Capítulo

5

5 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

NESTE CAPÍTULO VEREMOS COMO CRIAR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

OBJETIVO

Escrever uma política de segurança da informação envolve comprometimento de diversas áreas de interesse e deve ser abraçada por todos, desde a direção da organização até cada um dos funcionários, clientes e fornecedores com acesso ao sistema de informação, ou que possam de alguma forma comprometer o ativo protegido.

O documento de política de segurança da informação deve ser elaborado de forma a servir como uma regra a ser seguida. Constantemente exigirá atualizações que reflitam as necessidades do negócio e a realidade da organização.

Neste capítulo veremos como criar e organizar uma política de segurança da informação nas organizações.

Ao final deste capítulo você estará apto a:

- ❒ Conceituar o que é uma política de segurança da informação;
- ❒ Fazer uma análise crítica da política de segurança da informação;
- ❒ Estabelecer uma criteriosa política de segurança da informação conforme os requisitos do negócio;
- ❒ Entender os documentos requeridos para a implantação e divulgação da política de segurança da informação;

- "*Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes*"

- É preferível uma política mal escrita do que nenhuma política.

Segundo a norma ABNT NBR ISO/IEC 17799:2005, uma política de segurança da informação visa "*Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes*", ou seja, ela propõe uma política que sistematize um processo a fim de minimizar as preocupações da direção com a segurança de seus ativos.

Escrever uma política é uma tarefa muitas vezes difícil e deve contar com o envolvimento de várias pessoas, de vários departamentos. Isso não deve ser desanimador e não se deve procrastinar o início dos trabalhos, haja vista a fragilidade a que o negócio pode estar exposto.

Se necessário, para implementar e manter esta política, deverá ser utilizada consultoria especializada, com conhecimento nos diversos aspectos da segurança dos bens de informação e das tecnologias que os apóiam.

Possuir uma política de segurança da informação na organização é importantíssimo para o sucesso dos negócios. É preferível uma política mal escrita do que nenhuma política.

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política e segurança
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. Refaça o processo

O primeiro passo para a criação de uma política de segurança da informação é ter alguém responsável por ela. Deve haver uma área responsável pela política de segurança da informação, que se incumbirá de sua criação, implantação, revisão, atualização e designação de funções. Nessa área deve ser escolhido um gestor responsável pela análise e manutenção da política. Para garantir a aplicação eficaz da política, o ideal é que o alto escalão, como diretoria, gerentes e supervisores façam parte dessa área, além de usuários, desenvolvedores, auditores, especialistas em questões legais, recursos humanos, TI e gestão de riscos.

Thomas A. Wadlow [10], propõe um processo para se estabelecer uma política que prevê a possibilidade de implantação imediata na organização sem muita delonga. A princípio o processo não requer o engajamento imediato da direção, que, aos poucos deverá ser incluída. Essa abordagem, leva em consideração a experiência na implantação do processo da política.

Como a norma é explícita no comprometimento da direção, neste curso adotaremos uma abordagem adaptada de Thomas A. Wadlow como o ponto de partida para a tarefa de implantação da política de segurança da informação. Vamos supor que você leitor foi escolhido como o responsável pela implantação da política de segurança da informação. Siga os passos abaixo para dar início aos trabalhos o quanto antes:

Criando uma política de segurança da informação

1. ***Escreva o esboço do documento***
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política e segurança
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. Refaça o processo

1. ***Escreva o esboço do documento da política de segurança para sua organização***. Esse documento deve ser genérico, possuir apenas suas idéias principais, sem preocupação com precisão. Não deverá possuir mais do que 5 páginas. Escreva também uma justificativa para sua implantação, sempre com o foco nos negócios e riscos a que a organização está sujeita caso não se implante a política de segurança da informação.

   Procure fazer um documento com foco nos processos de negócio, e não na tecnologia. Para obter o apoio da diretoria é necessário que se mostre qual operação está em risco.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. ***Apresente seu esboço para a diretoria***
3. Crie um comitê de política e segurança
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. Refaça o processo

2. ***Apresente seu esboço para a diretoria***. O objetivo é angariar a confiança no projeto e o engajamento da direção. Uma vez que ela esteja convencida da importância da política, você terá carta branca para a o início da implantação.

   O apoio da diretoria é fundamental para o sucesso da política de segurança. Em algumas situações somente com o apoio da diretoria será possível aplicar as políticas criadas.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. ***Crie um comitê de política e segurança***
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. Refaça o processo

3. ***Crie um comitê de política de segurança***. Esse comitê deverá ser formado por pessoas interessadas na criação da política de segurança e devem ser de setores distintos na organização. Com base em seu documento, a função do comitê será:

    a. escrever as regras para a política;
    b. definir atribuições;
    c. detalhar os procedimentos bem como as penas para violações da mesma;
    d. aprovar as normas estipuladas e alterações propostas.

