Sistemas de Informação

Segurança e Auditoria em Sistemas de Informação

Prof. Jorge Raniere
E-mail: jorgeraniere@gmail.com

Slides: Profa. Paula Luciana

SEGURANÇA

1. Estado, condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais.
2. Estado, qualidade ou condição de seguro.
3. Condição daquele ou daquilo em que se pode confiar.
4. Certeza, firmeza, convicção.

[Dicionário Houaiss]

INFORMAÇÃO (*Lembrete Básico*)**:** Definição

A informação é um conjunto de dados, imagens, textos, etc., que representam valores, situações, posições, conhecimentos necessários para o funcionamento da empresa.

Sendo um ativo valioso para qualquer Organização, independente da atividade, a informação deve ser protegida contra perda, destruição indevida, divulgação e acessos não autorizados.

As informações confidenciais são importantes para a sua Organização...
...para a concorrência também !

Segurança da Informação: Classificação da Informação

Existe a necessidade de classificação da informação em níveis de prioridade, respeitando a necessidade de cada empresa, assim como, a importância da classe de informação para a manutenção das atividades da empresa:

- **Pública** – informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;

- **Interna** – o acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;

Segurança da Informação: Classificação da Informação

• **Confidencial** – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;

• **Secreta** – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia.

Segurança da Informação: Ciclo de Vida da Informação

O **Ciclo de Vida** é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa.

Segurança da Informação: Ciclo de Vida da Informação

Considerando às situações em que a informação é exposta a ameaças que colocam em risco suas propriedades e atingem a sua segurança, é importante conhecer **o ciclo de vida da informação**:

- **Identificação das necessidades e requisitos –** "mola propulsora"

- **Obtenção (Manuseio) –** Momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação Internet, ou, ainda, ao utilizar sua senha de acesso para autenticação, por exemplo.

Segurança da Informação: Ciclo de Vida da Informação

- **Tratamento** – Quando necessário, momento de organização, formatação, classificação ou análise da informação, para que a mesma fique mais acessível e de fácil utilização.

- **Transporte (Distribuição)** – Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico, ao postar um documento via aparelho de fax, ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo.

- **Uso** – Momento em que a informação é usada para gerar valor para a organização.

Segurança da Informação: Ciclo de Vida da Informação

• **Armazenamento** - Momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel, ou, ainda em uma mídia de USB depositada na gaveta da mesa de trabalho, por exemplo.

• **Descarte** – Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um USB usado que apresentou falha na leitura.

Ativos de Informação: Conceito

Ativo é tudo aquilo que armazena ou manipula direta ou indiretamente uma informação, inclusive ela, dentro da Organização.

Ativos de Informação: Divisão

Os ativos de informação são divididos em alguns grupos, são exemplos deles os citados abaixo:

Ativos de Informação: Banco de Dados, documentação de sistemas, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação;

Ativos de Software: Aplicativos, Sistemas (desenvolvidos internamente/comprados), Linguagens de programação, Utilitários;

Ativos Físicos: Equipamentos computacionais (processadores, monitores, modems), equipamentos de comunicação (roteadores, PABX, fax, secretárias eletrônicas), mídia magnética (fitas e discos), outros equipamentos técnicos (no-break, ar-condicionado), mobília, acomodações;

Serviços: Comunicação, aquecimento, iluminação, eletricidade, refrigeração

Fonte: NBR ISO/IEC 17799

Classificação
do sigilo e criticidade dos ativos de Informação

Classificação do sigilo e criticidade dos ativos de Informação

Como manipular, armazenar e tratar a informação?

Hoje em dia, a informação é reconhecida por todos como o patrimônio mais valioso em qualquer organização.

Para que sejam **manipuladas, armazenadas e tratadas de modo adequado**, as informações devem ser classificadas de acordo com o seu grau de sigilo e criticidade para que se possa assegurar que recebam um **nível apropriado de proteção.**

Classificação do sigilo e criticidade dos ativos de Informação

Exemplos de níveis de sigilo

Classificação quanto a Confidencialidade:

Nível 1: Informação pública
Nível 2: Informação Interna
Nível 3: Informação confidencial
Nível 4: Informação secreta

Classificação do sigilo e criticidade dos ativos de Informação

Exemplos de níveis de criticidade

Classificação quanto a Disponibilidade:

Nível 1: Informações que devem ser recuperadas em minutos
Nível 2: Informações que devem ser recuperadas em horas
Nível 3: Informações que devem ser recuperadas em dias
Nível 4: Informações que não são críticas

Classificação do sigilo e criticidade dos ativos de Informação

Qual informação deve ser classificada?

