SEGURANÇA DA INFORMAÇÃO

Prof. Luís Gonzaga de Paulo

TEMA 1 – SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Um gestor da área da tecnologia da informação e das comunicações – TIC deve garantir que os sistemas da organização sejam confiáveis e seguros. Para tanto, esse gestor deve se responsabilizar por prover os serviços demandados pelos usuários desses sistemas e principalmente se antecipar aos problemas, identificando e gerenciando as ameaças, de modo que seja mínima a possibilidade de um risco vir a transformar-se em um incidente.

Uma boa maneira de atingir esses objetivos é fazer uma profunda reflexão sobre o ambiente e o momento da organização no que tange às TICs, partindo de questões elementares, tais como:

- Por que os nossos sistemas de informação são vulneráveis a problemas de destruição, erro, abuso e má qualidade?
- Quais tipos de controles estão disponíveis para nossos sistemas de informação?
- Quais medidas especiais devem ser adotadas para garantir a confiabilidade, a disponibilidade e a segurança dos processos de negócios dependentes das informações digitais, incluído o comércio eletrônico?
- Quais são as técnicas de garantia de qualidade do *software* mais importantes para nossas demandas?
- Qual importância estamos dando à auditoria dos sistemas de informação e à salvaguarda da qualidade dos dados?

As respostas a essas questões são uma boa premissa para a administração da segurança dos sistemas de informação da organização. Em conjunto com os demais instrumentos já estudados, dos quais se pode fazer uso na formação de um arsenal amplo e efetivo, podem fazer a diferença no equilíbrio entre controle excessivo ou nenhum controle, e na garantia de uma adequação da segurança dos sistemas aos níveis requeridos pela organização.

1.1 Programa de segurança

O primeiro passo para a gestão da segurança de sistemas é elaborar e colocar em prática um programa de gerenciamento da segurança da informação. Profissionais da área de TI, de perfil mais técnico, geralmente argumentam que primeiro deve-se obter algum conhecimento de segurança que habilite gestores e profissionais da TIC para as discussões sobre segurança. Se esse pessoal não

tem um conhecimento mínimo, talvez a organização deva procurar orientação de alguém capacitado antes mesmo de começar a discutir o gerenciamento e os objetivos do programa de segurança.

Os objetivos do Programa de Segurança são notórios:

- Proteger a organização e seus ativos, gerenciar os riscos, fornecer a orientação para as atividades de segurança por meio do enquadramento de políticas, procedimentos, padrões, diretrizes e linhas de base de segurança da informação;
- Estabelecer a classificação de informação;
- Cuidar da organização dos processos de segurança e promover a educação para a segurança

O programa também deve considerar as responsabilidades de gerenciamento de segurança, que incluem, mas não se limitam à:

- Determinação de objetivos, escopo, políticas, e todas as demais atividades que, espera-se, sejam realizadas a partir de um programa de segurança;
- Avaliação dos objetivos de negócios, riscos de segurança, produtividade do usuário e funcionalidades requeridas;
- Definição das etapas para garantir que todos os itens sejam considerados e abordados adequadamente.

As possíveis abordagens para a efetivação de um programa de segurança incluem duas formas: a abordagem *top-down* (de cima para baixo), na qual a iniciação, o suporte e a direção vêm da alta gerência e passam pela gerência intermediária e, depois, pelos membros da equipe. Essa abordagem é tratada como a melhor, mas exige cuidado, pois pode gerar comportamentos negativos com base em “O que recebo a mais por isso?” ou “Devo saber muito mais do que os outros, então estou certo”. Porém essa abordagem garante que a gerência sênior, que em suma é o responsável final pela proteção, esteja conduzindo o programa.

Já na abordagem *bottom-up* (de baixo para cima), a equipe operacional apresenta um controle de segurança ou um programa, mesmo sem o suporte adequado da direção ou gerência. Muitas vezes é considerada menos eficaz e condenada a falhar pelo mesmo motivo comportamental anterior, com base no “Eu pago mais por isso, preciso saber mais sobre tudo”.

De toda forma, ou qualquer que seja a abordagem, é consenso que a

comunicação efetiva é essencial, e que os processos de segurança da informação devem ser respaldados por um programa de segurança da informação formal e aprovado pela alta direção.

