TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

Andressa Dellay Agra

Desafios éticos, sociais e de segurança da tecnologia da informação

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Relacionar o uso da tecnologia da informação com aspectos éticos.
- Definir os principais termos utilizados na área de segurança da informação.
- Identificar os diversos tipos de crimes relacionados com a tecnologia da informação.

Introdução

A segurança da informação está diretamente relacionada com a proteção de um conjunto de informações presentes em um servidor de empresa, computador pessoal ou *smartphone*. Atualmente, a informação digital é o bem mais valioso existente dentro das organizações; caso haja perda de parte ou de todo o banco de dados, um grande prejuízo deve ser esperado. Há fatores que podem afetar a integralidade das informações, como o comportamento dos próprios usuários, que pode envolver desafios éticos e sociais.

Neste capítulo, você vai estudar os aspectos éticos relacionados à tecnologia da informação (TI), além de verificar os principais termos utilizados na segurança da informação e identificar os diversos tipos de crimes que ocorrem no meio digital.

Aspectos éticos

A **ética** trata dos comportamentos habituais da sociedade e de como são atribuídos os conceitos de bem e mal a esses comportamentos. O mau uso do acesso a um sistema é uma das ameaças mais difíceis de se identificar. Por exemplo, um funcionário de uma empresa pode estar autorizado a acessar o sistema e, ainda assim, ser uma grande ameaça à segurança da informação.

A ética no tratamento de dados e informações se divide em quatro temas principais:

- **Privacidade** — preservação da privacidade ou identidade de acesso às informações. A privacidade de dados muitas vezes está ligada à segurança individual, explicando os controles rígidos adotados pelas empresas para a guarda dos endereços de celebridades ou dos saldos de contas bancárias, por exemplo. Para manter a privacidade, empresas possuem documentos descrevendo suas políticas e suas ações no que se refere à privacidade e ao sigilo das informações dos usuários e dos clientes.
- **Acuidade (precisão)** — as ações empresariais, como as ações de *marketing*, são essenciais nas corporações. Para que tais ações atinjam o objetivo determinado, é essencial que as informações disponíveis nos bancos de dados do sistema utilizado sejam precisas. Por exemplo, no caso de uma empresa desejar enviar um *flyer* de Dia da Mulher para todas as mulheres cadastradas no sistema, para que o *marketing* aconteça de forma correta, é necessário que as informações estejam precisas quanto ao sexo de todos os clientes cadastrados.
- **Propriedade** — a propriedade intelectual dos dados, modelos, conceitos e documentos utilizados pela empresa deve ser sempre bem estabelecida, sendo respeitada e devendo ser tomados os devidos cuidados para que os dados sejam preservados do acesso e uso indevidos. Por exemplo, ao cadastrar um cliente, inserindo no sistema seus dados pessoais, a empresa será responsável por informar ao mesmo que está sendo efetuado um cadastro e que a empresa se manterá responsável por resguardar essas informações.
- **Acesso** — para manter dados e informações em segurança, é necessário que a empresa estabeleça, claramente, quem pode ter acesso aos dados e às informações disponíveis.

A manutenção de um comportamento ético envolve os seguintes aspectos:

- **Conhecimento** — a empresa deve ter gerência e controle sobre os dados registrados em seus bancos de dados, e os clientes devem estar informados sobre a retenção desses dados.
- **Consentimento** — a empresa somente deve usar os dados com o consentimento e a autorização dos clientes, parceiros e fornecedores a que esses dados se referem.
- **Controle** — o cliente interessado deve poder consultar seus dados e modificá-los caso estejam incorretos.
- **Notificação** — se houver uso dos dados para outras finalidades diferentes das originais, o cliente deve ser avisado previamente.

Fique atento

Para o filósofo inglês Bertrand Russel, a ética é subjetiva e não contém expressões verdadeiras ou falsas; ela é a expressão dos desejos de um grupo, sendo que certos desejos devem ser reprimidos e outros reforçados para se atingir a felicidade ou o equilíbrio do grupo.

Com relação aos **deveres dos profissionais de Informática**, veja o que prevê o Código de Ética do Profissional de Informática, estabelecido pela Sociedade Brasileira de Computação em 15 de julho de 2013:

> Art. 1º: Contribuir para o bem-estar social, promovendo, sempre que possível, a inclusão de todos setores da sociedade.
> Art. 2º: Exercer o trabalho profissional com responsabilidade, dedicação, honestidade e justiça, buscando sempre a melhor solução.
> Art. 3º: Esforçar-se para adquirir continuamente competência técnica e profissional, mantendo-se sempre atualizado com os avanços da profissão.
> Art. 4º: Atuar dentro dos limites de sua competência profissional e orientar-se por elevado espírito público.
> Art. 5º: Guardar sigilo profissional das informações a que tiver acesso em decorrência das atividades exercidas.
> Art. 6º: Conduzir as atividades profissionais sem discriminação, seja de raça, sexo, religião, nacionalidade, cor da pele, idade, estado civil ou qualquer outra condição humana.

