Planos, procedimentos e políticas de segurança da informação

Apresentar a necessidade da implementação da politica de segurança da informação, como ferramenta de apoio para que possam ser implementados os controles de segurança necessários para preservar os dados e informações da organização.

Desafios para a implementação da segurança

Existem muitos desafios para que os profissionais alocados no processo de Gestão da Segurança da Informação possam implantar a segurança dentro das organizações.

Esses desafios estão ligados a diversos fatores de ordem cultural, administrativa, temporal, obtenção de verbas, gerenciamento de atividades e até mesmo a implantação de novas tecnologias. Dentre esses desafios, podemos citar:

- **Ausência de responsáveis direta e falta de orçamento –** Por causa de algumas empresas não possuírem uma área especifica para tratar do assunto e a falta de orçamento, existe muita dificuldade de se implantar uma infraestrutura padronizada e robusta de segurança e que não impacte nas atividades diárias da empresa.

- **Pessoas-chave no apoio –** A falta de apoio da alta administração também pode ser considerada outra dificuldade, pois geralmente não se consegue obter comprometimento dela para que se possam ser implantadas as medidas previstas no plano de ação de segurança.
- **Profissionais capacitados –** Como em qualquer empresa, a falta de profissionais capacitados de forma adequada contribui também para impactar no desenvolvimento e implantação das ações de segurança nas empresas.

- **Escopo muito abrangente –** O tamanho do projeto de segurança acaba impactando também por causa dos seus altos custos de implementação e das medidas de proteção que, muitas vezes, podem comprometer a receita da empresa, sendo, dessa forma, não aceito por parte da alta administração.
- **Definições de prioridade** – Como o foco da empresa é o negócio e o assunto segurança não é a sua prioridade número um, constantemente os responsáveis pelas organizações vivem nesse dilema entre implementar o controle de segurança ou comprar uma nova máquina para a realização de uma atividade de uma área da empresa.
- **Conscientização –** A falta de conscientização do corpo executivo e de todos os funcionários da organização cria uma barreira quando os controles de segurança necessitam ser implementados, uma vez que eles representarão algum tipo de desconforto para os envolvidos.
- **Organização da empresa** – A inexistência de processos empresariais mapeados contribuirão para dificultar o processo da implementação da segurança, principalmente no momento de se identificar o que é mais importante para a sobrevivência da empresa na ocorrência de um possível problema.

Política de segurança

A ideia da palavra politica está relacionada à ação de colocar ordem em uma determinada situação por meio da implementação de um conjunto de leis, regras e práticas que ajudarão nas situações comuns à coexistência de ideias diferentes e quase sempre conflitantes, de forma que a empresa consiga gerenciar e proteger os seus ativos de informação.

Por trás da política existe sempre a intenção de orientar ou determinar as atitudes que se espera das pessoas que estão envolvidas sob o raio de ação dela. Como cada empresa tem os seus métodos, maneiras de agir, bem como recursos e conceitos próprios, não existe uma receita única que sirva como padrão para ser implementada, analisando-se as situações. Por isso, cabe a cada uma decidir qual deverá ser a melhor maneira de implementá-la.

Muitas das organizações fazem o caminho inverso na elaboração da sua politica de segurança, ou seja, primeiro esperam que os problemas aconteçam para depois começar a implantar os controles necessários para que isso não "volte" a ocorrer, quando o correto seria agir de forma preventiva. A política de segurança da informação é um exemplo de algo que deveria ser feito antes

que o problema ocorresse.

Quanto mais diversificado e abrangente for essa comissão, maior será a possibilidade da divulgação das diretrizes de segurança por toda a empresa, além de que elas poderão identificar os requisitos de segurança particulares para os locais em que se trabalha.

Porém não podemos nos iludir com a ideia de que quanto maior melhor. O certo seria sempre que, na hora da formação dessa comissão, o bom-senso prevalecesse baseando-se em parâmetros, como:

- Tamanho da organização.
- Qual é o nível técnico e de decisão das pessoas que participaram dessa comissão.
- Qual será a sua abrangência.
- Quem são as pessoas-chave dos processos da organização.
- Hierarquia dentro da organização.

Muitas empresas acreditam que a política de segurança da informação deve ser construída com muitos detalhes tentando abordar tudo o que for possível, desde os objetivos estratégicos até detalhes de como deverá ser feita a senha do usuário. O que acaba ocorrendo é que esse tipo de politica geralmente desenvolve um grande volume de papéis e ninguém os segue, apenas servindo como documentos que podem ser apresentados no caso de um processo de auditoria. Com o envolvimento de diversas pessoas de diversas áreas da organização, podemos entender que a elaboração da política de segurança trata-se de uma tarefa complexa e trabalhosa, em que revisões e atualizações periódicas devem constantemente ser implementadas.

Seus benefícios, muitas vezes, só serão percebidos a um médio ou longo prazo, uma vez que a política de segurança será invisível aos olhos de grande parte das pessoas.

A política de segurança da informação pode ser considerada como uma importante ferramenta para combater os problemas de segurança, causados pelas ameaças que agem contra as vulnerabilidades dos diversos ativos da organização.

Ela conscientizará e orientará os funcionários, clientes, parceiros e fornecedores da necessidade do uso seguro dos ativos de informação da empresa, de forma que nem ela e nem os demais tenham problemas durante a manipulação das informações da organização.