1.2 Controles de segurança da informação

Para a efetividade do programa de segurança são exigidas medidas de ordem prática que possam ser planejadas, executadas, monitoradas e aprimoradas. Essas medidas compõem o rol dos *controles de segurança*, entre os quais temos:

- Os *controles administrativos*, que incluem: desenvolver e publicar políticas, normas, procedimentos e diretrizes; realizar adequadamente a gestão de pessoal, os treinamentos de conscientização de segurança e implementar procedimentos de controle de mudanças.
- Os *controles técnicos (*ou *lógicos),* que incluem: implementar e manter os mecanismos de controle de acesso, as senhas e o gerenciamento de recursos; prover os métodos de identificação e autenticação, os dispositivos de segurança e cuidar da configuração da infraestrutura.
- Os *controles físicos*, que incluem: controlar o acesso individual nas instalações e nas diferentes áreas da organização; controlar o tráfego de dados, os programas e sistemas, e o acesso à mídias removíveis e a serviços de acesso a dados; proteger o perímetro das instalações, providenciar o monitoramento contra intrusão e cuidar dos controles ambientais.

TEMA 2 – GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

A governança é um conjunto de responsabilidades e práticas exercidas pela administração da organização com o objetivo de fornecer direcionamento estratégico, garantir que os objetivos sejam alcançados, verificar se os riscos são gerenciados de forma adequada e verificar se os recursos da organização são utilizados com responsabilidade, incluindo-se aí os sistemas de informação. A *governança da segurança da informação* (*Information Security Governance* – ISG) é um subconjunto da governança corporativa voltada para os sistemas de segurança da informação, seu desempenho e o gerenciamento de risco.

A ISG emprega um conjunto de medidas, entre as quais as políticas de

segurança, os procedimentos, os padrões, as diretrizes e linhas de base para o direcionamento das ações do programa de segurança e para a avaliação do estado geral da segurança da informação, além de obter medidas e relatórios que permitam compartilhar esse estado com os parceiros de negócio, com as entidades civis, a comunidade e o governo.

2.1 A política de segurança da informação

Uma política de segurança é uma declaração geral comumente produzida pela alta gerência ou por um comitê especificamente constituído para isso, que dita qual função a segurança desempenha na organização. Uma política bem projetada aborda os seguintes aspectos:

- *O que está sendo protegido*, sendo normalmente um ativo da organização;
- *Quem deve cumprir a política*, normalmente pessoas – funcionários, terceiros ou parceiros de negócio;
- *Qual é e onde está a vulnerabilidade, ameaça ou risco*, geralmente uma questão ligada às características da segurança da informação (CID) ou à responsabilidade individual ou coletiva.

Essas políticas podem ser apresentadas de diversos modos, porém os principais utilizados são os seguintes:

- **Regulamento**: um tipo de política que garante que a organização siga os padrões definidos por regulamentações específicas do setor. Esse tipo de política é muito detalhado e específico para um tipo de indústria. Isso é usado em instituições financeiras, instituições de saúde, serviços públicos e outros setores regulamentados pelo governo. Um exemplo é a PCI-DSS, voltada para a indústria de cartões de pagamento.
- **Recomendação**: é um tipo de política que recomenda que os funcionários considerem quais tipos de comportamentos e atividades devem e não devem ocorrer dentro da organização. Também descreve possíveis consequências para os funcionários que não cumprirem os comportamentos e atividades estabelecidos. Esse tipo de política pode ser usado para descrever como lidar com informações pessoais, médicas, transações financeiras ou processar informações confidenciais.
- **Informativo**: esse tipo de política informa as pessoas sobre determinados tópicos. Não é uma política exequível, mas sim voltada para ensinar e

orientar pessoas sobre questões específicas relevantes para a empresa. Pode explicar como a organização interage com os parceiros, os objetivos e a missão da empresa e apresentar uma estrutura geral de relatórios e controles usados em diferentes situações.

Já no que se refere à abrangência, a política de segurança da informação pode atender à necessidade organizacional, a um problema ou situação específica ou a um sistema específico. Na *política organizacional*, a gerência estabelece como um programa de segurança será estabelecido, estabelece as metas do programa, atribui responsabilidades, mostra o valor estratégico e tático da segurança e descreve como a execução deve ocorrer, fornecendo escopo e direção para todas as futuras atividades de segurança dentro da organização.

Essa política deve abordar leis relativas, regulamentos e questões de responsabilidade e como eles devem ser satisfeitos. Também descreve a quantidade de risco que a gerência sênior está disposta a aceitar. São características típicas dessa política:

- Os objetivos de negócios devem orientar a criação, implementação e fiscalização da política. A política não deve ditar os objetivos de negócios;
- Deve ser um documento de fácil compreensão, que é usado como um ponto de referência para todos os funcionários e para o gerenciamento da segurança da informação;
- Deve ser desenvolvida e usada para integrar a segurança a todas as funções e processos de negócios;
- Deve derivar e apoiar toda a legislação e regulamentação aplicável à organização;
- Deve ser revisada e modificada à medida que a organização muda, como a adoção de um novo modelo de negócios, a fusão com outras organizações ou a mudança de propriedade.

Cada iteração da política deve ser datada e mantida sob controle de versão. As unidades e indivíduos que são regidos pela política devem ter acesso às partes aplicáveis e não se espera que tenham que ler todo o material político para encontrar orientação e respostas.

A *política específica de um problema* aborda problemas de segurança específicos que a gerência sente que precisam de explicações e atenção mais detalhadas, para garantir que uma estrutura abrangente seja construída, e que

todos os envolvidos entendam como devem cumprir esses problemas de segurança. Por exemplo: uma política de *e-mail* pode declarar que o gerenciamento pode ler as mensagens de qualquer colaborador que use o *e-mail* corporativo, mas não os de contas pessoais.

A *política específica de um sistema* apresenta as decisões do gerenciamento específicas ao uso dos equipamentos, redes, sistemas, aplicativos e dados da organização. Esse tipo de política pode fornecer uma lista de *softwares* aprovados, que contém uma lista de aplicativos que podem ser instalados em estações de trabalho individuais. Por exemplo: esta política pode descrever como os bancos de dados devem ser usados e protegidos, como os computadores devem ser bloqueados e como os firewalls, IDSs e *scanners* devem ser empregados.

2.2 Padrões e normas

Os padrões referem-se a atividades, ações, regras ou regulamentos obrigatórios, geralmente vinculados às entidades ou órgãos de fiscalização e controle. As normas podem dar a uma política seu apoio e reforço na direção. Os padrões podem ser internos ou externos e obrigatórios (leis e regulamentos governamentais).

2.3 Procedimentos

Procedimentos são ações detalhadas passo a passo que devem ser executados para atingir um determinado objetivo. Por exemplo: podemos criar procedimentos sobre como instalar sistemas operacionais, configurar mecanismos de segurança, implementar listas de controle de acesso, configurar novas contas de usuários, atribuir privilégios de computador, atividades de auditoria, destruir material, relatar incidentes e muito mais.

Os procedimentos são considerados o nível mais baixo na cadeia de políticas porque estão mais próximos dos equipamentos, sistemas, aplicativos e usuários (em comparação com as políticas) e fornecem etapas detalhadas para problemas de configuração e instalação. Procedimentos explicitam como a política, os padrões e as diretrizes serão realmente implementados em um ambiente operacional.

Se uma política declarar que todos os indivíduos que acessam informações

confidenciais devem ser devidamente autenticados, os procedimentos de suporte explicarão as etapas para que isso aconteça definindo os critérios de acesso para autorização, como os mecanismos de controle de acesso são implementados e configurados e como as atividades de acesso são auditadas.

2.4 Linhas de base

Uma linha de base (*base line*) se refere a um ponto no tempo que é usado como uma comparação para futuras alterações. Uma vez que os riscos tenham sido mitigados e a segurança implementada, uma linha de base é formalmente revisada e acordada, de modo que todas as posteriores comparações e desenvolvimento sejam comparados a ela. Uma linha de base resulta em um ponto de referência consistente.

As linhas de base também são usadas para definir o nível mínimo de proteção necessário. Em segurança, linhas de base específicas podem ser definidas por tipo de sistema, o que indica as configurações necessárias e o nível de proteção que está sendo fornecido.

2.5 Diretrizes

Diretrizes são as ações recomendadas e os guias operacionais para usuários, equipes de TI, equipes de operações e outros quando um padrão específico não se aplica. As diretrizes podem lidar com as metodologias de tecnologia, pessoal ou segurança física.

2.6 Integração

Uma política pode afirmar que o acesso a dados confidenciais deve ser auditado. Uma diretriz de apoio poderia explicar ainda que as auditorias devem conter informações suficientes para permitir a reconciliação com as revisões anteriores. Os procedimentos de suporte delineariam as etapas necessárias para configurar, implementar e manter esse tipo de auditoria. As políticas são estratégicas (longo prazo), enquanto os padrões, diretrizes e procedimentos são táticos (médio prazo).

TEMA 3 – COMPORTAMENTO ORGANIZACIONAL

O comportamento da organização é de fundamental importância para a segurança da informação, uma vez que o elo mais fraco em toda a cadeia da segurança é a pessoa, e são as pessoas que determinam e correspondem ao comportamento. E esse comportamento é resultado da cultura organizacional, mas também depende da estrutura da organização. Uma organização bem estruturada fortalece seu espírito organizacional, solidificando uma cultura e moldando o comportamento dos novos integrantes.

3.1 Melhores práticas

Para favorecer uma cultura organizacional são necessárias medidas e ações embasadas no conhecimento, na prática e no desenvolvimento – geralmente designadas como *best pratices* ou as melhores práticas: aquelas que partiram do estudo e do planejamento, e que, com sua aplicação, no decorrer do tempo foram sendo testadas e aprimoradas. Entre essas podemos citar:

- **Mudança de função** ou *Job Rotation* é uma abordagem para o desenvolvimento de gerenciamento, na qual um indivíduo é levado, por meio de um cronograma de tarefas, a atuar em novas áreas, de modo que possa conhecer melhor toda a operação da organização. Essa mudança também é praticada para permitir que funcionários qualificados obtenham mais *insights* sobre os processos da organização e aumentem a satisfação no trabalho por meio de novas oportunidades e desafios.
- **Separação de tarefas**: é o conceito de ter mais de uma pessoa necessária para concluir uma tarefa. É alternativamente chamado de *segregação de funções* ou, no âmbito político, *separação de poderes.* Em termos básicos, isso significa que os indivíduos não devem ter controles sobre duas ou mais fases de uma transação ou operação, de modo que uma fraude deliberada é mais difícil de ocorrer porque requer a participação de dois ou mais indivíduos ou partes. As funções críticas de negócios podem ser categorizadas em quatro tipos de funções: autorização, custódia, manutenção de registros e reconciliação. Em um sistema ideal, ninguém deve lidar com mais de um tipo de função.
- **Menor privilégio** (*Need to know*): o princípio do menor privilégio, também conhecido como *princípio de privilégio mínimo*, requer que, em uma

camada de abstração específica de um ambiente de computação, cada módulo (como um processo, um usuário ou um programa com base na camada que nós estamos considerando) deve ser capaz de acessar apenas as informações e recursos necessários para o seu propósito legítimo. Esse princípio é uma ferramenta de segurança útil, mas nunca foi bem-sucedido ao prover elevada segurança em sistemas críticos.

- **Férias obrigatórias**: um período de férias de uma a duas semanas é usado para auditar e verificar as tarefas e privilégios dos colaboradores. Isso geralmente resulta em fácil detecção de abuso, fraude ou negligência, e também reforça a verificação da aplicação das políticas e a verificação de conformidade.
- **Sensibilidade da posição de trabalho**: no caso das regras específicas aplicáveis a uma determinada função ou posto de trabalho, é necessária uma contínua avaliação tanto da adequação daquelas regras perante às mudanças conjunturais quanto às mudanças de pessoal, bem como a verificação do resultado da sua aplicação.

3.2 Funções e responsabilidades

As funções exercidas pelas pessoas na organização devem corresponder aos níveis de responsabilidades pela segurança da informação. A gerência sênior e outros níveis de gerenciamento entendem a visão da empresa, os objetivos do negócio e os objetivos. Os gerentes funcionais entendem como seus departamentos individuais funcionam, quais são os papéis que os indivíduos desempenham na empresa e como a segurança afeta diretamente o departamento. E os gerentes operacionais e demais colaboradores estão mais próximos das operações reais da empresa. Eles conhecem informações detalhadas sobre os requisitos técnicos e de procedimentos, os sistemas e como os sistemas são usados. Os funcionários dessas camadas entendem como os mecanismos de segurança se integram aos sistemas, como configurá-los e como afetam a produtividade diária. Cada uma dessas funções deve ocupar-se de papéis e de suas responsabilidades perante a segurança da informação, descritos a seguir.

3.2.1 Proprietário dos dados

O *Data Owner* geralmente é um membro da gerência, responsável por uma unidade de negócios específica e, em última análise, é responsável pela proteção e uso de um subconjunto específico de informações. O proprietário dos dados decide sobre a classificação dos dados pelos quais é responsável e altera essa classificação se as necessidades do negócio exigirem. Também é responsável por garantir que os controles de segurança necessários estejam em vigor, garantindo o uso de direitos de acesso adequados, definindo requisitos de segurança por requisitos de classificação e *backup*, aprovando atividades de divulgação e definindo critérios de acesso do usuário.

O proprietário dos dados aprova as solicitações de acesso ou pode optar por delegar essa função aos gerentes da unidade de negócios. E é o proprietário dos dados que lidará com as violações de segurança referentes aos dados que ele é responsável por proteger. O proprietário dos dados delega a responsabilidade da manutenção diária dos mecanismos de proteção de dados ao custodiante de dados.

3.2.2 Custodiante

O *Data Custodian*, guardião de dados ou custodiante de informações, é responsável por manter e proteger os dados. Essa função geralmente é preenchida pelo departamento de TI, e as tarefas incluem realizar *backups* regulares dos dados, validar periodicamente a integridade dos dados, restaurar dados da mídia de *backup*, reter registros de atividade e atender aos requisitos especificados na política de segurança da empresa, padrões e diretrizes relacionados à segurança da informação e proteção de dados.

3.2.3 Proprietário do sistema

O proprietário do sistema é responsável por um ou mais sistemas, cada um dos quais pode reter e processar dados pertencentes a diferentes proprietários de dados. Um proprietário de sistema é responsável por integrar considerações de segurança nas decisões de compra de aplicativos e sistemas e em projetos de desenvolvimento. O proprietário do sistema é responsável por garantir que a segurança adequada esteja sendo fornecida pelos controles necessários, pelo gerenciamento de senha, pelos controles de acesso remoto, pelas configurações

do sistema operacional e assim por diante. Essa função precisa garantir que os sistemas sejam avaliados adequadamente quanto às vulnerabilidades e relatar à equipe de resposta a incidentes e ao proprietário dos dados.

3.2.4 Administrador de segurança

As tarefas de um administrador de segurança são muitas e incluem a criação de novas contas de usuário do sistema, a implementação de novos *softwares* de segurança, o teste de *patches* e componentes de segurança e a emissão de novas senhas. A função de administrador de segurança precisa garantir que os direitos de acesso fornecidos aos usuários suportem as diretivas de políticas e de proprietários de dados.

3.2.5 Analista de segurança

Essa função se dá em um nível mais alto e mais estratégico do que as funções descritas anteriormente e ajuda a desenvolver políticas, padrões e diretrizes e define várias linhas de base. Enquanto as funções anteriores estão na lida diária e se concentram em suas partes e partes do programa de segurança, um analista de segurança ajuda a definir os elementos do programa de segurança e a garantir que os elementos estejam sendo executados e praticados adequadamente. Essa pessoa trabalha mais em um nível de *design* do que em um nível de implementação.

3.2.6 Proprietário da aplicação

Um proprietário de aplicativo – geralmente um gerente de unidade de negócios – é responsável por ditar quem pode ou não acessar seus aplicativos, como o *software* de contabilidade, o *software* para teste e desenvolvimento etc.

3.2.7 Supervisor

Essa função, também chamada de *gerenciador de usuários*, é responsável por todas as atividades do usuário e quaisquer ativos criados e pertencentes a esses usuários, como garantir que todos os funcionários entendam suas responsabilidades com relação à segurança, distribuindo as senhas iniciais, garantindo que as informações da conta dos funcionários estejam atualizadas e informando ao administrador de segurança quando um funcionário entra em férias

ou licença, quando é demitido, suspenso ou transferido.

3.2.8 Analista de controle de mudanças

O analista de controle de mudanças é responsável por aprovar ou rejeitar solicitações para fazer alterações na rede, nos sistemas ou no *software*. Essa função precisa garantir que a alteração não introduza nenhuma vulnerabilidade, que tenha sido testada adequadamente e que esteja adequadamente implementada. O analista de controle de alterações precisa entender como várias mudanças podem afetar a segurança, a interoperabilidade, o desempenho e a produtividade.