Art. 7º: Respeitar a legislação vigente, o interesse social e os direitos de terceiros.
Art. 8º: Honrar compromissos, contratos, termos de responsabilidade, direitos de propriedade, copyrights e patentes.
Art. 9º: Pautar sua relação com os colegas de profissão nos princípios de consideração, respeito, apreço, solidariedade e da harmonia da classe.
Art. 10: Não praticar atos que possam comprometer a honra, a dignidade, privacidade de qualquer pessoa.
Art. 11: Nunca apropriar-se de trabalho intelectual, iniciativas ou soluções encontradas por outras pessoas.
Art. 12: Zelar pelo cumprimento deste código (SOCIEDADE BRASILEIRA DE COMPUTACÃO, 2013, documento on-line).

Exemplo

Vejamos um exemplo ilustrativo de falta de ética na área de segurança da informação.

Suponha que um amigo disponibilizou o seu computador pessoal para que você possa acessar um *software*. Ao acessar o computador, você verificou que a caixa de entrada de e-mails estava aberta e resolveu abrir os e-mails recebidos e enviados de seu amigo. Essa ação é antiética, pois você não recebeu autorização para ler os e-mails do seu amigo e mesmo assim o fez. No caso desse exemplo, você não está respeitando a privacidade do terceiro.

Hoje, um dos maiores desafios é unir de maneira concreta e homogênea valores humanos éticos com objetivos técnicos; por isso, é de extrema importância a conscientização de comportamentos corretos e incorretos relacionados à segurança da informação.

Segurança da informação e estratégias

A segurança da informação é primordial para que as informações sejam salvaguardadas de quaisquer desvios ou interferências que ocasionem a sua alteração. Pensando em uma empresa, atente para as características, os desafios, a missão, a visão, os produtos e os serviços que a mesma possui. Por mais que outras empresas se assemelhem a esta, cada uma tem diferenças que a tornam única, cada qual com suas características personalizadas, que contribuem para a tomada de decisões estratégicas.

Segundo Albuquerque Junior (2017), a **informação** constitui um elemento primordial no processo de tomada de decisões. De fato, a informação é reputada como um ativo essencial que precisa ser adequadamente protegido, pois os avanços da tecnologia, que trouxeram às organizações equipamentos móveis e redes de alta capacidade, em contrapartida tornaram a informação exposta a ameaças e vulnerabilidades diversas.

As **ameaças à segurança da informação** são relacionadas diretamente à perda de uma das suas três principais características: a confidencialidade, a integridade e a disponibilidade. Vejamos o que acontece em caso de prejuízos a cada uma delas:

Perda de confidencialidade — há uma quebra de sigilo de uma determinada informação permitindo que sejam expostas informações restritas, as quais seriam acessíveis apenas por um determinado grupo de usuários. Por exemplo: os executivos podem estar preocupados com a proteção dos planos estratégicos de sua empresa em relação aos concorrentes; as pessoas, por outro lado, estão preocupadas com o acesso não autorizado aos seus registros financeiros. A confidencialidade assegura que o nível necessário de sigilo seja aplicado em cada elemento de processamento de dados e impede a divulgação não autorizada. Algumas medidas para garantir a confidencialidade:

- O acesso à informação é concedido com base na "necessidade de conhecer". Apenas funcionários com extrema necessidade de acesso a determinadas informações terão acesso à parte do sistema.
- Os funcionários tomam medidas para garantir que a informação não vá para pessoas que não necessitam dela.

Perda de integridade — determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação. A integridade se refere a ser correto e consistente com o estado ou a informação pretendida. Qualquer modificação não autorizada de dados, quer deliberada ou acidental, é uma violação da integridade dos dados.

Perda de disponibilidade — a informação deixa de estar acessível para quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio que apresentou uma falha devido a um

erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção. As características da disponibilidade são:

- oportunidade — a informação está disponível quando necessário;
- continuidade — a equipe consegue continuar trabalhando no caso de falha;
- robustez — existe capacidade suficiente para permitir que toda a equipe trabalhe no sistema.