Armazenada no Banco de Dados da empresa;
Enviada por e-mail;
Enviada através de fax;
Enviada pela rede da empresa;
Impressa ou escrita em papel;
Gravada em dispositivos móveis;
Apresentada em reunião/projetor
Falada em conversa ao telefone
… ou outro método usado para transmitir conhecimento e/ou idéias.

Classificação do sigilo e criticidade dos ativos de Informação

Requisitos de controle

Reprodução: Devem ser especificados os procedimentos para reprodução (em papel ou eletrônica) e impressão de informações através de relatórios, etc.

Distribuição/Divulgação: Deve ser especificado quem tem autorização para determinar os critérios para distribuição e/ou divulgação de informações sensíveis.

Transmissão (por voz, fax, e-mail, correio, viagem):
Devem estar descritos os procedimentos para o controle de transmissão de informações por voz, telefones, celulares, secretárias eletrônicas e correio de voz.

Classificação do sigilo e criticidade dos ativos de Informação

Requisitos de controle

Armazenamento: Devem estar descritas todas as diretrizes que digam respeito aos procedimentos para guarda física e eletrônica das informações.

Destruição: Devem ser especificados os critérios para eliminação e/ou destruição física e eletrônica de informações.

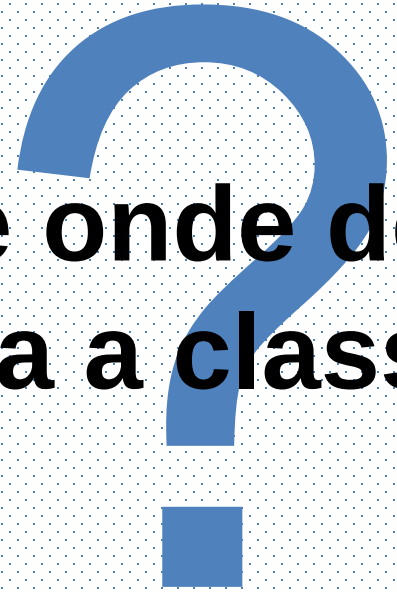
Classificação do sigilo e criticidade dos ativos de Informação

Exemplo de itens que podem necessitar descarte seguro:

Documentos em papel;
Papel carbono;
Relatórios impressos;
Fitas magnéticas;
Disquetes;
CD;
Listagem de programas;
Dados de teste;
Documentação de sistemas.

Classificação do sigilo e criticidade dos ativos de Informação

Rótulo da classificação



Como e onde deve estar indicada a classificação

Classificação do sigilo dos ativos de Informação

Rótulo da classificação

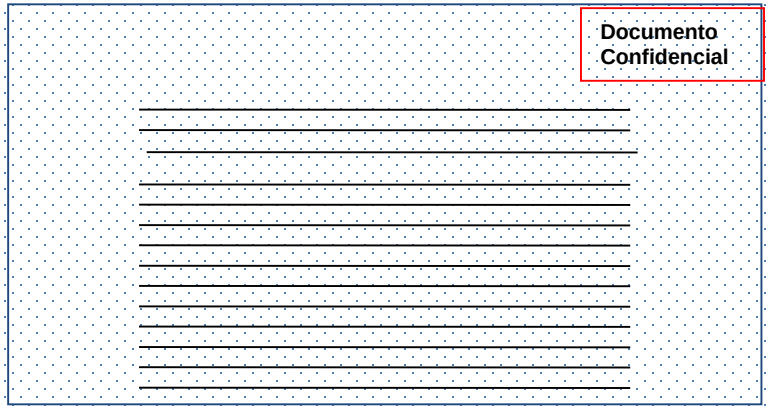
Deve existir um conjunto de procedimentos para rotular e tratar a informação, de acordo com o esquema de classificação adotado pela empresa.

