**Anotações segurança da informação**

**Aula 6**

A política de segurança da informação é o que direciona e, portanto, antecede as ações práticas de segurança da informação.

É importante conhecer os requisitos necessários para a elaboração da Política de Segurança da Informação. Confira:

* Especificar a organização -> Com base no perfil da organização a ser protegida, descreva o que precisa ser protegido, tanto internamente quanto externamente. A organização deve eleger um Comitê Gestor, formado por diretores e gerentes da organização.
* Especificar os itens -> Analise os itens a serem protegidos, avalie se há necessidade de ajustes, com inclusão ou remoção de itens.
* Avaliar itens -> Avalie para cada item quais os riscos, como deve ser protegido, de quem e por quanto tempo (o Comitê Gestor deve avaliar e propor melhorias e ajustes).
* Normas e procedimentos -> Elaborar normas, procedimentos e proibições para tudo relativo à organização, como controle de acesso, restrição na navegação na internet, cuidados na manipulação de arquivos, etc.
* Treinamento -> 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 funcionários da organização.
* Prazos -> Determinar de quanto em quanto tempo a política precisa ser reavaliada e ajustada. A política de segurança da informação deve ser sempre melhorada.
* Aceite -> A proposta de Política de Segurança da Informação deve ser apresentada e aprovada pelos gestores da organização (Comitê Gestor).

Os cinco passos da política de segurança e as boas práticas

1. Avaliação das informações

Neste primeiro passo deve-se avaliar as informações e a sua importância no negócio da organização. Essa avaliação determina a prioridade das informações, a necessidade de redundância de uma informação com cópia de segurança, mecanismos de recuperação e o controle de acesso a esses dados

1. Classificação das informações

o segundo passo é classificar a informação em pública, interna, confidencial ou secreta.

* Pública -> São as informações que, se forem divulgadas fora da organização, não causarão impactos aos negócios.
* Interna -> Esse tipo de informação deve ser protegido e sua divulgação dever ser evitada, porém, caso seja divulgada, não causará impactos à organização.
* Confidencial -> São informações confidenciais dentro e fora da organização e que não podem ser acessadas por pessoas não autorizadas.
* Secreta -> As informações secretas são aquelas que não devem de forma alguma ser divulgadas, pois podem afetar os negócios da organização.

1. Regras de Acesso e Responsabilidades

No terceiro passo temos que criar as diretrizes em relação ao acesso, cada setor da organização deve especificar quais informações cada pessoa terá acesso, além disso deve especificar como irá recuperar alguma informação perdida, como e em quanto tempo.

1. Treinamento

No quarto passo será o treinamento dos funcionários, onde deve comtemplar todos os cuidados necessários durante a execução de suas atividades e informar a importância da gestão da informação. O treinamento deve ser formalizado em um documento, disponibilizado a todos os funcionários e atualizado constantemente.

1. Punições

O último passo é definir quais punições serão aplicadas em caso de desobediência das normas. O grau de punição deve ser relativo ao valor da informação e ao prejuízo causado.

As punições devem ser claras e justas, para isso as políticas de segurança devem ser transparentes, obrigatórias e de fácil leitura e compreensão

Boas práticas:

* Ao se ausentar do computador suspenda a sessão.
* Coloque o modo de proteção de tela com exigência de senha após um curto período de inatividade.
* Guarde bem documentos confidenciais.
* Ao compartilhar alguma informação, confirme se o destinatário está correto.
* Ao receber algum visitante na organização, identifique-o e não o deixe desacompanhado.
* Não crie senhas com dados pessoais.
* Em caso de detecção de vírus no seu computador, solicite o suporte da organização e faça uma cópia dos dados importantes.

Aula 7

Criação de aplicações seguras

Quando se desenvolve uma aplicação são necessários cuidados relacionados à segurança que envolvem tanto o ambiente como a equipe técnica de desenvolvimento.

É possível avaliar o nível de segurança de uma aplicação em função dos recursos utilizados para impedir ataques.

