QUESTÕES BASEADAS NA NBR ISO/IEC 17799 - ATIVIDADE EM GRUPO.

Membros: Andrey, Davi, Eduardo Ribas e Felipe 3ºC

O que é a informação e como ela pode existir dentro de uma organização? Por que é importante protege-la?

R: A informação pode ser definida por compartilhamento de conhecimento e dados. Ela é importante em uma organização para manter a comunicação entre os funcionários, que pode ser feita através arquivos digitais, documentos, relatórios ou e-mails. A proteção desses dados é necessária para manter a segurança de todos dentro de uma organização, protegendo informações gerais da empresa e dos funcionários.

Quando falamos de segurança da informação o que significa os termos: confidencialidade, integridade e disponibilidade?

R: Quando estamos se referindo ao conceito de confidencialidade se trata da proteção de informações e dados que não podem ser acessados por qualquer pessoa que não possua permissão. Ao falar de integridade estamos mencionando o fato de que a informação deve se manter inalterável, ou seja, da maneira em que recebida, deve ser armazenada sem nenhuma alteração em seu conteúdo. Por fim, a disponibilidade garante o acesso à informação e aos dados quando realmente for necessário, estando disponível a qualquer momento, necessitando de uma estrutura organizada.

Como podemos obter Segurança da Informação?

R: A Segurança da Informação pode ser obtida usando esses métodos:

Identificação dos riscos: Realizar uma análise de risco para identificar ameaças e vulnerabilidades nas informações da empresa.

Controles de acesso: Implementar políticas de controle de acesso para proteger as informações de acessos não autorizados, como autenticação de usuário, senhas, tokens, biometria, entre outros.

Criptografia: Utilizar criptografia para proteger as informações confidenciais, de forma a garantir a privacidade e a integridade dos dados.

Backup e recuperação: Realizar backups regulares dos dados para garantir a recuperação em caso de perda de informações.

Políticas e procedimentos: Estabelecer políticas e procedimentos de segurança da informação para orientar os funcionários sobre como lidar com as informações da empresa.

Treinamento e conscientização: Realizar treinamentos e conscientização dos funcionários sobre a importância da segurança da informação e como evitar incidentes de segurança.

Atualizações e correções: Manter atualizados os sistemas, aplicativos e dispositivos utilizados para armazenar e processar informações, aplicando correções de segurança quando necessário.

Monitoramento: Monitorar constantemente os sistemas e a rede da empresa para identificar possíveis ameaças e vulnerabilidades, e tomar as medidas preventivas necessárias.

Quais são os principais tipos de ameaças à segurança da informação?

R: Existem vários tipos de ameaça, e entre elas estão:

Malware: programas maliciosos, como vírus, cavalos de Troia e ransomware, que se infiltram em sistemas de computador para danificá-los ou roubar informações.

Ataques de phishing: tentativas de obter informações confidenciais, como senhas e informações financeiras, por meio de e-mails, mensagens de texto ou outras formas de comunicação eletrônica.

Ataques de engenharia social: manipulação psicológica de pessoas para que revelem informações confidenciais.

Acesso não autorizado: tentativas de entrar em sistemas de computador ou redes sem permissão.

Roubo de dispositivos: perda ou roubo de laptops, smartphones, tablets ou outros dispositivos que contêm informações sensíveis.

Como uma organização pode identificar os seus requisitos de segurança?

R: Para identificar os requisitos de segurança, é necessário realizar alguns desses passos:

Avaliar os riscos: a organização deve identificar os ativos de informação que possui e avaliar os riscos associados a cada um deles. Isso ajudará a determinar quais informações são mais críticas e precisam de mais proteção.

Definir políticas e padrões de segurança: a organização deve desenvolver políticas e padrões de segurança da informação para orientar as práticas de segurança e garantir que todos os colaboradores estejam cientes das expectativas de segurança.

Identificar os requisitos regulatórios e legais: a organização deve entender as regulamentações e leis aplicáveis à sua indústria e garantir que esteja em conformidade com elas.

Identificar os requisitos do cliente: se a organização estiver processando informações confidenciais do cliente, ela deve garantir que esteja atendendo às expectativas de segurança do cliente.

Identificar os requisitos internos: a organização deve entender seus próprios requisitos internos de segurança, incluindo requisitos de acesso, treinamento e controle de acesso.

Como realizar análises críticas periódicas dos riscos de segurança e dos controles?

R: Para realizar análises criticas é preciso:

Identificação dos ativos de informação: é necessário identificar quais são os ativos de informação da organização, ou seja, quais informações são críticas para o negócio e precisam ser protegidas.

Identificação das ameaças e vulnerabilidades: é importante identificar as possíveis ameaças que podem comprometer a segurança dos ativos de informação, bem como as vulnerabilidades que podem ser exploradas por essas ameaças.

Avaliação dos riscos: com base nas informações coletadas nos passos anteriores, é necessário avaliar os riscos associados aos ativos de informação, definindo a probabilidade de ocorrência e o impacto que cada risco pode causar na organização.

Definição dos controles de segurança: após a avaliação dos riscos, é preciso definir os controles de segurança necessários para mitigar ou reduzir esses riscos, bem como estabelecer uma hierarquia de prioridades para implementá-los.

Implementação dos controles de segurança: com os controles definidos, é hora de implementá-los na organização, de acordo com a hierarquia de prioridades estabelecida.