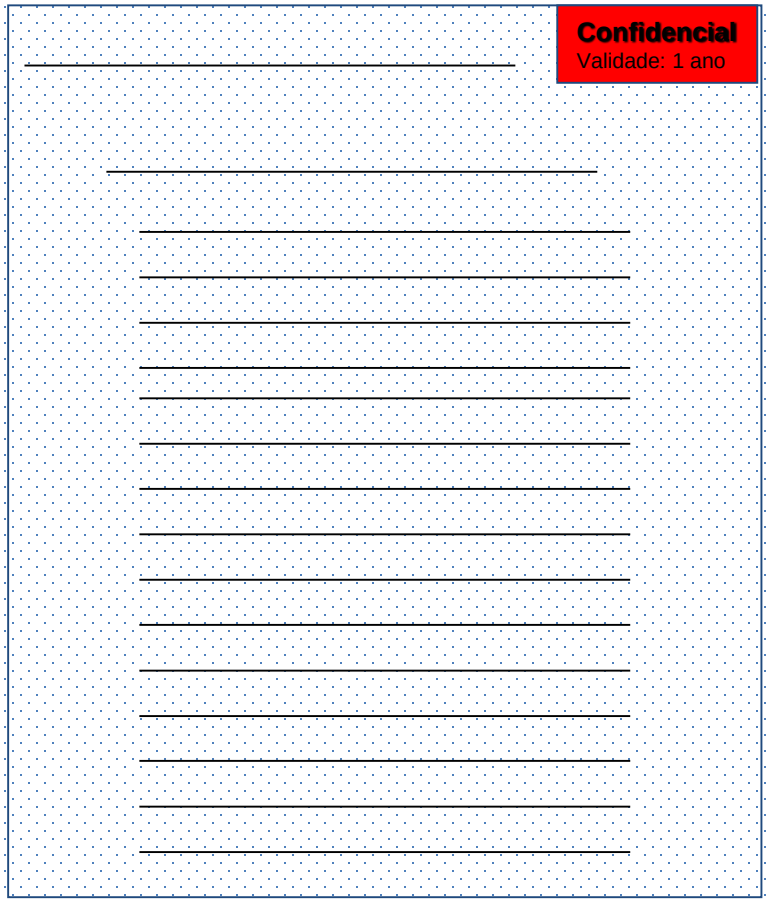
Os procedimentos para classificação devem abranger informações nos formatos:

- Físicos
- Lógicos

Classificação do sigilo dos ativos de Informação

Exemplos de Rótulo da classificação





Segurança da Informação: Definição

É um processo contínuo de proteção aos ativos de informação contra os diversos tipos de ameaças que possam impactar negativamente o ambiente, garantindo a continuidade dos negócios, minimizando danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

Segurança da Informação: Exemplo

Segurança da Informação: Exemplo

Conceitos

• **hackers -** São indivíduos que elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas. Os Hackers utilizam todo o seu conhecimento para melhorar softwares de forma legal. Além de a maioria dos hackers serem usuários avançados de Software Livre como o GNU/Linux.

• **crackers -** Invasores de computadores são denominados Cracker e o termo designa programadores maliciosos e ciberpiratas que agem com o intuito de violar ilegal ou imoralmente sistemas cibernéticos.

Segurança da Informação: Objetivo

A Segurança da Informação tem o objetivo de assegurar os seguintes quesitos de segurança:

Disponibilidade

Integridade

Confidencialidade

Segurança da Informação: Quesitos

Quesito: **Disponibilidade**

Garantia de que os usuários autorizados obtenham acesso a informação e aos ativos correspondentes **sempre que necessário.**

Segurança da Informação: Disponibilidade

Incidente de segurança gerando quebra de disponibilidade:

- **perda de documentos,**
- **computadores "fora do ar",**
- **servidores inoperantes em função de ataques e invasões.**

Motivos para tornar informações indisponíveis:

- **incêndio,**
- **enchentes,**
- **tempestades,**
- **terremotos,**
- **ataques físicos,**
- **bombas,**
- **vandalismo.**

Segurança da Informação: Quesitos

Quesito: **Integridade**

Garantia de que a informação se manterá integra e portanto não sendo permitida a sua **alteração ou destruição de maneira não autorizada.**

Segurança da Informação: Integridade

Quando intencionalmente ou não uma informação é alterada, por falsificação, alteração de registro de banco de dados, configura-se num *incidente de segurança* da informação por quebra de integridade.

Podem alterar informações:

- **migração de dados em base de dados,**
- **arquivo sem chave,**
- **salas não trancadas,**
- **líquido sobre papéis ou**
- **meios magnéticos**

Segurança da Informação: Integridade

Podemos citar que algum individuo malicioso tenha enviado um e-mail falso para algum usuário da rede, dizendo ser o administrador. Neste ponto entraria o treinamento do usuário da rede, e no quanto este é ingênuo. Lógico que também varia o quanto o Cracker é malicioso e criativo. Nunca devemos subestimar o inimigo.