Etapas para o desenvolvimento de uma política de segurança da informação

Para que uma política de segurança tenha uma aceitação, é necessário que a alta administração esteja comprometida e dê apoio, além de participar do processo de implantação. O aval da alta administração é muito importante, obrigando de forma indireta que todos aceitem/respeitem as normas e procedimentos que estarão vinculados á política de segurança.

Existem diversas maneiras de se desenvolver uma política de segurança, pois todos os países possuem as suas próprias legislações e normas que podem interferir nos itens que deverão ser abordados.

Levantamento de informações

Podemos começar o nosso trabalho fazendo um levantamento do perfil da empresa e como está a sua atual situação de segurança, ou seja, quais são as iniciativas de segurança existentes, manuais, documentações, normas e procedimentos ou até mesmo de checklists de segurança.

Se a empresa possuir os seus processos internos documentados será de grande ajuda, pois dessa forma poderão ser identificados os principais processos de negócios e a inter-relação existente entre as áreas, bem como as principais dependências dos ativos de informação.

Esse levantamento inicial também ajudará a identificar os principais controles existentes na empresa, além de conhecer o negócio e suas principais vulnerabilidades.

Durante esse levantamento, é de grande importância que as deficiências e fatores de risco sejam numerados e catalogados. Esse levantamento poderá ser feito por meio da utilização de alguns questionários, bem como entrevistas pessoais às pessoas-chave dos processos.

Durante o levantamento será estudado o que deve ser protegido, verificando-se o atual estado de segurança da empresa.

Desenvolvendo os conteúdos da política

Iniciar a criação dos documentos que ajudarão a sustentar a politica de segurança da organização, ou seja, deverão ser elaborados documentos que definirão o que a empresa entende como assunto "segurança da informação" e quais deverão ser os seus objetivos de gerenciamento.

Neste momento também deverão ser criados o comitê de segurança e a área responsável pela segurança da informação. Com base nas informações levantadas anteriormente, deverão ser identificados os proprietários da informação, bem como deverão ser definidos os critérios para a classificação das informações.

Durante o processo de desenvolvimento da documentação são definidas as principais normas de segurança da informação que serão aplicadas aos colaboradores e funcionários da organização. A norma deve ser um documento criado por consenso de todos que estão envolvidos na sua elaboração e deve ser aprovada por um organismo ou entidade reconhecida dentro da organização, com o poder de criar regras, diretrizes ou características para atividades de uso comum e repetitivo de todos os funcionários da organização.

Dentre essas normas podemos citar: norma de backups; norma de segurança física; norma de segurança lógica; norma de controles de acessos; norma do uso da internet; norma do uso do correio eletrônico; norma do uso da computação móvel; norma de classificação da informação; norma de utilização de computadores e notebooks dentro ou fora da organização; norma do uso do ambiente sem fio; norma de utilização de programas; norma para bloqueios e acesso a sites; norma para utilização dos recursos tecnológicos; norma para desenvolvimento e manutenção de sistemas; norma de segurança e gerenciamento de redes e comunicações de dados; norma para o manuseio, transporte, armazenamento e descarte das informações; norma de segregação de funções dentro da organização; norma de definição sobre direitos, permissões e de acesso a recursos de informação etc.

Formato do documento

O documento que contém a política de segurança da informação deve ser formal e aprovado pela alta administração da organização, bem como deve ser escrito de forma clara, objetiva.

Todo e qualquer documento elaborado deve ter um responsável direto que responda por ele e principalmente o mantenha atualizado.

Os documentos da política de segurança devem atingir o nível de segurança adequado aos bem que se deseje proteger, bem como deve ser flexível o suficiente para se adaptar às mudanças tecnológicas e de negócios/legislação que ocorrem frequentemente nas empresas.

Muitas vezes as organizações criam documentos que são impossíveis de serem cumpridos e por isso os documentos devem ser factíveis, ou seja, devem ter a possibilidade de serem feitos, pois senão acabarão no esquecimento.

Os documentos devem prever as ações de segurança que serão realizadas, bem como quem as realizará. Eles também devem prever as ações e as punições claras que serão aplicadas para quem deixar de cumprir algum item ou procedimento de segurança.

Sucesso e fracasso da implementação

Muitas vezes a política de segurança não atinge o seu objetivo, pois alguns itens deixaram de ser observados e com o passar do tempo comprometeram todas as atividades do projeto. Itens estes como a inexistência de uma pessoa graduada dentro da organização para dar o aval nas ações, punições e orientações que a política indicou.

Outro fator importante que acaba por comprometer a política é que a própria alta direção da empresa não esteja integralmente comprometida com a política, não dando dessa forma apoio aos profissionais responsáveis pela implantação.

Muitos dos problemas de segurança ocorrem por causa da inexistência de treinamento para os profissionais envolvidos. A falta de comprometimento por parte dos funcionários e colaboradores da organização também interfere no sucesso da implantação da política. A inexistência de um orçamento próprio para as ações de segurança também acaba por dificultar a implantação da politica, pois geralmente o orçamento é destinado para as operações específicas dos negócios da organização, e não para a aquisição de componentes de segurança.

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento.
Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

A seguir, preencha a(s) lacuna(s) com a(s) palavra(s) adequada(s) às afirmações.

Referências

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de Segurança da Informação*: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. *Gerenciamento de Serviços de TI na Prática*: uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de. *Segurança de Redes em Ambientes Cooperativos*. São Paulo: Berkeley, 2002.

SÊMOLA, Marcos. *Gestão da Segurança da Informação*: uma visão executiva. Rio de Janeiro: Elsevier, 2003.

WADLOW, Thomas A. Segurança de Redes: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2001