Quais são os controles considerados essenciais para uma organização?

R: Existem diversos controles considerados essenciais para uma organização, mas alguns exemplos são:

Políticas de segurança da informação: documento que estabelece as diretrizes e as regras para o uso da informação na organização, incluindo as medidas de proteção a serem adotadas.

Controle de acesso: conjunto de medidas que garantem que somente pessoas autorizadas tenham acesso à informação e aos recursos da organização.

Criptografia: técnica de codificação de informações que impede que elas sejam acessadas por pessoas não autorizadas.

Backup e recuperação de dados: medidas para garantir a disponibilidade e a integridade das informações, mesmo em caso de perda de dados.

Gerenciamento de vulnerabilidades: processo para identificar, avaliar e corrigir as vulnerabilidades de segurança da informação na organização.

Monitoramento de segurança: atividade que tem como objetivo identificar e responder a possíveis incidentes de segurança da informação.

Conscientização e treinamento em segurança: programas para conscientizar os colaboradores sobre a importância da segurança da informação e para treiná-los em boas práticas de segurança.

Quais são os controles considerados como melhores práticas para a segurança da informação?

R: Existem várias melhores práticas para a segurança da informação. Algumas delas são:

Utilização de senhas fortes e complexas, com trocas periódicas;

Utilização de criptografia para proteger informações confidenciais;

Implementação de firewalls e antivírus para proteger redes e sistemas;

Utilização de autenticação de dois fatores para aumentar a segurança de contas e sistemas;

Implementação de controles de acesso para limitar o acesso às informações confidenciais apenas para usuários autorizados;

Realização de backups regulares para proteger as informações em caso de perda de dados ou falhas no sistema;

Realização de treinamentos regulares de conscientização em segurança da informação para os funcionários;

Realização de testes de invasão e vulnerabilidade periodicamente para identificar possíveis brechas de segurança;

Implementação de políticas claras de segurança da informação e conformidade com regulamentações e leis aplicáveis.

Quais são os fatores críticos para o sucesso da implementação da segurança da informação dentro de uma organização?

R: Para o sucesso da implementação, é necessário seguir uma série de condutas que garantem a segurança da informação. São alguns deles: Política de segurança; Enfoque consistente para implementação; Comprometimento e apoio visível da direção; Proporcionar educação e treinamento adequado;

As empresas podem criar suas próprias recomendações de segurança?

R: Sim, porém é necessário seguir certas normas, como objetivo, termos e definições, segurança da informação, avaliação de risco, gerenciamento de risco e política de segurança.

Qual a diferença entre avaliação de risco e gerenciamento de risco?

R: Em resumo, a avaliação de risco é um processo que envolve a identificação de riscos e a avaliação da probabilidade de sua ocorrência. Já o gerenciamento de risco é um processo mais abrangente que inclui a identificação, avaliação e controle dos riscos. O objetivo do gerenciamento de risco é minimizar ou mitigar os riscos identificados por meio de medidas preventivas, corretivas e de contingência. É um processo contínuo que exige revisão e atualização constante das estratégias de gerenciamento de risco para garantir que os riscos estejam sendo adequadamente gerenciados e controlados.

Qual o objetivo de uma Política de segurança da informação e o que deve conter este documento?

R: O objetivo é prover à direção uma orientação e apoio para a segurança da informação. Convém que a direção estabeleça uma política clara e demonstre apoio e comprometimento com a segurança da informação através da emissão e manutenção de uma política de segurança da informação para toda a organização.

Como deve ser feita a Análise crítica e avaliação da Política de Segurança de uma empresa?

R: Convém que a política tenha um gestor que seja responsável por sua manutenção e análise crítica, de acordo com um processo de análise crítica definido. Convém que este processo garanta que a análise crítica ocorra como decorrência de qualquer mudança que venha a afetar a avaliação de

risco original, tais como um incidente de segurança significativo, novas vulnerabilidades ou mudanças organizacionais ou na infra-estrutura técnica. Convém que também sejam agendadas as seguintes análises críticas periódicas:

Efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados;

Custo e impacto dos controles na eficiência do negócio;

Efeitos das mudanças na tecnologia

Com relação a Segurança organizacional de uma empresa, porque é importante a criação de uma Infraestrutura da segurança da informação?

R: Para gerenciar a segurança da informação em uma organização, é necessário estabelecer uma estrutura de gerenciamento, com fóruns de liderança para aprovar políticas, coordenar a implementação e buscar especialistas externos para apoio. Deve-se encorajar uma abordagem multidisciplinar, envolvendo gestores, usuários, administradores, projetistas de aplicativos, auditores, equipes de segurança e especialistas em seguros e gerenciamento de riscos.

Quais são as responsabilidades dos gestores de um fórum de segurança da Informação?

R: Convém que a política tenha um gestor que seja responsável por sua manutenção e análise crítica, de acordo com um processo de análise crítica definido. Convém que este processo garanta que a análise crítica ocorra como decorrência de qualquer mudança que venha a afetar a avaliação de risco original, tais como um incidente de segurança significativo, novas vulnerabilidades ou mudanças organizacionais ou na infra-estrutura técnica. Convém que também sejam agendadas as seguintes análises críticas periódicas: a) efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados; b) custo e impacto dos controles na eficiência do negócio; c) efeitos das mudanças na tecnologia.