Segurança da Informação: Quesitos

Quesito: **Confidencialidade**

Garantia de que o acesso à informação seja obtido **somente por pessoas autorizadas.**

Segurança da Informação:
Confidencialidade

Casos típicos de quebra de confidencialidade:
- Invasões de sistemas de computadores.

Casos corriqueiros e menos notados de quebra de confidencialidade:
- Pessoas de determinada organização conversam sobre assuntos de trabalho, muitas vezes confidenciais, em locais públicos, disponibilizando a informação para aqueles à sua volta.

Segurança da Informação:
Confidencialidade

Técnica utilizada para obter informações confidenciais:

- **Engenharia social: Indivíduo utiliza-se de métodos de sugestão e convencimento para induzir uma pessoa a quebrar um protocolo ou procedimento de segurança.**

Para que haja confidencialidade não basta que uma rede tenha criptografia.
De que adiantaria ter tudo isso se um individuo malicioso possui acesso livre na rede? Ele acaba de alguma forma, não muito difícil, conseguindo a chave dos outros usuários (‘se você recebesse um e-mail da rede dizendo, para você enviar sua senha, você enviaria? a maioria sim!').

Segurança da Informação:
Confidencialidade

Por isso a rede tem que estar protegida de todas as maneiras possíveis.

Deve haver um treinamento com todos os usuários da rede para que não passem suas senhas para outras pessoas. Somente em casos extremos! Talvez até, se possível, exigindo que seja feita a negociação pessoalmente.

Segurança da Informação

O CID (Confidencialidade, Integridade e Disponibilidade) é, sem dúvida, a propriedade básica da segurança da informação. Qualquer sistema que se diga seguro deve garantir a Confidencialidade, Integridade e Disponibilidade.

Mas se pensarmos bem, o CID também funciona sem um dos seus princípios. Por exemplo, em sites abertos ao publico você precisa de Integridade e Disponibilidade, mas não precisa de Confidencialidade, uma vez que qualquer pessoa poderá ver aquelas informações, a não ser em áreas que precisam de algum tipo de login.

Segurança da Informação

O item integridade não pode ser confundido com confiabilidade do conteúdo (seu significado) da informação. Uma informação pode ser imprecisa, mas deve permanecer integra (não sofrer alterações por pessoas não autorizadas).

A combinação em proporções apropriadas dos itens confidencialidade, disponibilidade e integridade facilitam o suporte para que as empresas alcancem os seus objetivos, pois seus sistemas de informação serão mais confiáveis.

Segurança da Informação

Outros Itens Importantes:

- **Autenticação –** Garante que o usuário é de fato, quem alega ser.

- **Retratabilidade (Não-repúdio)** – Capacidade do sistema de provar que um usuário executou uma determinada ação.

- **Privacidade –** Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve ser vista / lida / alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste caso é atribuído o caráter de confidencialidade a informação); É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.

Segurança da Informação

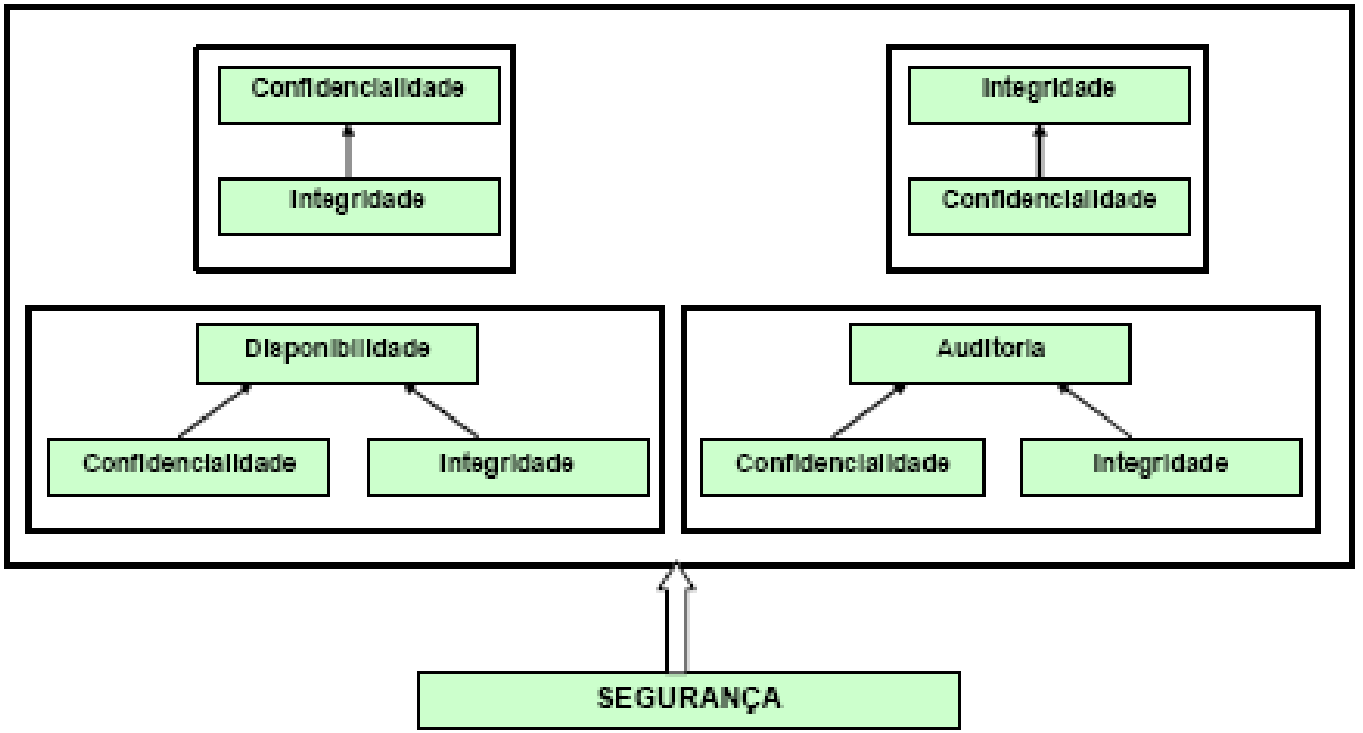
Outros Itens Importantes:

- **Legalidade –** Garante que o sistema está aderente à legislação pertinente.

- **Auditoria –** Rastreabilidade dos diversos passos que um negócio ou processo realizou ou a que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa. Auditoria em software significa uma parte da aplicação, ou conjunto de funções do sistema, que viabiliza uma auditoria; Consiste no exame do histórico dos eventos dentro de um sistema para determinar quando e onde ocorreu uma violação de segurança.

Segurança da Informação

É sugerido que a segurança somente é obtida através da relação e correta implementação de 4 princípios da segurança: confidencialidade, integridade, disponibilidade e auditoria.



Segurança da Informação

A confidencialidade é dependente da integridade, pois se a integridade de um sistema for perdida, os mecanismos que controlam a confidencialidade não são mais confiáveis.

A integridade é dependente da confidencialidade, pois se alguma informação confidencial for perdida (senha de administrador do sistema, por exemplo) os mecanismos de integridade podem ser desativados.

Auditoria e disponibilidade são dependentes da integridade e confidencialidade, pois estes mecanismos garantem a auditoria do sistema (registros históricos) e a disponibilidade do sistema (nenhum serviço ou informação vital é alterado).

Segurança da Informação

Benefícios para a Organização

- Segurança das informações;
- Segurança para a continuidade do negócio;
- Novas aplicações e negócios viabilizados com segurança;
- Baixo índice de perdas por fraudes e erros (tendendo a zero);
- Baixo índice de vazamento de informações (tendendo a zero);
- Relação de confiança com clientes e fornecedores fortalecida pelo sistema de segurança;
- Colaboradores atentos à segurança;
- Identificação e redução de riscos;
- Redução de despesas com prejuízos por paralisação do negócio e vazamento de informações, dentre outros;
- Etc…

Segurança da Informação: Morais da Segurança

Como não poderia deixar de ser, a segurança também possui algumas "morais" que surgiram no decorrer do tempo:

• As portas dos fundos são tão boas quanto às portas da frente.

Segurança da Informação: Morais da Segurança

- **Uma corrente é tão forte quanto o seu elo mais fraco.**

Segurança da Informação: Morais da Segurança

- **Um invasor não tenta transpor as barreiras encontradas, ele vai ao redor delas buscando o ponto mais vulnerável.**