A norma que especifica as diretrizes para criação de aplicações seguras é a norma ISO/IEC 15408 e tem como objetivo fornecer um conjunto de critérios fixos que especifique a segurança de uma aplicação, de forma não ambígua, a partir de características do ambiente da aplicação, e definir formas de garantir a segurança da aplicação para o cliente final.

A ISO/IEC 15408 apresenta 4 níveis de garantia de segurança(EAL – Evaluation Assurance Level):

* Nível 1 -> A sua função é testar as funcionalidades do sistema(ver se os requisitos foram atendidos) e identificar as proteções necessárias contra ameaças.
* Nível 2 -> A sua função é certificar que a aplicação desenvolvida atenda aos padrões estabelecidos. Além disso, deve-se realizar uma busca por vulnerabilidades do sistema e aplicar testes em relação a segurança e validação dos dados.
* Nível 3 -> A sua função é aplicar procedimentos de segurança sem que o sistema sofra com mudanças, além de propiciar testes completos do sistema sem precisar da reengenharia.
* Nível 4 -> A sua função é garantir maior segurança durante o desenvolvimento do sistema, aplicando procedimento de testes.

Características de um ambiente seguro

A segurança inicia no ambiente de trabalho com a aplicação de controles relacionados aos acessos físicos, além da proteção lógica dos servidores.

Etapas para segurança no ambiente de desenvolvimento

Para se manter um ambiente seguro deve-se ter regras formalmente especificadas, de fácil entendimento, e que tenha alguém responsável por as regras em uso na empresa, avaliando-as e adaptando-as periodicamente.

Etapas do modelo de segurança:

1. Gerência de configuração -> é sugerido que haja uma gerência permanente no ambiente de desenvolvimento. Essa gerência tem por função prevenir modificações, inserções e deleções sem autorização na documentação do sistema.
2. Distribuição -> é importante garantir que a versão disponibilizada para implantação tenha as características especificadas de segurança.
3. Desenvolvimento -> As funcionalidades de segurança devem ser representadas em todos os níveis de abstração. Desde o projeto lógico até a implementação.
4. Documentação -> Deve-se ter dois manuais de auxílio um para usuários (deve conter instruções de uso, descrição das funções de segurança e outro para os administradores(deve conter informações para manutenção, administração e configuração, garantindo um uso correto e seguro do sistema).
5. Suporte ao ciclo de vida -> Os requisitos para assegurar o sistema depende do modelo de ciclo de vida adotado.
6. Testes de segurança -> podem ser criados mecanismos de testes para garantir que a aplicação esteja atendendo aos requisitos. Como o uso de ferramentas CASE (*Computer-Aided Software Eninnering)* que disponibiliza testes automatizados.
7. Avaliação de vulnerabilidades -> Deve-se verificar se houve introdução de vulnerabilidades no sistema, seja na fase de desenvolvimento, mau uso do sistema ou aplicação de configurações incorretas. E corrigir caso seja identificada.

A Norma ISO sugere a aplicação de um método de desenvolvimento já bem estruturado, que contemple no mínimo as atividades de planejamento, acompanhamento e definição dos testes para verificação.

Segurança no ciclo de vida de desenvolvimento da aplicação

A garantia da segurança de um sistema está associada a aplicação de cuidados especiais durante seu desenvolvimento, resultando em um código fonte confiável mais seguro e robusto. Com isso a produção do código seguros torna a aplicação mais lenta, mas pode-se realizar investimentos em equipamentos.

São definidos quatro normas e práticas da boa programação:

1. Funções intrinsecamente seguras -> É fazer uso de linguagens no qual o programador poderá criar funções ou utilizar funções que sejam seguras.
2. Verificar códigos de erro retornado por função ou método -> Sempre que se fizer uma chamada da função, a mesma deve ser testada.
3. Atentar para tamanho de buffers e arrays do sistema -> Sempre operar o sistema de acordo com as permissões requeridas para executar suas tarefas de forma adequada.
4. Documentar o código -> documentar corretamente todo o código evita mal-entendidos na leitura dele ou ainda usá-lo incorretamente.