    O comitê terá a função legisladora do processo. Porém, continua sendo sua a responsabilidade pela aplicação da política. O comitê deverá se reunir pelo menos uma vez a cada três meses e, extraordinariamente, se houver necessidade. A reunião tem o objetivo de avaliar e aprimorar a política de segurança, os incidentes ocorridos e as ações tomadas para correção.

    O documento criado por você, juntamente com o comitê, deverá ter uma linguagem simples a fim de que todos os usuários a entendam e possam aplicá-la com facilidade. Assim, para que a política de segurança da informação seja eficaz, o documento será na verdade, um conjunto de políticas inter-relacionadas. A partir deste momento, você já terá em mãos um documento oficial que deverá ser aceito e aprovado pela direção. Dependendo da natureza da organização esse documento tende a ser muito extenso com dezenas ou centenas de páginas.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política e segurança
4. ***Divulgue a política***
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. Refaça o processo

4. ***Divulgue a política de segurança da informação***. A política deve ser de conhecimento de todos e compreensível para todos que interagem com a organização, usuários internos e externos.

   Deve sempre estar nas mãos de quem vai utilizá-la. Porém, de nada vale colocar o documento inteiro nas mãos de quem vai utilizar apenas uma parte.

   Se um funcionário da limpeza precisa saber como limpar um determinado equipamento preservando a integridade física do mesmo. Caso veja, por exemplo, um fio desencapado, deve saber a quem avisar para solucionar o incidente. Um funcionário da contabilidade precisa saber sua senha para acessar o banco de dados pertinente ao seu setor. Precisa saber também a quem recorrer caso precise acessar dados antigos, armazenados em fita, e que precisam ser restaurados. Porém, não precisa saber os detalhes de como são realizados os backups.

   A divulgação eficaz é aquela que atinge a pessoa certa com a informação que ela precisa saber. Ela não precisa ler toda a política de segurança, mas a parte que lhe interessa. Essa divulgação segmentada é fator imprescindível para o sucesso da empreitada. É claro que isso não exclui a necessidade de divulgação de todo o documento caso alguém se interesse em lê-lo.

   Uma forma prática de divulgação é a criação de um Web site na intranet da empresa. Nele todas as informações sobre a política devem ser bem redigidas e separadas em seções, facilitando o acesso a políticas gerais às quais todos devem obedecer e a políticas específicas para cada setor. Este site servirá de

repositório de tudo o que for estabelecido na política e servirá também para coletar sugestões.

Outras formas de divulgação também poderão ser usadas como um fórum, e-mails periódicos, ferramentas colaborativas de troca de informação.

Se a política de segurança da informação for divulgada fora da organização, tome o cuidado de não revelar informações sensíveis. Lembre-se de classificar as informações sigilosas para acesso apenas a pessoas específicas.

5. ***Trate a política e as emendas como regras absolutas com força de lei***. Uma vez que a política já é do conhecimento de todos, não pode haver violações da mesma. Caso isso ocorra, devem ser previstos procedimentos que vão de advertências a punições. As violações devem ser analisadas em suas causas, conseqüências e circunstâncias, a fim de sejam tomadas medidas preventivas e corretivas que alterem a política para evitar nova situação de vulnerabilidade. Lembre-se que tudo deve ser documentado.

   Neste ponto, o apoio da diretoria tratado nos itens 1 e 2 é fundamental para que se possa cumprir as punições previstas na política. Caso estas deixem de ser cumpridas a política perde sua credibilidade e força junto aos demais colaboradores da organização.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política e segurança
4. Divulgue a política
5. Leve a política a sério
6. ***Acate sugestões***
7. Reavalie periodicamente
8. Refaça o processo

6. ***Sugestões são sempre bem-vindas***. Incentive que os colaboradores proponham sugestões de melhorias. Todas devem ser levadas em consideração. As pessoas que estão na rotina do trabalho, são as que mais estão aptas a levantar problemas de segurança na respectiva área, ou mesmo provocá-los.

   Algumas sugestões podem mostrar também que a política possui um rigor exagerado em determinado item, o que pode tornar seu cumprimento demasiadamente oneroso. Neste caso devemos analisar as críticas e estudar uma forma alterá-las ou criar tratamento de exceções para garantir o cumprimento das normas.

   Facilite o canal de comunicação para que as sugestões cheguem ao comitê. As sugestões pertinentes deverão virar emendas à política.