Exemplo

Vamos pensar no quão importante é manter a confidencialidade, a integridade e a disponibilidade em uma organização. Suponha uma clínica de saúde: no sistema, há o cadastro de todas as pessoas atendidas, bem como os seus dados pessoais. Caso a sua integridade gere descrença devido a alguma ameaça no sistema, um caos vai se instalar pela clínica, pois será necessário fazer a recuperação de todos os cadastros na íntegra e verificar a sua veracidade, para, por exemplo, manter conveniados e realizar a cobrança de consultas. A partir desse exemplo, percebe-se a necessidade de manter segura qualquer informação de uma empresa, sendo considerada o bem mais valioso.

Uma ameaça constante nas corporações é a **ameaça humana intencional**. Nessa ameaça, as pessoas intencionalmente causam danos às informações por várias razões. Um fato corriqueiro é o desligamento de um colaborador que possui acesso remoto ao sistema. Caso haja má intenção por parte do ex-funcionário, ao verificar que seu acesso não foi bloqueado, esse usuário pode afetar a integridade e a disponibilidade das informações, ou até mesmo compartilhar informações consideradas sigilosas. De fato, a grande problemática da segurança da informação surge de forma intencional por pessoas maliciosas que querem obter algum benefício próprio, chamar a atenção ou causar prejuízos.

Para que não haja surpresas quanto à segurança das informações dentro das empresas, devemos atentar para algumas **estratégias de segurança**:

- Detectar vulnerabilidades de *hardware* e *software* — os equipamentos estão sujeitos a defeitos de fabricação, instalação ou utilização incorreta, quebra ou queima de componentes e má conservação, o que pode comprometer um ou mais dos princípios da segurança da informação.

Para isso, é necessário fazer a manutenção frequente do *hardware*, com um profissional especializado. Já com relação ao *software*, devem ser adotadas práticas de segurança específicas para que não haja falhas técnicas e de configurações, uso equivocado ou negligência na guarda de *login* e senha de acesso.

- Cópias de segurança — é um mecanismo fundamental para garantir a disponibilidade da informação, caso as bases onde a informação está armazenada sejam danificadas ou roubadas, como o servidor físico ou lógico. O mais importante é que haja pelo menos duas cópias das bases de dados guardadas em locais distintos da instalação original.
- Redundância de sistemas — disponibilização de infraestrutura replicada, ou seja, ter, por exemplo, mais de um servidor funcionando em perfeitas condições, pois, caso um deles falhe, existe o outro que poderá atender às necessidades da corporação.
- Mecanismos de segurança eficazes — existem mecanismos de segurança da informação físicos, lógicos ou uma combinação deles:
  - O mecanismo físico pode ser uma sala de infraestrutura de TI com acesso restrito e com sistema de câmeras de monitoramento. Outra forma de restrição de acesso é o uso de travas especiais nas portas, acionadas por senha. As instalações elétricas e o sistema de refrigeração são imprescindíveis para assegurar condições ideais de funcionamento da infraestrutura de TI, evitando perda de dados por falta ou sobrecarga de energia ou superaquecimento, que danificam os equipamentos de informática.
  - O mecanismo lógico é representado pelo *firewall*, que é o mecanismo de controle do tráfego de dados entre os computadores de uma rede interna e destes com outras redes externas. Utiliza-se também a assinatura digital, uma forma de identificação do usuário que está acessando os recursos de TI. Ela dá validade legal aos documentos digitais, assegurando a autenticidade do emissor da informação. Já por meio da biometria o acesso às informações é liberado somente para a pessoa autorizada, levando em consideração as suas características físicas (impressão digital, voz ou padrões da íris ou do rosto inteiro).
- Política de segurança da informação — é um documento que estabelece diretrizes comportamentais para os membros da organização no que tange às regras de acesso e uso dos recursos de TI. Nesse documento, pode-se determinar a política de senhas, como uma estrutura de configuração que permita induzir a criação de senhas fortes, a fim de dificultar

a ação de *hackers*. Deve-se ainda definir um mecanismo automático que obrigue a troca de senhas periodicamente pelos usuários ativos, fazendo também o cancelamento de senhas de usuários inativos/desligados da organização. Essa é uma das práticas de segurança mais negligenciadas.

- Reconhecimento de malícias — as ações mal-intencionadas de colaboradores internos insatisfeitos e de pessoas externas tornam instável a segurança da informação, especialmente se não houver mecanismos de detecção de intrusões.
- Cultura da organização — a cultura organizacional precisa se adequar à transformação digital, modernizando os seus processos internos sem descuidar da segurança. Com isso, velhos conceitos, práticas e formas de pensar e trabalhar precisam ser revistos e até reinventados, para que todos estejam cientes dos riscos e saibam como proteger as informações empresariais.
- Contratos de confidencialidade — os colaboradores internos de uma organização e os terceirizados, especialmente aqueles vinculados à área de TI, muitas vezes têm acesso a informações sigilosas, que precisam ser resguardadas. A melhor forma de preservar a segurança da informação nesses casos é fazer um contrato de confidencialidade com todas as pessoas que conhecem e acessam informações sigilosas.
- Privilégios mínimos — apenas pessoas com necessidade de acesso a determinadas informações devem tê-lo, caso contrário, o nível de risco aumenta.

