Segurança da Informação

Aula8 _ Políticas de Segurança

Curso de Ciência da Computação

Prof. Dr. Rodrigo Xavier de Almeida Leão

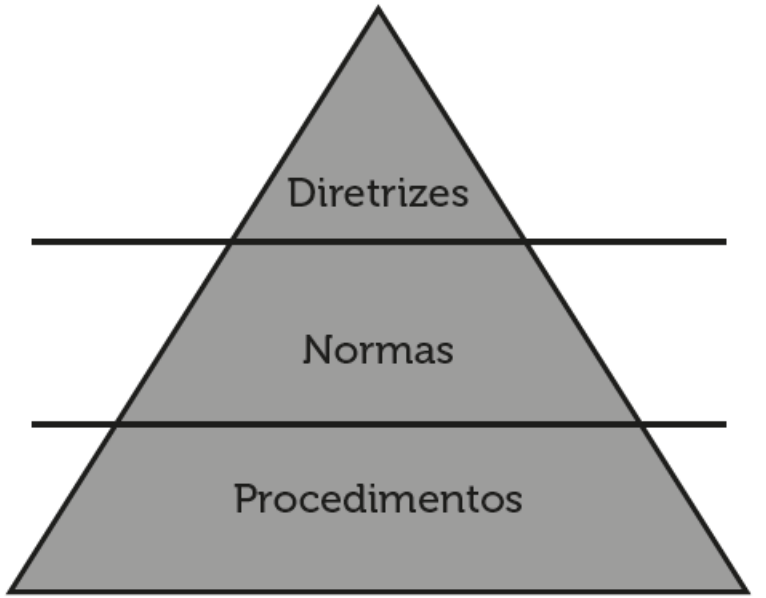
Como já vimos neste curso, as informações podem existir em meio digital, em meio físico ou na cabeça das pessoas. A segurança da informação deve buscar a manutenção da confidencialidade, da integridade e da disponibilidade dessas informações, para tanto, os controles de segurança, como *firewalls*, antivírus ou criptografia podem ser aplicados para proteger informações que existem em meios digitais (NAKAMURA; GEUS, 2007; ISO 27001, 2013; ISO 27002, 2013).

Já para as informações que existem em meios físicos, como em papéis, e também para as informações que estão na cabeça das pessoas, é necessária uma política de segurança. Mesmo os controles tecnológicos dependem da política de segurança, que estabelece as diretrizes para que a proteção seja efetiva (NAKAMURA; GEUS, 2007; PCI, 2013; ISO 27001, 2013; ISO 27002, 2013).

Assim, a política de segurança possui um dos papéis mais importantes em organizações de qualquer natureza. Segundo PCI (2013, p. 111), em seu Requisito 12, temos: "Uma política de segurança sólida determina o tom da segurança para toda a empresa e informa aos funcionários o que é esperado deles". Além disso, a norma ainda diz: "Todos os funcionários devem estar cientes da confidencialidade dos dados e de suas responsabilidades para protegê-los". O PCI DSS (*Payment Card Industry Data Security Standard*), padrão para a segurança de dados da indústria de cartões, adotado em todo o mundo, torna claro um dos principais conceitos que uma política de segurança deve seguir: de que ela existe para direcionar a segurança da informação de uma empresa, sendo necessário que todos colaboradores tenham conhecimento sobre ela e cumpram o que nela está estabelecido.

A política de segurança é composta por um conjunto de documentos ou capítulos que devem ser lidos, compreendidos e seguidos pelos respectivos responsáveis. A política em si, que possui as diretrizes gerais para a segurança da informação na organização, deve ser acessada e seguida por todos. Além disso, há as normas. Já os processos e procedimentos específicos, como o de desenvolvimento de software, ou o de administração de sistemas, por exemplo, devem ser seguidos pelos respectivos responsáveis, não sendo necessário, por exemplo, que o administrador de *firewall* tenha acesso aos processos e procedimentos de gestão de identidades (NAKAMURA; GEUS, 2007; PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013).

Estrutura de uma política de segurança



A política de segurança é um conjunto de documentos que devem ser destinados ao público correto para ser efetiva. Assim, diretrizes são para o público em geral, enquanto processos e procedimentos são específicos, como no caso do administrador do servidor de arquivos, que deve seguir o procedimento de configuração segura e rastreabilidade do serviço, por exemplo.

Como tornar conhecida uma política de segurança

Uma política de segurança só possui utilidade se for conhecida de seus funcionários. Há três estratégias básicas para que todos da empresa tenham conhecimento da política de segurança (NAKAMURA; GEUS, 2007; PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013):

1. Termo assinado de que o funcionário leu a política de segurança e que se compromete a cumpri-la: as empresas adotam o termo normalmente em conjunto com a assinatura do contrato de trabalho, na admissão.

2. Campanhas e tecnologias: as empresas podem criar quadros para enfatizar a política de segurança espalhadas em pontos estratégicos da empresa. Além disso, tecnologias como protetores de tela de computadores ou mensagens direcionadas também ajudam na disseminação da política de segurança na empresa. Outra ação importante é a realização de campanhas de conscientização, como as relacionadas a senhas ou ao acesso a sites duvidosos, por exemplo. Essas campanhas resultam em diminuição do número de incidentes, contribuindo para a segurança da organização.

3. Ser direta e objetiva: o documento deve ser simples de entender e direto nos seus objetivos, de modo que todos que o leiam percebam sua importância e o memorizem.

4. Treinamentos periódicos em segurança da informação: normas e procedimentos podem ser discutidos e trabalhados em grupos específicos, como o dos desenvolvedores de sistemas ou dos profissionais de suporte e TI. Outro treinamento mais geral pode ser feito para o público mais amplo.

O que direciona uma política de segurança

Cada organização deve ter a sua própria política de segurança, que deve ser desenvolvida de acordo com suas próprias características, linguajares e contextos específicos. Assim, os seguintes aspectos devem ser utilizados para a definição da política de segurança de uma organização (NAKAMURA; GEUS, 2007; PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013):

- Análise de riscos: os riscos de segurança da informação devem ser mapeados para direcionar as ações que devem constar na política de segurança.
- Estratégia e requisitos de negócios: diferentes negócios requerem diferentes níveis de segurança, que direcionam o conteúdo da política de segurança. Uma empresa que quer vender a imagem de privacidade, por exemplo, direcionará a política de segurança para esses aspectos específicos.
- Requisitos legais: alguns setores possuem obrigações legais a serem cumpridas com relação à segurança da informação, que refletem diretamente na política de segurança.

Um exemplo de requisito legal é a Resolução nº 3.380, do Banco Central do Brasil (BACEN, 2006), que estabelece a necessidade de gerenciamento de risco operacional, levando à necessidade de controles de segurança da informação como o plano de continuidade de negócios, que atua na disponibilidade.

BANCO CENTRAL DO BRASIL. **Resolução nº 3.380, de 29 de junho de 2006**. Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional. Disponível em <http://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3380_v2_L.pdf>. Acesso em: 29 ago. 2016.

Cultura em segurança da informação

Um dos principais fatores que resulta em proteção concreta da organização, em conjunto com uma política de segurança efetiva, é a cultura em segurança da informação (NAKAMURA; GEUS, 2007; PCI, 2013; MONTEIRO, 2009; ISO 27001, 2013; ISO 27002, 2013).

Assimile

A segurança da informação só é possível se todos da organização seguirem os mesmos princípios e realizarem suas tarefas do dia a dia com base em preocupações comuns de manutenção de confidencialidade, integridade e disponibilidade da informação.

Em cultura de segurança da informação, a percepção de todos é fundamental. Caso o funcionário de uma organização tenha a percepção de que o presidente é de fato zeloso quanto à proteção da informação, naturalmente ele irá também agir com cuidado para proteger as informações.

A segurança da informação, assim, deve começar pelo topo, em uma abordagem top-*down*, que auxilia na construção de uma cultura forte em segurança da informação.

A análise de riscos irá direcionar os principais controles de segurança necessários, que podem ser baseados em normas como a NBR ISO/IEC 27002, que define controles de segurança da informação.

A gestão de segurança da informação, definida na norma NBR ISO/IEC 27001, também indica caminhos para o desenvolvimento de uma política de segurança da informação, incluindo outros aspectos para a proteção efetiva da organização.

Algumas perguntas que a política de segurança deve responder são:

- Os usuários sabem em quais links não devem clicar?
- Os funcionários da empresa sabem o que devem publicar em redes sociais sobre a empresa?
- Há preocupações sobre vazamento durante as discussões de novos produtos ou serviços?
- Quais são as regras para uso de dispositivos móveis?

Prof. Dr. Rodrigo Xavier de Almeida Leão

Prof. Dr. Rodrigo Xavier de Almeida Leão