Criando uma política de segurança da informação

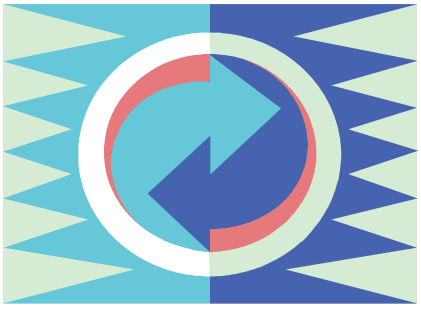
1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política e segurança
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. ***Reavalie periodicamente***
8. Refaça o processo

7. ***Realize reuniões periódicas para consolidar a política e as emendas***. Essas reuniões deverão ocorrer pelo menos uma vez ao ano. Deverão participar todo o comitê de política de segurança, a direção, e os responsáveis com funções delegadas. O objetivo é realizar uma análise crítica da política de segurança vigente, das emendas e dos incidentes relatados. Esta avaliação poderá gerar um documento atualizado que inclua todas as alterações.

   Neste ponto devemos considerar as sugestões levantadas no item 6 e todas as alterações do ambiente desde a ultima reunião, para que sirvam como base para o processo de revisão.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política e segurança
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. ***Refaça o processo***



8. ***Refaça o processo***. A nova declaração gerada no passo 7 deverá passar por todo o processo novamente, a fim de que entre em vigor e seja do conhecimento de todos.

Esses passos não são fáceis e envolvem muito trabalho, porém criam uma metodologia por etapas que uma vez seguida levará ao sucesso da criação da política de segurança da informação.

O conteúdo do documento elaborado para a política de segurança da informação varia de uma organização para outra, em função de sua maturidade, disponibilidade de recursos, necessidades do negócio, área de atuação, etc... Deve ser simples, objetivo e compreensível para todos.

O Documento consta normalmente de:

a. ***Definição de segurança da informação, metas, escopo e importância da segurança da informação como mecanismo que possibilita o compartilhamento da informação***. Esse item é um texto explicativo do que é segurança da informação, como o texto apresentado no capítulo 3, subitens "Conceitos básicos de Segurança da Informação" e "Objetivos da Segurança da Informação".

b. ***Declaração do comprometimento da direção apoiando metas e princípios***. Mais uma vez, uma etapa bem simples de ser executada. Pode ser apenas uma frase assinada pela direção, como por exemplo:

   "A Diretoria da XYZ S/A declara-se comprometida em proteger todos os ativos ligados à Tecnologia da Informação, apoiando as metas e princípios da segurança da informação estabelecidas neste documento, a fim de garantir a confiabilidade, disponibilidade e integridade da informação, alinhada com as estratégias do negócio".

O importante nesse item é que a assinatura da direção realmente expresse a vontade e engajamento do alto escalão da empresa, apoiando ativamente as ações a serem implantadas e definindo atribuições de forma explícita.

c. ***Estrutura para estabelecer objetivos de controles e controles, incluindo estrutura e análise/avaliação e gerenciamento de risco.*** Veja o capítulo 4.

d. ***Princípios de conformidade com a legislação e regulamentos contratuais***. Aqui deve ser avaliada a questão legal do negócio, suas conformidades com a legislação vigente e com regulamentos e contratos. As cláusulas do documento de política de segurança da informação devem estar em conformidade com essa avaliação. Por exemplo, caso a organização seja uma entidade pública, ela está obrigada a obedecer uma política de segurança conforme o decreto presidencial nº 3.505.

e. ***Plano de treinamento em segurança da informação***. É muito importante que todos os envolvidos com a segurança da informação, tenham não só acesso ao documento de política, como também sejam instruídos no processo de implantação e uso da política. Tendo conhecimento e formação adequada, a eficácia do plano de segurança terá mais chances de sucesso. Além disso, todos passam a ser co-responsáveis pelo processo uma vez que não podem alegar desconhecimento do mesmo. O treinamento poderá ser feito, por exemplo, através de seminários programados, distribuições de cartilhas com informações sobre a segurança da informação, e-mails regulares com dicas sobre o assunto e site de divulgação da política.

f. ***Plano para gestão de continuidade do negócio***. É um conjunto de estratégias e procedimentos que visam garantir que não haverá interrupção das atividades do negócio, além de proteger os processos críticos no caso de alguma falha. É um conjunto de medidas que combinam ações preventivas e de recuperação.

g. ***Conseqüência das violações na política de segurança***. É necessário que todos saibam das conseqüências da violação na política. Essas conseqüências passam por punições que devem ser explicitadas no documento. O responsável pela aplicação da política deve estar bem preparado para a eventualidade de ter que, por exemplo, solicitar a demissão de um bom funcionário que tenha violado a política. Isso pode ser constrangedor, mas necessário. Por isso, explicite e divulgue bem essa parte para evitar desculpas de desconhecimento das normas.