Saiba mais

Alinhado com as questões de segurança da informação, foi criada a Lei Geral de Proteção de Dados LGPD (Lei Nº 13.709, de 14 de agosto de 2018). Essa lei objetiva proteger os direitos fundamentais, relacionados a privacidade e liberdade, em relação aos dados de indivíduos que se localizam em território Brasileiro. Saiba mais sobre ela em:

https://bit.ly/2YKAzdY

Crimes relacionados com a tecnologia da informação

Com a expansão do uso de tecnologias e o compartilhamento de informações, há um crescimento de **crimes** nas áreas em questão. Castells (2008) indica como sintomático o fato de as atividades criminosas e as organizações ao estilo da máfi a, de todo o mundo, terem se tornado globais e, com a ajuda dos meios informacionais, serem capazes de proporcionar, em qualquer parte do mundo, meios para viabilizar negócios ilícitos, desde o contrabando de armas sofi sticadas até o de substâncias químicas ilegais, passando pelo comércio de favores sexuais e pelo tráfi co de pessoas. O autor acrescenta que uma das redes mais poderosas da sociedade contemporânea — a de produção e distribuição de narcóticos —, juntamente com seu componente intrínseco — a lavagem de dinheiro —, construíram uma geografi a específi ca, toda conectada em rede, a qual fl ui para a mãe de toda a acumulação, que é a rede fi nanceira global.

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, foram registrados mais de 722 mil **incidentes de segurança** na Internet em 2015. Os cinco tipos mais comuns foram: *scan*, fraude, ataques a servidores *web*, *worms* e *Denial of Service* (DoS). As invasões de computadores, que costumam ser o tipo de ataque mais temido, representaram menos de 1%. Vejamos a descrição de cada um desses **tipos de ataque**:

- *Scan* — é um ataque que quebra a confidencialidade com o objetivo de analisar detalhes dos computadores presentes na rede (como sistema operacional, atividades e serviços) e identificar possíveis alvos para outros ataques. As principais formas de prevenção são a manutenção de um *firewall* na empresa e uma configuração adequada da rede.
- Fraude — a fraude, ou o *scam* (com "m"), abrange uma quantidade ampla de tipos de ataque. Um dos mais comuns é o *phishing*, que, para obter informações do usuário, utiliza estratégias como a cópia da interface de *sites* famosos e o envio de e-mails ou mensagens falsas com *links* suspeitos. O principal meio de evitar fraudes é a conscientização dos usuários por meio de treinamentos sobre cuidados na rede.

- Ataques ao servidor *web* — os primeiros ataques de rede exploravam as vulnerabilidades relacionadas com a implementação de conjuntos de protocolos TCP/IP. O princípio básico durante qualquer desenvolvimento informático é que não se deve confiar nos dados enviados pelo cliente. Quase todas as vulnerabilidades dos serviços *web* estão relacionadas à negligência dos desenvolvedores, que não são cuidadosos o suficiente em relação ao formato dos dados inseridos pelos usuários. Os ataques contra os aplicativos *web* são sempre prejudiciais, porque denigrem a imagem da empresa.
- *Worms* — são alguns dos *malwares* mais comuns e antigos. *Malwares* são *softwares* que têm como intuito prejudicar o computador "hospedeiro". Essa categoria engloba tanto os vírus quanto os *worms,* entre diversos outros tipos de programas maliciosos. Os worms são perigosos devido à sua capacidade de se espalhar rapidamente pela rede e afetar arquivos sigilosos da empresa. Os principais meios de prevenção são a manutenção dos antivírus e os treinamentos de conscientização.

- *DoS Attack* — é um ataque em que um computador denominado mestre pode ter sob o seu comando até milhares de computadores "zumbis". Esse ataque consiste em fazer com que as máquinas infectadas e sob o comando do computador mestre se preparem para obedecer a um determinado recurso em um determinado servidor. Dependendo do recurso atacado, o servidor pode chegar a reiniciar ou até mesmo ficar travado.