**Aula 8**

Segurança cibernética -> é um esforço contínuo para proteger indivíduos, organizações e governos de ataques digitais

Os 3 níveis de proteção:

* Particular -> Você precisa proteger sua identidade, seus dados e seus dispositivos de computação.
* Corporativo -> É responsabilidade de todos proteger a reputação, os dados e os clientes da empresa.
* Governo -> À medida que mais informações digitais são coletadas e compartilhadas, sua proteção se torna ainda mais vital pois pode influenciar a segurança nacional, a estabilidade econômica, a segurança e o bem-estar dos cidadãos.

Dados pessoais são informações que possam ser usadas para identificar um individuo, pode existir tanto offline quanto online.

* Identidade offline -> é a pessoa da vida real que você apresenta em casa, escola, trabalho etc. são detalhes sobre sua vida pessoal como, nome completo, idade, endereço.
* Identidade Online -> É quem você é e como você se apresenta aos outros on-line. Ele inclui o nome de usuário que você usa para suas contas online, bem como a identidade social que você estabelece e retrata em comunidades e sites online. Você deve limitar a quantidade de informações pessoais que revela através de sua identidade on-line.

Dados corporativos são dados normalmente gerados e mantidos por todas as organizações, grandes e pequenas. Ele inclui o seguinte:

* Dados Transacionais -> São as informações para tomar decisões de trabalho como detalhes relacionados a compras e vendas, atividades de produção e operações organizacionais básicas.
* Propriedade Intelectual -> São patentes, marcas registradas e planos de novos produtos. Essas informações são geralmente consideradas um segredo comercial e perdê-las pode ser desastroso para o futuro de uma empresa.(informação secreta – aula 6)
* Dados Financeiros -> São dados de pagamentos, balanços, fluxos de caixa, proporcionam detalhes da saúde financeira da empresa. (informação confidencial - aula 6)

Internet das Coisas (IoT) e Big Data

A IoT é uma grande rede de objetos físicos conectados à Internet, com a capacidade de coletar e compartilhar dados. Com o crescimento de exponencial dos dados foi criada uma área da tecnologia chamada de “Big Data”.

O cubo

O Cubo de McCumber é uma estrutura de modelo criada por John McCumber em 1991 para ajudar as empresas a estabelecer e avaliar iniciativas de segurança da informação considerando todos os fatores relacionados que as afetam. Esse modelo de segurança tem três dimensões:

1. Princípios fundamentais para proteger as informações:

* Confidencialidade -> é um conjunto de regras que evita a divulgação de dados sensíveis. Os métodos para garantir a confidencialidade incluem **criptografia de dados**, **prova de identidade**e **autenticação de dois fatores**.
* Integridade -> garante que as informações ou os processos do sistema sejam protegidos contra modificações. Os métodos para garantir a integridade incluem o **uso de função HASH** ou **soma de verificação**.
* Disponibilidade -> significa que os usuários autorizados podem acessar sistemas e dados quando e onde necessário. Os métodos para garantir a disponibilidade são a **manutenção de equipamentos, manter os sistemas operacionais e software atualizados** e **criando de backups**.

1. Proteção da informação em cada um de seus possíveis estados:

* Em processamento -> refere-se aos dados que estão sendo usados para executar uma operação.
* Em armazenamento -> refere-se a dados armazenados na memória ou em um dispositivo de armazenamento permanente.
* Em transmissão -> refere-se a dados que trafegam entre sistemas de informações.

1. Medidas de segurança usadas para proteger os dados:

* Treinamento, Conscientização e educação -> são as medidas adotadas por uma organização para garantir que usuários tenham conhecimento sobre as possíveis ameaças à segurança e as ações que podem tomar para proteger os sistemas de informações.
* Tecnologia -> se refere às soluções de software e hardware projetadas para proteger sistemas de informações.
* Política e Procedimento -> se referem aos controles administrativos que fornecem uma base sobre como uma empresa implementa a garantia de informações.