3.2.9 Analista de dados ou informações

O analista de dados ou de informações é responsável por garantir que os dados sejam armazenados de uma forma que faça mais sentido para a empresa e para os indivíduos que precisam acessar e trabalhar com eles. A função de analista de dados pode ser responsável por arquitetar um novo sistema que contenha informações da empresa ou a assessoria na compra de um produto que faça isso. O analista de dados trabalha com os proprietários de dados para ajudar a garantir que as estruturas configuradas coincidam e suportem os objetivos de negócios da empresa.

3.2.10 Proprietário do processo

A segurança deve ser considerada e tratada como apenas outro processo de negócios. O *process owner* ou proprietário do processo é responsável por definir, melhorar e monitorar adequadamente esses processos. Um proprietário de processo não está necessariamente vinculado a uma unidade de negócios ou aplicativo. Processos complexos envolvem muitas variáveis que podem abranger diferentes departamentos, tecnologias e tipos de dados.

3.2.11 Provedor de soluções

Esse papel é chamado quando uma empresa tem um problema ou exige que um processo seja aprimorado. Um provedor de soluções trabalha com os gerentes de unidades de negócios, proprietários de dados e gerenciamento sênior para desenvolver e implantar uma solução para reduzir os pontos problemáticos

da empresa.

3.2.12 Usuário

O usuário é qualquer pessoa que use os dados rotineiramente para tarefas relacionadas ao trabalho. O usuário deve ter o nível necessário de acesso aos dados para executar as tarefas dentro de sua posição e é responsável por seguir os procedimentos operacionais de segurança para garantir a confidencialidade, integridade e disponibilidade dos dados a outras pessoas.

3.2.13 Gerente de linha

É o responsável por explicar os requisitos de negócios aos fornecedores e analisar se o produto ou serviço é adequado para a empresa. É responsável também por garantir a conformidade com os contratos de licença, por traduzir os requisitos de negócios em objetivos e especificações para o desenvolvedor de um produto ou solução. Decide se sua empresa realmente precisa atualizar seus sistemas atuais. Essa função deve entender os impulsionadores de negócios, os processos de negócios e a tecnologia necessária para suportá-los.

O gerente de linha de produto avalia diferentes produtos no mercado, trabalha com fornecedores, compreende as diferentes opções que uma empresa pode ter e aconselha as unidades de negócios e gerenciamento sobre as soluções adequadas que são necessárias para atingir seus objetivos.

3.2.14 Diretor de segurança da informação

O CSO – *Chief Security Officer* é o responsável por comunicar riscos à gestão executiva, preparar e administrar o orçamento para atividades de segurança da informação, garantir o desenvolvimento de políticas, procedimentos, linhas de base, padrões e diretrizes, desenvolver e fornecer programa de conscientização sobre segurança. É necessário também que entenda os objetivos de negócios, mantenha consciência das ameaças e vulnerabilidades emergentes, avalie incidentes e respostas de segurança de modo que possa desenvolver o programa de conformidade de segurança, estabelecer métricas de segurança, participar de reuniões de gerenciamento e garantir o cumprimento dos regulamentos do governo. Deve também apoiar os auditores internos e externos e manter-se a par das tecnologias emergentes.

TEMA 4 – CONSCIENTIZAÇÃO, TREINAMENTO E EDUCAÇÃO

As diretrizes da gerência relativas à segurança são capturadas na política de segurança, e os padrões, procedimentos e diretrizes são desenvolvidos para dar suporte a essas diretivas. No entanto, essas diretivas não serão eficazes se ninguém as conhecer e souber como a empresa espera que elas sejam implementadas. Para que a segurança seja bem-sucedida e efetiva, a gerência sênior deve estar totalmente ciente da importância da segurança corporativa e da informação.

4.1 O programa de treinamento

Todos os funcionários devem entender o significado subjacente da segurança e os requisitos específicos relacionados à segurança aos quais devem atender. Os controles e procedimentos de um programa de segurança devem refletir a natureza dos dados que estão sendo processados. O programa de segurança deve ser desenvolvido de uma maneira que faça sentido para as diferentes culturas e ambientes.

O programa de segurança deve comunicar o que, como e o porquê da segurança para os colaboradores. O treinamento de conscientização de segurança deve ser abrangente, adaptado para grupos específicos e para toda a organização, com o objetivo de que cada funcionário compreenda a importância da segurança para a empresa como um todo e para cada indivíduo. As responsabilidades esperadas e os comportamentos aceitáveis precisam ser esclarecidos, e as penalidades por não conformidade, que podem variar de uma advertência até a demissão, precisam ser explicadas antes de serem aplicadas.

4.2 Os tipos de treinamento

Existem diferentes tipos de treinamentos de conscientização de segurança. Geralmente há pelo menos três públicos-alvo separados para um programa de conscientização de segurança: gerenciamento, equipe e técnicos. Cada tipo de treinamento de conscientização precisa ser direcionado para o público individual para garantir que cada grupo entenda suas responsabilidades e expectativas específicas.

Os membros da gerência se beneficiariam mais com uma orientação de conscientização de segurança curta e focada que discuta ativos corporativos e

ganhos e perdas financeiros relacionados à segurança. A gerência intermediária se beneficiaria de uma explicação mais detalhada das políticas, procedimentos, padrões e diretrizes e de como eles mapeiam os departamentos individuais pelos quais são responsáveis. Os gerentes de nível médio devem aprender por que seu suporte para seus departamentos específicos é essencial e qual é o nível de responsabilidade deles para garantir que os funcionários pratiquem atividades de computação seguras. Eles também devem mostrar como as consequências da não conformidade por parte de indivíduos que se reportam a elas podem afetar a empresa como um todo e como eles, como gerentes, podem ter que responder por tais indiscrições.

Os departamentos técnicos devem receber uma apresentação diferente que se alinhe mais às suas tarefas diárias. Eles devem receber um treinamento mais aprofundado para discutir configurações técnicas, tratamento de incidentes e indicações de diferentes tipos de comprometimento de segurança, para que possam ser devidamente reconhecidos.

Os funcionários não devem tentar combater um invasor ou tratar de atividades fraudulentas sozinhos. Ao invés disso, devem ser instruídos a relatar esses problemas à alta gerência, e a alta gerência deve determinar como lidar com a situação. A apresentação dada aos membros da equipe precisa demonstrar por que a segurança é importante para a empresa e para eles individualmente. Quanto melhor eles entenderem como atividades inseguras podem afetá-los negativamente, mais dispostos estarão em participar na prevenção de tais atividades.

Geralmente, é melhor que cada funcionário assine um documento indicando que ele ouviu e compreendeu todos os tópicos de segurança discutidos e compreende as consequências do não cumprimento. O treinamento de segurança deve ocorrer periodica e continuamente.

TEMA 5 – PRINCÍPIOS ÉTICOS

A ética é o campo de estudo preocupado com questões de valor, isto é, julgamentos sobre que tipo de comportamento humano é “bom” ou “ruim” em qualquer situação. Ética são os padrões, valores, moral, princípios etc. nos quais basear as decisões ou ações de alguém: muitas vezes não há uma resposta clara do tipo “certo” ou “errado”.

O termo *ética computacional* está aberto a interpretações amplas e

restritas. No lado mais restrito, a ética computacional pode ser entendida como o esforço de filósofos profissionais de aplicar teorias éticas tradicionais, como o utilitarismo, o kantismo ou a ética da virtude, às questões relativas ao uso da tecnologia da computação. No sentido lato, pode ser entendido como um padrão de prática profissional, códigos de conduta, aspectos do direito computacional, políticas públicas, ética corporativa – até mesmo certos tópicos em sociologia e psicologia da computação.

5.1 Código de ética profissional

Profissionais certificados – por exemplo, aqueles que detêm o CISSP (acrônimo de *Certifyed Information Systems Security Professional* ou Profissional de Segurança de Sistemas de Informação Certificado, uma certificação provida pelo ISC^2) – são mantidos moralmente, e às vezes legalmente, em um padrão mais elevado de comportamento ético. Ao promover o comportamento apropriado da computação dentro do setor e os limites de nossas fronteiras corporativas, os profissionais devem incorporar a ética em suas políticas organizacionais e programas de conscientização. Várias organizações abordaram a questão do comportamento ético por meio de diretrizes éticas, tais como:

- O CEI – Instituto de Ética em Computação;
- O IAB – Conselho de Atividades da Internet;
- A ICSA – International Computer Security Association;
- A ISSC – Associação de Segurança de Sistemas de Informação;
- O (ISC)^2 – Consórcio Internacional de Certificação de Segurança de Sistema de Informação

5.2 CEI – Instituto de Ética em Computação

O CEI apresenta o que denomina “Os dez mandamentos da ética computacional”:

I. Não usarás um computador para prejudicar outras pessoas;
II. Você não deve interferir no trabalho do computador de outras pessoas;
III. Você não deve bisbilhotar os arquivos de computador de outras pessoas;
IV. Não usarás um computador para roubar;
V. Não usarás um computador para dar falso testemunho;
VI. Você não deve copiar ou usar *software* proprietário pelo qual não pagou;

VII. Não usará recursos de computadores de outras pessoas sem autorização ou compensação adequada;

VIII. Você não deve se apropriar da produção intelectual de outras pessoas;

IX. Você deve pensar nas consequências sociais do programa que está escrevendo ou do sistema que está projetando;

X. Você sempre usará um computador de maneiras que garantam consideração e respeito por seus semelhantes.

5.3 IAB – Internet Architecture Board

O *Internet Architecture Board* – IAB é o comitê de coordenação para *design*, engenharia e gerenciamento da internet. É um comitê independente de pesquisadores e profissionais com interesse técnico na saúde e evolução da Internet. O IAB tem duas principais forças-tarefa subsidiárias: a Força-Tarefa de Engenharia da Internet (IETF) e a Força-Tarefa de Pesquisa na Internet (IRFT). O IAB emite declarações relacionadas à ética relacionadas ao uso da internet. Considera que a internet é um recurso que depende da disponibilidade e acessibilidade para ser útil a uma ampla gama de pessoas.

O IAB se preocupa principalmente com atos irresponsáveis na internet que possam ameaçar sua existência ou afetar negativamente os outros. Ele vê a internet como um grande presente e trabalha duro para protegê-la de todos os que dela dependem. O IAB vê o uso da internet como um privilégio, que deve ser tratado como tal e usado com respeito. O IAB considera os seguintes atos como um comportamento antiético e inaceitável:

- Propositadamente buscar obter acesso não autorizado aos recursos da internet;
- Interromper o uso pretendido da internet;
- Desperdiçar recursos (pessoas, capacidade e computadores) por meio de ações intencionais;
- Destruir a integridade das informações baseadas em computador;
- Comprometer a privacidade dos outros;
- Realizar experimentos em toda a internet de maneira negligente

5.4 O código de ética do $(ISC)^2$

Todos os profissionais de segurança de sistemas de informação

certificados pelo (ISC) reconhecem que essa certificação é um privilégio que deve ser obtido e mantido. Em apoio a esse princípio, todos os profissionais de segurança de sistemas de informação certificados (CISSPs) se comprometem a apoiar totalmente este código de ética. Os CISSPs que intencional ou conscientemente violem qualquer disposição do código estarão sujeitos a ação por um painel de revisão por pares, o que pode resultar na revogação da certificação. O Código de ética do ISC^2 tem o seguinte preâmbulo: “A segurança da comunidade, o dever para com os nossos diretores e uns para com os outros exige que nos respeitemos e respeitemos os mais elevados padrões éticos de comportamento. Portanto, a adesão estrita a este código é uma condição de certificação” (ISC^2, 2018). O *Código de cânones de ética* estabelece como deveres:

- Proteger a sociedade, a comunidade e a infraestrutura.
- Agir honrosa, honesta, justa, responsável e legalmente.
- Fornecer serviço diligente e competente aos gestores.
- Desenvolver e proteger a profissão.

REFERÊNCIAS

ABNT. **Coletânea de normas técnicas de segurança da informação**. Rio de Janeiro: ABNT, 2013.

FONTES, E. **Segurança da informação**. São Paulo: Saraiva, 2001.

KIM, D. **Fundamentos de segurança de sistemas de informação**. Rio de Janeiro: LTC, 2014.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw Hill, 2008.

ISC². **Código de ética**. ISC², 2018. Disponível em: <https://www.isc2.org/about>. Acesso em: 8 jan. 2019.

ITI – Instituto Nacional da Tecnologia da Informação. **ICP-Brasil**. ITI, 27 jun. 2017. Disponível em <https://www.iti.gov.br/icp-brasil>. Acesso em: 8 jan. 2019.

STALINGS, W. **Criptografia e segurança de redes** – princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

TANENBAUM, A. S. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2001.