede publica utilizando o conceito de “tunneling”.

A principal vantagem da VPN é o seu baixo custo para conexões locais e internacionais.

Comumente é chamada de extranet pois permite conexões externas nos servidores internos. Muito utilizada por vendedores e agentes externos.

Mecanismos de Segurança

Assinatura Digital

A assinatura digital utiliza-se do algoritmo “hash” executado no documento digital resultando em um “fingerprint”. Em seguida encripta-se o “fingerprint” com a chave privada do remetente.

O destinatário decripta a assinatura original utilizando-se da chave pública do remetente e recalcula o “fingerprint”.

Coincidindo, o documento é válido.

A prova que o signatário do documento é quem diz ser é realizada por meio de um Autoridade Certificadora que tem a autoridade para conferir as credenciais do proprietário do par de chaves assimétricas.

Mecanismos de Segurança

Certificados Digitais e “Public Key Infraestruture – PKI”

A tecnologia da certificação está baseada na criptografia assimétrica e exige uma estrutura complexa, muito bem definida, chamada “Public Key Infraestructure – PKI”.

Entidade de registro

Registro e Comprovação e aprovação para emissão

Entidade de Certificação

Emissão, Suspensão, Revogação, Expiração e Armazenamento

Diretório

Diretório

Mecanismos de Segurança

Secure Eletronic Transaction – SET

É um conjunto de especificações técnicas desenvolvidas pela Visa e Mastercard em conjunto com diversas empresas entre elas IBM, e Microsoft.

Este conjunto permite a realização de transações financeiras em redes abertas de modo seguro e homogêneo.

A segurança é garantida com técnicas de criptografia durante as etapas de identificação, autorização, autenticação e da compra e venda eletrônica.

Mecanismos de Segurança

Monitoramento

Sistema de Detecção de Intrusos

- Sistema de detecção de intrusos de rede
- Verificadores de integridade de sistema
- Honeypot
- Monitores de log
- Sniffers

Vírus e Antivírus

Log e trilhas de auditoria

Uma visão geral do contexto

(Explicação)

Sistema Brasileiro de Pagamentos

(Explicação)

Referências

- PricewaterhouseCoopers, **Segurança em Banco Eletrônico. São Paulo**, 2000
- Cartilha Ministério Planejamento – **A segurança das Informações e a Internet**
- Cartilha Ministério Planejamento – **Fundamentos do Modelo de Segurança da Informação**
- **Decreto nro. 3505 de 13 de junho de 2000**

www.certisign.com.br

www.serasa.com.br

www.redegoverno.gov.br

www.trueaccess.com.br

FIM