Além dos incidentes de segurança da informação citados, vamos apontar os **principais crimes cometidos na Internet**:

- Injúria e difamação — divulgar informações falsas em relação a uma pessoa ou a uma empresa é crime e pode levar a diversas penalidades. Quando esse crime ocorrer por meio da Internet, será considerado um crime virtual. Vale destacar que as vítimas podem acessar o poder judiciário e requerer indenização e reparação do dano. Para isso é essencial procurar uma delegacia especializada e registrar denúncia. Vejamos o que o Código Penal brasileiro dispõe sobre a injúria e a difamação nos arts. 139 e 140: "Art. 139. Difamar alguém, imputando-lhe fato ofensivo à sua reputação: […]"; "Art. 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro […]" (BRASIL, 1940, documento on-line).
- Utilização de *softwares* falsos — alguns *softwares*, quando instalados em um computador, permitem acesso a todos os dados pessoais registrados na máquina. Com os dados em mãos, é possível falsificar cartões de créditos, realizar transações bancárias e muito mais. O crime de invasão e roubo de dados é mais comum do que pode parecer e está previsto no art. 154-A do Código Penal brasileiro, nos seguintes termos:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: […] (BRASIL, 1940, documento on-line).

- Criação de perfis falsos — ao criar contas utilizando nomes falsos, os usuários podem divulgar conteúdos mentirosos e gerar vários problemas, como a disseminação de *fake news*.

- Apologia ao crime — é comum a criação de páginas e perfis que estimulem a prática de crimes como pedofilia, racismo, furtos, etc. Esses perfis geralmente possuem acesso privado, e os membros compartilham dicas e sugestões para a prática de atos ilícitos.
- Plágio — é a cópia de informações veiculadas por terceiros sem a indicação da fonte. O crime está previsto na Lei nº. 9.610, de 19 de fevereiro de 1998, que dispõe sobre a proteção dos direitos autorais, e aquele que o comete pode sofrer pena de detenção e ser obrigado ao pagamento de multa.

Fique atento

Desde 2012, existe a norma conhecida como Lei Carolina Dieckmann (Lei nº. 12.737, de 30 de novembro de 2012), a qual faz algumas alterações no Código Penal brasileiro. Essa lei é um dos primeiros esforços para estabelecer segurança jurídica para a vida privada *on-line*. A Lei em questão prevê parte do novo texto dos arts. 154, 266 e 298 do Código Penal, determinando, em suma, que a invasão de dispositivo informático alheio para obtenção de dados sem autorização é punível com detenção de três meses a um ano mais multa.

Referências

ALBUQUERQUE JUNIOR, A. E. *Adoção de medidas de segurança da informação:* a influência das respostas estratégicas das subunidades na conformidade organizacional. 2017. 368 f. Tese (Doutorado em Administração) — Universidade Federal da Bahia, Salvador, 2017.

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 10 maio 2018.

CASTELLS, M. A era da informação: economia, sociedade e cultura. In: *A Sociedade em rede*. São Paulo: Paz e Terra, 2000. v. 1.

SOCIEDADE BRASILEIRA DE COMPUTACÃO. Código de Ética do Profissional de Informática. 15 de julho de 2013. Disponível em: <http://www.sbc.org.br/jdownloads/02.codigo_de_etica_da_sbc.pdf>. Acesso em: 8 out. 2018.

Leituras recomendadas

CARNEIRO, L. D. Infrações penais e a informática: a tecnologia como meio para o cometimento de crimes. *Revista Jus Navigandi*, Teresina, ano 21, n. 4921, 21 dez. 2016. Disponível em: <https://jus.com.br/artigos/52698/infracoes-penais-e-a-informatica--a-tecnologia-como-meio-para-o-cometimento-de-crimes>. Acesso em: 8 out. 2018.

CARVALHO, L. S. Ética no tratamento de dados e informações. *Administradores*, 31 dez. 2009. Disponível em: <http://www.administradores.com.br/artigos/tecnologia/etica--no-tratamento-de-dados-e-informacoes/37258/>. Acesso em: 8 out. 2018.

HINTZBERGEN, J. et al. Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002. 3. ed. Rio de Janeiro: Brasport, 2018.

LEMOS, H. D. Ética em informática. *DevMedia*, 16 out. 2009. Disponível em: <https://www.devmedia.com.br/etica-em-informatica/14636>. Acesso em: 8 out. 2018.

OLIVEIRA, D. Conheça 16 tipos de ameaças virtuais que podem invadir seu computador. *ITF 365*, 2014. Disponível em: <https://www.itforum365.com.br/seguranca/conheca-16-tipos-de-ameacas-virtuais-que-podem-invadir-seu-computador/>. Acesso em: 8 out. 2018.

SÊMOLA, M. *Gestão da segurança da informação.* 2. ed. Rio de Janeiro: Elsevier, 2014.

Conteúdo: