Sistemas de informação em segurança

Sistemas de informação em segurança

Sergio da Costa Ferreira

Dados Internacionais de Catalogação na Publicação (CIP)

Ferreira, Sergio da Costa
F383s Sistemas de informação em segurança / Sergio da Costa Ferreira. – Londrina : Editora e Distribuidora Educacional S.A. 2017.
224 p.

ISBN 978-85-522-0225-7

1. Computadores – medidas de segurança. I. Título.

CDD 005.8

2017
Editora e Distribuidora Educacional S.A.
Avenida Paris, 675 – Parque Residencial João Piza
CEP: 86041-100 — Londrina — PR
e-mail: editora.educacional@kroton.com.br
Homepage: http://www.kroton.com.br/

Sumário

Palavras do autor

Caro aluno,

Para compreender a importância dos sistemas de informação em segurança é necessário entender que, hoje em dia, a humanidade está vivendo a era da informação automatizada. Era esta em que todos manipulam informações a todo momento, tanto informalmente, num momento de lazer quanto assistindo a um filme no tablet, interagindo com suas redes sociais no smartphone, ou profissionalmente no trabalho, operando sistemas da empresa que automatizam os processos de negócio. Ou você conhece alguém que não usa nenhuma tecnologia no dia a dia? É raro, não é?! Pois, então, toda essa informação é processada por sistemas das mais diversas naturezas e graus de complexidade. Esses sistemas são denominados sistemas de informação (SI) e, nas diversas áreas de conhecimento e atuação profissional, é extremamente importante que se consiga entender o papel deles no cotidiano do nosso ramo de atividade. Daí a grande importância da disciplina de sistemas de informação em segurança, qual seja, saber e entender como e onde os sistemas de informação podem contribuir para operacionalizar e melhorar a segurança que está sendo implantada, sendo objetivo do estudo da disciplina compreender a atuação desses sistemas de informação na área de segurança pública e privada.

Atualmente, os sistemas de informação evoluem muito rapidamente, por conta do surgimento contínuo de novas tecnologias, gerando a necessidade da manutenção de um estudo autônomo constante sobre o assunto, visando manter-se sempre atualizado com as soluções oferecidas pelo mercado de sistemas de informação para segurança.

Para compreender o papel dos sistemas de informação na segurança, serão trabalhadas uma competência geral, a de interpretar o papel dos sistemas de informação e da gestão do conhecimento, a partir do contexto da segurança pública e da segurança privada, além de duas competências profissionais, quais sejam: identificar os conceitos de dados, de informação, de sistemas de informação, de tecnologia da informação e suas aplicações na segurança pública

e privada; e distinguir o papel dos sistemas e das informações nas seguranças públicas e privadas.

Com o intuito de desenvolver as competências acima durante a disciplina, o conteúdo deste livro didático foi dividido em quatro grandes blocos de assuntos, ou unidades de ensino (UE). Na primeira unidade de ensino – "Sistemas de Informação" –, estudaremos uma introdução aos SI, os SI nas organizações e o conceito de tecnologia da informação (TI) e sua aplicação na segurança pública e privada; na segunda – "A Gestão e a Segurança da Informação" –, veremos a gestão estratégica da informação, a segurança da informação e a segurança na era da Internet; na terceira – sistemas e informações na segurança pública e privada –, nos aprofundaremos na lei de acesso à informação e nos sistemas e informações na segurança pública e privada; e, finalizando, na quarta unidade de ensino – "A Gestão do Conhecimento na Segurança Pública e Privada" –, buscaremos conhecer a gestão do conhecimento, as técnicas e tecnologias para o suporte do conhecimento e a gestão do conhecimento nas organizações e na segurança pública e privada.

Dessa forma, caminharemos ao longo de todos esses conteúdos, desejando que os ensinamentos sejam proveitosos e que realmente o qualifiquem para o desempenho técnico de suas funções com qualidade e eficiência, evidenciando um aprendizado sólido e consistente. Mas, para que isso tudo se torne realidade, você, aluno, é o principal ator nesse processo. E esperamos contar com todo o seu esforço, dedicação e vontade de aprender para atingir seus objetivos de vida e realizar seus sonhos. Desejamos, desde já, bons estudos e sucesso na disciplina.

Sistemas de informação

Convite ao estudo

Olá! Vamos começar nossos estudos entendendo que, atualmente, a informação e os sistemas de informação baseados em tecnologias da informação e comunicação vêm alterando o perfil de negócio das empresas em todos os ramos de atividade. Sendo assim, é fundamental que um profissional do ramo de segurança tenha condições de identificar os conceitos de dados e informações, de sistemas de informação, de tecnologia de informação e suas aplicações na segurança pública e privada, para, por exemplo, produzir um boletim de ocorrência eletrônico, procedimento no qual será necessário saber interpretar o papel dos sistemas de informação na segurança; identificar os conceitos de dados e informações e suas aplicações na segurança; e distinguir o papel dos sistemas e das informações nas seguranças públicas e privadas.

Consideraremos, então, o seguinte contexto para desenvolver os nossos estudos: o ramo da segurança privada não é tão tranquilo como algumas pessoas pensam. O país vive um problema recorrente quanto à questão da criminalidade. A cada dia, aumentam as estatísticas dos crimes relacionados às questões patrimoniais nas empresas e organizações. Dependendo do valor agregado de um produto e de quão esse é valoroso para o mercado do crime, as empresas têm sofrido todo o tipo de ação da marginalidade, até mesmo assaltos de grandes proporções, com elementos fortemente armados.

Por sua parte, o Estado tem certa dificuldade em prover uma situação de segurança plena, haja vista os altos índices de criminalidade. Além disso, se, por um lado, crescem as demandas nessa área pelos serviços particulares, por outro, os riscos que a segurança privada tem de prever e gerenciar são cada vez maiores.

Nessa complexa conjuntura, a JRW Defender, empresa de grande porte especializada em segurança privada, que atua fortemente no Brasil como um todo, nos ramos de segurança patrimonial, ronda e escolta e segurança bancária, tem tido cada vez mais registros de eventos relacionados a furtos e roubos em sua rotina. Em seu cadastro de serviços que presta às diversas empresas, tem sido cada vez mais comum as ocorrências, e essas devem ser registradas para que os gestores da JRW possam analisá-las em detalhes, o que permitirá tomar medidas que visem impedir ou mitigar novos eventos.

A alta administração da empresa já percebeu que essa sistemática de registro dos fatos e anormalidades nas organizações em que presta serviços não está a contento. Por vezes, os profissionais da segurança realizam a escrituração da anormalidade em fichas específicas em papel, que, muitas vezes, acabam se extraviando. Livros registros são utilizados, mas, dependendo da caligrafia do vigilante, os dados exatos daquela ocorrência podem ficar ilegíveis e comprometidos.

A JRW Defender está em fase de estudos no sentido de rever todos os seus sistemas de informações, e a intenção da diretoria é implementar sistemas com suporte da tecnologia de informação que permitam o lançamento em aplicativos e bancos de dados de todas as séries de fatos ou eventos isolados que possam se tornar informações relevantes para a tomada de decisão.

Você já pensou quais conhecimentos serão necessários para que a empresa consiga se atualizar? Será que a implantação de um sistema de informação automatizado fará com que a empresa atinja os resultados esperados? Será que isso se aplica ao ramo da segurança?

Para que nós possamos responder a todas essas perguntas, estudaremos, ao longo da Unidade 1, os seguintes temas: introdução aos sistemas de informação, os sistemas de informação nas organizações e o conceito de tecnologia da informação e sua aplicação na segurança pública e privada. Você está animado para o estudo? Vamos lá, então!

Seção 1.1

Introdução aos sistemas de informação

Diálogo aberto

Agora, vamos imaginar uma situação muito comum no dia a dia de um profissional da área de segurança, como o nosso amigo João Wanderson, inspetor de segurança patrimonial muito bem qualificado, que trabalha na JRW há mais de dez anos, e recebeu orientações do seu diretor regional, no sentido de permanecer atento a todos os eventos que ocorram nos locais onde são prestados os serviços de segurança patrimonial, na área de sua responsabilidade, com a finalidade de dimensionar todos os aspectos que contribuam para rever todos os sistemas de informações e agilizar a tomada de decisão por parte dos responsáveis.

Certo dia, ao assumir seu turno de trabalho, João recebeu no rádio um chamado de um dos seus vigilantes de confiança, Antônio das Neves, informando que ocorrera furto de materiais particulares dos funcionários no banheiro masculino da Flextram Suporte e Soluções em RH, escritório em que a JRW presta seus serviços de segurança patrimonial. Os donos da empresa estavam indignados com a falha na segurança e solicitavam a presença do inspetor de segurança para realizar, o mais rápido possível, o registro da ocorrência em uma Delegacia de Polícia (DP), com a finalidade de dar um retorno aos funcionários que tiveram suas carteiras e documentos furtados nos armários dos colaboradores.

João Wanderson se deslocou até a Flextram e solicitou ao vigilante Antônio das Neves os dados sobre o local, condições em que se encontrava o material furtado, bem como se foi possível dimensionar o horário mais preciso em que ocorrera o furto, o horário em que foi dada a falta do material, os colaboradores que tiveram seu material subtraído, se houve testemunhas, quem poderia ser responsabilizado e outros aspectos que pudessem elucidar claramente a infração. Nesse momento, João percebeu que o vigilante Antônio não tinha levantado todas essas informações. Talvez, não fosse tão simples realizar o registro na DP.

João Wanderson, experiente inspetor, já tinha realizado diversos

Boletins de Ocorrência (BO) e decidiu ir até a Delegacia Especializada em Roubos e Furtos para registrar a ocorrência e verificar se tinha as informações necessárias para realizar um BO adequado, que serviria plenamente para dar um retorno aos donos da empresa Flextram e às pessoas prejudicadas. Ele sabe que as investigações e inquéritos só iniciam com o registro dos fatos.

Na delegacia, o escrivão elencou todos os dados necessários para a elaboração de um BO de furto. O desafio de João Wanderson será verificar se tem todas as informações para a confecção do Boletim de Ocorrência. Quais serão, então, os dados mais importantes? Será que o vigilante Antônio deixou de relatar algum fato essencial que implicará um BO pouco consistente, o qual não permitirá qualquer investigação por parte da polícia?

Caro aluno, sua tarefa será elaborar uma lista de dados fundamentais e necessários, aqueles que o inspetor João Wanderson deve apresentar por escrito, para a elaboração de um Boletim de Ocorrência. Você elaborará um checklist com os dados necessários e, posteriormente, demonstrará como esses dados podem se transformar em informações e em conhecimento. Lembramos a você que essa apresentação por escrito dos dados necessários para a ocorrência contribuirá para a elaboração da primeira parte de seu produto. Para solucionar esses problemas, você necessitará conhecer os conceitos sobre dado, conhecimento, informação e sabedoria, bem como o papel e valor das informações nas organizações. Vamos iniciar, então?

Não pode faltar

Para nós compreendermos o que é um sistema de informação, vamos inicialmente procurar entender o que é um sistema e o que é uma informação. Segundo Von Bertalanffy (2012), os sistemas estão presentes em toda parte no mundo moderno. Com isso, ele quis evidenciar que é fundamental que pessoas, empresas, países e qualquer outro tipo de organização interajam com outras organizações, sendo essa uma condição para sua própria existência. Ou seja, aquele ou aquilo que não interage com nenhum outro está fadado ao desaparecimento. Para Bertalanffy,

os sistemas estão presentes desde a mais simples célula do corpo humano até o mais completo bioma existente na natureza, que, agregando o clima, a fauna, a flora, o relevo, a hidrografia, formam um complexo ecossistema.

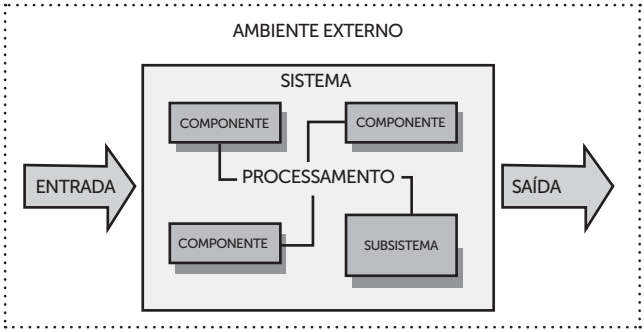
A teoria de Von Bertalanffy também enuncia que é preciso avaliar e compreender as organizações como um todo, no qual cada parte, departamento ou setor interage com os demais de forma colaborativa para que os resultados ou objetivos da organização sejam alcançados; e não enxergar a organização em partes separadas, em que cada setor ou departamento seja independente e isolado. Essa teoria está presente em todas as tecnologias atuais, e o pensamento sistêmico está presente em todas as áreas do conhecimento atualmente, produzindo resultados nunca antes imaginados.

Pesquise mais

Para entender melhor, leia: AUDY, Jorge Luis Nicolas; ANDRADE, Gilberto Keller de; CIDRAL, Alexandre. **Fundamentos de sistemas de informação**. Porto Alegre: Bookman 2009.

Compreendida a teoria de Von Bertalanffy, vamos agora formular o conceito de sistema. O conceito de sistema é tratado de diversas formas na literatura e com uma grande variação, dependendo da área do conhecimento, entretanto veremos o conceito básico de sistema, justamente para entender o que é um sistema e imaginar como esse conceito pode estar presente no nosso dia a dia e na área da segurança. Pode-se afirmar que um sistema é um conjunto de componentes (que podem ser subsistemas) os quais interagem entre si e com o ambiente externo, formando um todo organizado para atingir um objetivo comum ou resultado. Um sistema, normalmente, recebe uma entrada, que passa por um processamento ou transformação, gerando uma saída ou produto, que, além de ser a razão da existência do sistema, também pode servir como entrada para outro sistema e assim por diante. A figura a seguir (Figura 1.1) representa o esquema simplificado de um sistema.

Figura 1.1 | Esquema de sistema simplificado



Fonte: elaborada pelo autor.

Assimile

Componentes: são as partes que constituem o sistema, podendo também ser subsistemas.

Entrada: tudo aquilo que o sistema deve receber para ser processado e convertido em saída.

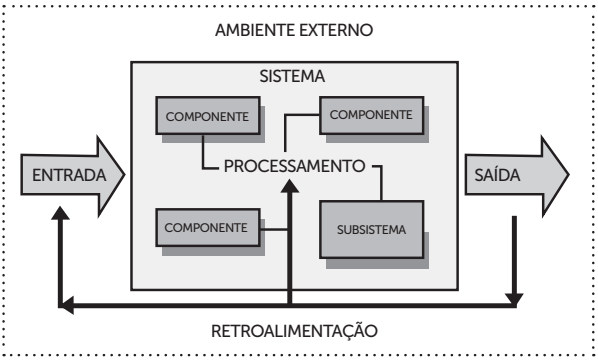
Processamento: é a operação realizada pelos componentes do sistema para transformar as entradas em saídas.

Saída: produto gerado pelo processamento das entradas no sistema ou objetivo comum que levou os componentes do sistema a interagirem entre si.

Outro conceito muito importante no estudo dos sistemas é o da retroalimentação ou feedback. Como vimos anteriormente, os sistemas recebem entradas, executam o processamento e geram as saídas. Todo esse processo é repetido continuamente durante o ciclo de vida do sistema, portanto, deve existir uma rotina de avaliação do resultado do sistema, para que ele esteja em constante evolução e melhoria. A fim de avaliar se o resultado produzido pelo sistema está adequado ou para melhorar o resultado atingido, é preciso avaliar as saídas ou o produto do sistema. Essa avaliação deve se transformar em uma nova entrada para melhorar a qualidade dos componentes do sistema, das próprias entradas e do processamento que ele executa. Em outras palavras, da avaliação das saídas do sistema, originar-se-ão novas entradas, e, assim, o sistema estará se retroalimentando ou recebendo feedbacks, que

garantirão a qualidade de seu produto e a certeza da evolução contínua do sistema (Vide Figura 1.2).

Figura 1.2 | Retroalimentação no sistema



Fonte: elaborada pelo autor.

Reflita

Agora que compreendemos o conceito de sistema, que tal tentar imaginar como esse conceito aparece em nosso dia a dia, buscando identificar componentes, entradas, processamentos, saídas e feedback?

Você provavelmente já ouviu falar nestes sistemas:

- Sistema digestivo
- Sistema de ensino
- Sistema solar
- Sistema eleitoral
- Sistema financeiro

E aí? Como você compreende esses sistemas agora?

Uma vez entendido o conceito de sistemas, vamos nos dedicar a compreender o que é uma informação. O termo informação é largamente empregado nos dias de hoje. A informação está movendo o mundo. Um fato acontece em uma região distante do planeta e em questão de instantes todos já estão tomando conhecimento, isso se não ocorrer em tempo real, como foi o caso do atentado às torres gêmeas nos EUA em 2001 e o tsunami no Japão em 2011, que o mundo inteiro assistiu ao vivo pela televisão. Portanto, está mais do que evidenciada a importância

da informação, que é considerada atualmente como o bem mais valioso de uma organização. Mas será que esse termo está sendo empregado corretamente? Ou está sendo confundido com outro conceito correlato, tal como dado ou conhecimento? Vamos, então, definir exatamente o que é dado, o que é informação e o que é conhecimento. Assim, nós compreenderemos o conceito de informação e poderemos refletir sobre a sua importância para as organizações e para a segurança.

Segundo Stair e Reynolds (2015), os **dados** são fatos brutos, com pouca importância ou significado, por exemplo: a nota de um aluno na prova (7,5), a temperatura ambiente (25 ºC), o preço de um produto (R$ 50,00), a distância entre duas cidades (20 km), a quantidade de homicídios em uma região por mês (17), a altura de um prédio (18,67 m), a data de nascimento de uma pessoa (15/03/1994), e assim por diante. Percebam que um dado isolado apresenta um significado irrelevante, isto é, não é capaz de nos transmitir uma mensagem ou entendimento sobre algum assunto, simplesmente nos apresentando um fato do mundo real.

No entanto, quando o dado sofre algum processo de tratamento, no qual passa a apresentar algum significado relevante, transforma-se em uma **informação**, que nada mais é do que uma organização de dados que passam a ter um significado além do significado individual de cada dado isolado. Por exemplo: o aluno obteve nota 7,5 e foi aprovado; o quilo da carne de primeira chegou a R$ 50,00, o maior já registrado; a competição foi realizada em uma cidade próxima, a 20 km de distância; o número de homicídios na região caiu 40%, chegando ao índice de 17 por mês; o prédio onde moro fica localizado em uma área onde só tem casas, destacando-se com seus 18,67 m de altura; a atleta mais jovem da competição tinha 23 anos de idade. Notem que, em todos esses exemplos, nós conseguimos tirar conclusões, fazer inferências e até tomar decisões.

Dentro do nosso conhecimento de sistemas, podemos concluir que, para transformar um dado em informação, é necessário

processá-lo, ou seja, o dado é a entrada e a informação é a saída, e o processo é o conjunto de atividades desenvolvidas pelos componentes do sistema para produzir o resultado esperado.

Ainda dentro desse raciocínio, vamos explorar o conceito de **conhecimento**, o qual indica um grau de compreensão que vai além das informações; pois além de um significado, o conhecimento pode ter uma aplicação. O conhecimento encerra a ideia de compreensão de um conjunto de informações e como essas informações podem ser úteis para a execução de uma determinada tarefa ou tomada de decisão (STAIR; REYNOLDS, 2015). Ter conhecimento significa adquirir ideia ou noção de alguma coisa. Por exemplo, o conhecimento necessário para implantar um sistema de segurança em uma residência é a compreensão de que tipos de ameaças essa residência está sujeita e quais as vulnerabilidades que essa residência possui, além da compreensão das probabilidades de as ameaças agirem sobre as vulnerabilidades existentes, podendo-se, assim, tomar medidas passivas e ativas para administrar os riscos que essa residência está passível, prevenindo-se de possíveis ataques ou investidas. A partir do conhecimento, pode-se chegar à **sabedoria**, que é a experiência adquirida com a aplicação do conhecimento, ou seja, a sofisticação do conjunto de conhecimentos adquiridos ao longo do tempo, geralmente por meio de reflexão e experiência; é saber quando e como empregar o conhecimento correto.

Assimile

Dado: fatos brutos.

Informação: conjunto de dados com um significado relevante.

Conhecimento: compreensão de um conjunto de informações e como essas podem ser úteis para a execução de uma determinada tarefa ou tomada de decisão.

Sabedoria: experiência com a aplicação do conhecimento.

Exemplificando

Dado: número de assaltos a agências bancárias no estado de SP.

Informação: estatísticas apontam para um aumento significativo no número de assaltos a agências bancárias no estado de SP, no último período.

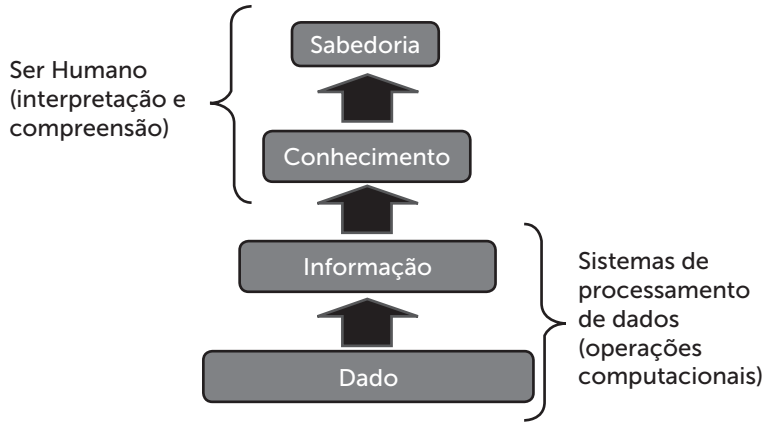
Conhecimento: o gestor de segurança sabe que, quando a ameaça sofre alteração, o sistema de segurança também deve ser modificado, normalmente atuando-se sobre as vulnerabilidades que estão sendo alvo das novas ameaças. Então, em virtude do aumento de assaltos a agências bancárias no estado de SP, a segurança das agências será reforçada com mais dois agentes e serão instaladas novas portas com detector de metais, além de haver melhoria no sistema de acionamento da Polícia Militar.

Sabedoria: a experiência adquirida para lidar com situações dessa natureza no futuro, ou seja, devemos ficar atento às ocorrências de delitos cometidos contra empresas do mesmo ramo de atividade, analisando tendências e buscando identificar as vulnerabilidades exploradas, visando reestruturar a segurança para evitar reveses.

As informações realmente são muito valiosas, mas o conhecimento constitui um saber e produz ideias e experiências que as informações por si só não são capazes de externar. Considerando que uma informação é um dado processado por um sistema de processamento de dados, podemos concluir que o conhecimento é a informação processada, só que, nesse caso, processada pelo ser humano, já que o ser humano é o único processador capaz de produzir conhecimento e sabedoria.

Para resumir e ilustrar o que foi apresentado sobre dado, informação, conhecimento e sabedoria, vamos observar a figura a seguir (Figura 1.3), que representa o dado como elemento base ou matéria-prima para a elaboração da informação, por meio do processamento computacional; já o processamento da informação para gerar conhecimento e sabedoria é feito pelo ser humano, através de suas interpretações e compreensões acerca do conjunto de informações disponibilizadas.

Figura 1.3 | Dado, informação, conhecimento e sabedoria



Fonte: elaborada pelo autor.

Aproveitando todo o conhecimento adquirido até o momento – principalmente sobre sistemas e informação, podemos prosseguir conceituando sistema de informação.

Para Laudon e Laudon (2007), sistema de informação pode ser definido como um conjunto de elementos inter-relacionados e operando colaborativamente para coletar ou recuperar, processar, armazenar e transmitir informações em uma organização, apoiando a tomada de decisão, a coordenação e o controle. Já para Stair e Reynolds (2015), sistema de informação é um conjunto de elementos que se relacionam entre si para coletar (entrada), manipular (processo) e disseminar (saída) informações. Percebe-se que ambos os autores possuem definições bem parecidas de sistema de informação e, se enunciarmos outra definição, também não seria muito diferente deles, por isso, podemos definir sistema de informação como sendo um todo coeso, contendo componentes, que podem ser pessoas, processos e tecnologias (hardware, software, rede, banco de dados), que se organizam e se relacionam para coletar dados, processá-los, armazená--los e difundir informações, provenientes desses dados, para a organização, proporcionando o aprimoramento dela e maximizando a produtividade da empresa. Normalmente, os sistemas de informação organizacionais são apoiados em tecnologias da informação e comunicação, estruturando a

manipulação dos dados e automatizando o fluxo de informações, agilizando a rotina de negócio da empresa e proporcionando um suporte sólido e oportuno para o processo decisório da empresa. Dessa maneira, um sistema de informação passa a fazer parte do sistema organizacional da empresa, normalmente se ramificando por todos os setores da organização e atingindo todos os seus colaboradores e clientes. A finalidade de um sistema de informação organizacional será sempre coletar dados internos e externos da empresa, processá-los e disponibilizar informação para todos os departamentos, colaboradores e clientes.

Agora que já conhecemos a parte conceitual sobre a informação e os sistemas de informação, vamos estudar como eles se enquadram nos processos das organizações.

Atualmente, a informação desempenha um papel fundamental nas organizações, afetando diretamente o funcionamento das empresas, desde o nível operacional, estabelecendo como será a produção dos produtos pelos operários, passando pelo nível tático, alterando a forma como os gerentes administram os recursos de produção, até chegar ao nível estratégico, interferindo diretamente no planejamento estratégico e no processo decisório dos executivos de alto escalão.

Os maiores responsáveis por esse crescimento do papel da informação nas organizações são os sistemas de informação, que, além de armazenarem uma quantidade muito grande de dados, disponibilizam informações de uma forma mais rápida e estruturada, elevando muito a qualidade da informação, ou o significado útil dos dados, permitindo uma produção de conhecimento que acaba resultando em decisões estratégicas que se transformam em ações de melhoria para o negócio da empresa. Muitas vezes, esses conhecimentos acabam tendo uma importância muito grande e até vital para o crescimento e sobrevivência da empresa no mercado.

Mas como a informação, disponibilizada pelos SI, está modificando o perfil dos negócios? Segundo o artigo publicado no site B2W Digital (2016), o comércio eletrônico no Brasil faturou cerca de R$ 41 bilhões em 2015, crescendo 15,3% em relação

a 2014, com mais de 100 milhões de pedidos realizados. Esse aumento foi devido ao crescimento do acesso à Internet e ao avanço nas vendas de smartphones. A Associação Brasileira de Comércio Eletrônico divulgou que nos próximos anos o setor deve continuar crescendo e ampliando sua participação em relação ao comércio varejista convencional, com destaque para o aumento nas vendas de bens digitais. E esse setor continuará crescendo, porque os investimentos estrangeiros serão feitos não apenas na forma de capital, mas também como tecnologias e conhecimento. Em 2016, projeta-se que o comércio eletrônico no Brasil atinja um faturamento de mais R$ 44 milhões.

A partir da publicação acima, principalmente do trecho em destaque, pode-se identificar claramente que a forma de fazer negócio vem se alterando com o passar dos anos e também fica muito evidenciado o crescimento dos sistemas de informação nas empresas, sem os quais seria impossível migrar para a área de comércio eletrônico. Para Laudon e Laudon (2007), esse crescimento é devido aos sistemas de informação que viabilizam a consecução de seis objetivos organizacionais, sejam eles: excelência operacional; criação de novos produtos, serviços e modelos de negócio; relacionamento mais estreito com clientes e fornecedores; melhoria no processo de tomada de decisão; obtenção de vantagem competitiva; e sobrevivência no mercado. Isto é, uma organização moderna que não automatiza seu processo informacional com o emprego de um sistema de informação dificilmente conseguirá se estabelecer no mercado e manter-se em condições competitivas com seus concorrentes.

Dentro desse contexto, a informação ganhou uma importância muito grande dentro das organizações, de tal forma que passou a agregar mais valor até do que os bens de produção, o capital e os recursos humanos da empresa. Para Caruso (1995), recentemente a informação assumiu uma importância vital para a manutenção dos negócios de qualquer empresa, pois estamos vivendo em uma sociedade globalizada, marcada pelo dinamismo e permanentemente conectada, de maneira tal que não existe mais uma organização não dependente da informação e da tecnologia da informação. Muito bem, aluno, adquirimos muitos conhecimentos até agora. Vamos em frente.

Sem medo de errar

Vamos à solução da nossa situação-problema, compreendendo que Boletim de Ocorrência é um documento muito importante, porque contém todas as informações sobre a ocorrência de um fato que poderá gerar uma investigação policial e até mesmo um processo no judiciário, por isso deve ser completo e preciso. Na verdade, os dados contidos no BO são as entradas necessárias para o sistema de informação da polícia, que passará a executar os procedimentos policiais decorrentes da comunicação desses delitos, uma investigação, por exemplo, e que, de alguma forma, produzirá resultados ou saídas, que podem ser uma denúncia, um processo judicial etc. Perceba que os dados e informações provenientes de um boletim de ocorrência passam a ter um valor muito grande para os órgãos de segurança pública, uma vez que podem transformar-se em informações que irão compor peças de processos e servir como base para condenação de infratores, bem como determinar a tomada de decisão de, por exemplo, áreas que necessitam de um policiamento mais efetivo, decorrente de uma tendência crescente no número de assaltos à mão armada, relatados em boletins de ocorrência nos últimos tempos.

Pois bem, como sua tarefa era elaborar uma lista de dados fundamentais e necessários, aqueles que o inspetor João Wanderson deve apresentar por escrito, para a elaboração de um Boletim de Ocorrência, veja como poderia ser solucionada:

- Local da ocorrência (onde o furto aconteceu)
    - logradouro (rua, avenida, travessa etc.)
    - número
    - bairro
    - cidade
    - estado
    - CEP
    - complemento
    - ponto de referência

- Quando aconteceu o fato
  - data
  - hora

- Comunicante da ocorrência (pessoa que registrou o BO)
  - nome completo
  - sexo
  - telefone
  - e-mail
  - CPF
  - RG (com órgão expedidor)
  - data de nascimento
  - nacionalidade
  - naturalidade
  - estado civil
  - nome dos pais
  - endereço completo (logradouro, número, bairro, cidade, estado, CEP, complemento e ponto de referência)

- Detalhamento da ocorrência (narrar o fato ocorrido)
  - tipo de ocorrência (se foi furto ou perda)
  - descrição do que aconteceu (contar resumidamente como o fato ocorreu)
  - relação dos documentos e objetos perdidos/furtados (com o máximo de detalhes possível)

Muito bem, conseguimos vencer esta etapa com sucesso e muita aprendizagem. Você está pronto para prosseguir?

Avançando na prática

Informatizando a portaria

Descrição da situação-problema

Imagine que você é supervisor de segurança em um condomínio de casas que ainda adota um procedimento totalmente manual para controlar a entrada de visitantes. E você estabeleceu o seguinte: quando um visitante chega à portaria, o porteiro deve solicitar o seu documento de identificação, confrontando a foto com a pessoa. Em seguida, deve verificar na "Prancheta Autorizados" se o visitante está previamente autorizado a entrar no condomínio, sendo que essa prancheta é preenchida quando um morador liga para a portaria, autorizando previamente a entrada de visitantes, a qual contém número da casa, nome do morador que autorizou e nome do visitante. Caso o visitante conste na "Prancheta Autorizados", ele só preenche os dados na "Prancheta Visitantes", que são: nome, RG, casa de destino, nome do autorizador, data e hora da entrada e nome dos acompanhantes. Mas, caso não conste, ele primeiro solicita, por telefone, ao morador da residência de destino do visitante, a autorização para entrada no condomínio (para isso, deve consultar a lista telefônica afixada na portaria) e, uma vez autorizada a entrada, ele, então, preenche a "Prancheta Visitantes". Caso não seja autorizada a entrada do visitante, o porteiro não permite que o visitante entre no condomínio. Após tudo isso, ele abre o portão, se for o caso, por meio do controle remoto da portaria, para que o visitante siga seu destino.

Como esse procedimento é muito lento e vem trazendo problemas para a segurança do condomínio, resolveu-se instalar um sistema informatizado na portaria. Para tanto, a empresa contratada para desenvolver o sistema mandou um analista de sistemas para entrevistar o porteiro e, durante a entrevista, o analista de sistemas solicitou que você, o supervisor de segurança, o ajudasse a identificar as entradas, os processamentos e as saídas naquele procedimento, identificando, ainda, o que eram dados e o que eram informações. Você é capaz de ajudá-lo? Então, você se lembra da teoria geral dos sistemas? Identifique as entradas, os processamentos e as saídas esperadas no procedimento com visitantes na portaria do condomínio. Depois, cite os dados e informações envolvidos na atividade.

Resolução da situação-problema

As entradas são: o documento com foto e os dados do visitante, a casa de destino, o telefone do morador, data e a hora da entrada, nome do autorizador, autorização do morador, nome dos acompanhantes. Os processamentos são: consultar a "Prancheta Autorizados", consultar a lista de telefone afixada na portaria, ligar para o morador solicitando autorização, preencher a "Prancheta Visitantes", abrir o portão. Já as saídas são: ambas as pranchetas preenchidas corretamente e os visitantes aos seus respectivos destinos.

Os dados: nome, número do RG do visitante, foto do visitante, casa de destino, nome do autorizador, data e hora da entrada, nome dos acompanhantes.

Informação: telefone do morador, autorização para entrada.

Faça valer a pena

1. Ludwig von Bertalanffy é considerado o principal autor da teoria geral dos sistemas e, segundo ele, os sistemas estão presentes em toda parte no mundo, evidenciando que é fundamental a interação entre pessoas, empresas, países e qualquer outro tipo de organização.

Acerca da definição de sistema enunciada por Von Bertalanffy, assinale a alternativa que contém o conceito correto de sistema.

a) Sistema é tudo aquilo que está a nossa volta e envolve a natureza.

b) Sistema é um conjunto de elementos que formam um todo organizado com um objetivo comum, recebendo entradas, realizando processamentos e produzindo saídas.

c) Sistema é um conjunto de componentes que interagem com o meio externo, sem uma finalidade específica.

d) Sistema é um todo organizado, que processa entradas e saídas, resolvendo uma tarefa genérica.

e) Sistema é um conjunto de componentes que formam um todo organizado, processando entradas e saídas e formando um resultado, que é a retroalimentação.

2. Geralmente, o conceito de sistema está associado aos componentes do sistema, suas entradas, seus processamentos e suas saídas e ao significado de cada um deles para o sistema.
Associe a parte do sistema da coluna da esquerda com seus respectivos significados da coluna da direita.
(1) Componentes
(2) Entrada
(3) Processamento
(4) Saída
( ) São as operações realizadas pelos componentes do sistema para transformar as entradas em saídas.
( ) São as partes que constituem o sistema, podendo também ser subsistemas.
( ) Produto gerado pelo processamento das entradas no sistema ou objetivo comum que levou os componentes do sistema a interagirem entre si.
( ) Tudo aquilo que o sistema deve receber para ser processado e convertido em saída.
a) 3-1-4-2
b) 4-1-3-2
c) 2-1-3-4
d) 1-2-3-4
e) 3-2-4-1

3. Sempre que se aproxima um pleito eleitoral, grande parte dos meios de comunicação, particularmente a televisão, começa a divulgar os resultados de pesquisas eleitorais, sejam elas recentes ou passadas, enfatizando o histórico de pontos de cada candidato, apresentando gráficos e sugerindo tendências. Geralmente com a finalidade de informar o eleitor e permitir que ele possa ter uma visão geral do desempenho dos candidatos para melhorar, definir suas preferências e votar com mais critério e precisão.
Analisando o conteúdo dessas pesquisas apresentadas pela mídia, normalmente são mostrados percentuais de votos dos candidatos, nos seguintes termos: o candidato "A" possuía 8%, foi para 10% e agora está com 13%; o candidato "B" começou com 48%, desceu para 43% e agora se encontra com 38%; já o candidato "C" iniciou com 27%, subiu para 34% e agora atingiu 41%; e assim por diante. Podemos considerar que isso é um exemplo de:
a) conhecimento
b) dado
c) sistema
d) informação
e) sistema de Informação

Seção 1.2

Sistemas de informação nas organizações

Diálogo aberto

Caro aluno, depois do furto de carteiras dos funcionários da Flextram Suporte e Soluções em RH, escritório em que a JRW Defender presta seus serviços de segurança patrimonial, João Wanderson, o inspetor designado para realizar o registro da respectiva ocorrência, retornou da Delegacia de Polícia com as informações necessárias para a confecção de um Boletim de Ocorrência. Ele deve, agora, confrontar os dados que foram levantados pelo vigilante Antônio das Neves, o funcionário que estava no turno em que o fato aconteceu, com aqueles que o escrivão de polícia forneceu, para que João Wanderson pudesse providenciar um BO.

É política da JRW Defender que todo tipo de ocorrência em qualquer local em que preste seus serviços de segurança seja notificado por meio de um documento específico denominado de Relatório de Ocorrência. Esse tipo de relatório servirá para que os gerentes de segurança possam tomar as providências necessárias, dentro dos limites de suas atribuições, permitindo que a informação chegue até a alta administração da JRW. Para tal, o inspetor sabe que tudo começa com o preenchimento em detalhes do Livro de Ocorrências. Então, ele solicitará que o vigilante Antônio realize o mais rápido possível sua correta escrituração. O registro nesse livro, que concentra todos os fatos e eventos dos vigilantes em seus respectivos postos, facilitará a confecção do relatório de responsabilidade de João Wanderson.

O desafio do inspetor de segurança será elaborar um bom relatório, que contemple todos os dados que sejam relevantes e que possam ser transformados em informações que sustentem a tomada de decisão dos diretores da empresa, lembrando que a JRW está em fase de revisão de todos os seus sistemas de informação. Ela deseja modificar o fluxo da informação e implantar sistemas com suporte da tecnologia da informação, que permitam tomar as decisões de forma ágil.

João, como está na empresa há algum tempo, já percebeu que determinadas ocorrências podem ter como consequência a

substituição dos vigilantes envolvidos, a modificação das procedimentos e rotinas dos agentes de segurança e a sugestão de inserção de outros equipamentos como câmeras e sensores, dentre outras, tudo visando evitar que acontecimentos de mesma natureza ocorram novamente.

Então, caro aluno, na posição de João Wanderson, quais seriam os principais dados que você faria constar no Relatório de Ocorrências? O que seria tão relevante para que todo o sistema de informações pudesse ser aperfeiçoado? Para solucionar essa parte da situação-problema, será necessário conhecer um pouco sobre os impactos e vantagens dos sistemas de informação nas organizações, assim como conhecer os níveis e classificações dos SI, bem como as modalidades dos sistemas. Como esse relatório contemplará uma quantidade maior de informações, ele servirá sobremaneira para a elaboração do Boletim de Ocorrência, lembrando a você que essa é mais uma parte do produto, o qual deverá ser entregue ao final da unidade didática. Mãos à obra. Vamos, então, elaborar um bom relatório de ocorrências!

Não pode faltar

Muito bem, vamos prosseguir nossos estudos, buscando identificar os impactos e vantagens do emprego dos sistemas de informação, principalmente aqueles baseados na tecnologia da informação e comunicação, nos processos e atividades das organizações de uma forma geral. Lembrando de que nós devemos enxergar a organização, segundo a abordagem sistêmica e não como um organismo isolado e autossuficiente.

Uma organização pode ser conceituada como sendo um arranjo de profissionais, processos, tecnologias e todos os outros recursos que interagem entre si e com o ambiente externo, como clientes, fornecedores, concorrentes, economia, acionistas, órgãos de fiscalização, dentre outros, tudo com a finalidade de alcançar um conjunto de objetivos. A atividade de uma organização normalmente envolve pessoas, máquinas, recursos financeiros, insumos materiais, dados, informações, conhecimentos e decisões. Em linhas gerais, os recursos financeiros, a mão de obra e os insumos materiais caracterizam as entradas, que passam a ser processadas pelas máquinas e subsistemas da organização, sendo transformadas nas

saídas, que são produtos e serviços com grande valor agregado, por meio dos quais a organização espera atingir seus objetivos (STAIR; REYNOLDS, 2015).

Nesse contexto, enquadram-se os sistemas de informação que também são parte da organização e estão diretamente envolvidos em todas as atividades organizacionais, seja atuando no fornecimento de entradas – disparando pedido de insumos para os fornecedores -, seja apoiando o processamento – através da programação das máquinas -, ou produzindo saídas – relatórios de qualidade da produção. Assim, os sistemas de informação permeiam toda a estrutura da organização, atendendo as diferentes necessidades de informação dos mais diversos segmentos da empresa.

Até meados do século passado, o ambiente que envolvia grande parte das organizações era muito restrito, tanto geograficamente, isto é, a empresa coabitava, produzia e concorria com outras empresas do mesmo bairro ou cidade, quanto em termos de aquisição de conhecimento, pois era muito difícil se obter novas informações e até mesmo ampliar a visibilidade da empresa, tudo isso decorrente dos rudimentares meios de comunicação da época. Assim sendo, as mudanças eram muito mais demoradas e existiam empresas que atravessavam décadas sobrevivendo da fabricação do mesmo produto, com as mesmas características e com a mesma qualidade.

No entanto, esse cenário foi radicalmente transformado nos últimos anos e, hoje em dia, vivemos num mundo globalizado e totalmente conectado, e isso faz com que as organizações passem a interagir com um ambiente de dimensões intercontinentais, transformando o mercado em um universo assustadoramente competitivo e hostil. Essa mudança de cenário fez com que as organizações sentissem a necessidade de se adaptarem aos novos tempos, em que as mudanças acontecem muito rapidamente e de forma inexorável, ou seja, inevitavelmente tudo isso impulsionado pelo largo emprego das informações, como vimos anteriormente.

Exemplificando

No início da década de 1980, um supermercado, mesmo sendo de grande porte, abastecia seu estoque através de pedidos preenchidos manualmente pelo gerente, a partir da conferência física dos itens no estoque e entregues pessoalmente ao fornecedores. Esses itens saíam

do estoque e recebiam uma etiqueta com o preço, de uma maquininha muito rudimentar chamada etiquetadora e eram colocados nas prateleiras; o cliente, por sua vez, pegava os produtos nas prateleiras, colocava em seu carrinho e passava pelo caixa; no caixa, a operadora digitava num teclado numérico da caixa registradora o preço de cada um dos produtos e simultaneamente era impressa uma lista com o preço do produto e no final o total da venda; e, para finalizar, o cliente fazia o pagamento, que poderia ser em dinheiro ou cheque. Hoje em dia, em qualquer supermercado de médio porte, o gerente nem precisa fazer pedido, e muitos não possuem estoque além das prateleiras. Está tudo automatizado. O cliente pega o produto na prateleira e consulta o preço em um dos terminais de consulta existentes na loja através do código de barras impresso na embalagem pelo fabricante do produto e esse mesmo código está cadastrado no sistema do supermercado, permitindo controlar todo estoque, preço, validade etc., do produto. Quando o cliente passa no caixa, a operadora simplesmente vai passando o código de barras dos produtos no leitor e finaliza com o pagamento, que pode ser em dinheiro, cheque, cartão de débito ou crédito, cartões de convênios, vales-compra, à vista, parcelado, financiado, com cartão do supermercado ou qualquer outra bandeira. Além disso, a passagem pelo caixa abate a quantidade de produtos vendidos no estoque, permitindo a emissão automática de pedidos aos fornecedores e, às vezes, até fazendo o pagamento também. Vejam que mudança significativa ocorreu no negócio de um simples supermercado, por causa do emprego dos sistemas de informação.

Diante dessa nova realidade, as empresas se viram obrigadas a mobilizarem-se em busca de soluções que lhes permitissem obter vantagens para sobreviver nesse moderno e adverso ambiente de mercado. Fruto dessa busca, as empresas passaram a investir pesado no desenvolvimento, implantação e manutenção de sistemas de informação, já que a informação foi o grande pivô dessa revolução. Em virtude dessa busca, as organizações obtiveram bons resultados, ou seja, conseguiram gerenciar melhor suas funções básicas; agilizar e otimizar seus processos; acelerar a implantação de melhorias; reduzir custos operacionais; aprimorar a qualidade dos seus produtos; aumentar a produtividade; ampliar seus relacionamentos com o ambiente externo, incrementando, principalmente, seu conjunto de clientes e compartilhando experiências com outras empresas parceiras. Dessa forma, as organizações foram conseguindo se

adaptar aos tempos modernos e acompanhar o ritmo intenso dos acontecimentos e das mudanças no mercado consumidor.

De maneira geral, o impacto dos sistemas de informação nas empresas foi muito positivo, porque promoveu o desenvolvimento das organizações, alterando, inclusive, os ambientes de trabalho, pois possibilitaram a execução de tarefas mais complexas e com maior agilidade; promoveu o surgimento de novos produtos e serviços, beneficiando diretamente os consumidores e facilitando a vida das pessoas; e aumentou significativamente a produção de conhecimento, impactando até no surgimento de novas profissões para atender às demandas produtivas contemporâneas.

Podemos perceber, então, baseados em Laudon e Laudon (2007), que os sistemas de informação trouxeram várias vantagens para as empresas, sendo as principais delas as seguintes:

- Excelência operacional: produzir em maior quantidade, com mais eficiência, melhor qualidade e de forma mais ágil.

- Desenvolvimento de novos produtos e serviços: identificar mais rápido e de forma mais precisa quais são as novas demandas do mercado consumidor e fazer frente a essa demanda de forma oportuna e vantajosa.

- Relacionamento com o cliente: estar constantemente em contato com o cliente, atendendo suas demandas, prestando auxílio em caso de necessidade, ouvindo suas reclamações e sanando seus problemas, além de estabelecer uma relação de fidelidade com a empresa e seus produtos.

- Melhoria do processo decisório: permitir que os atores do processo decisório da empresa tomem suas decisões de forma mais precisa e com maior agilidade, baseados em informações claras e concisas.

- Obter vantagem competitiva: estar sempre um passo à frente da concorrência, em termos de qualidade, inovação e satisfação do cliente.

- Sobrevivência: a empresa deve conseguir se manter no mercado no qual atua, praticando seu negócio e produzindo bens e serviços capazes de atingir seus objetivos.

Reflita

A informação e os sistemas de informação realmente alteraram a rotina das organizações? Será que as mudanças foram tão significativas assim? O que acontece hoje em dia que era totalmente diferente no passado, quando não existiam os sistemas de informação? Será que existe algum tipo de organização que sobrevive atualmente sem o emprego de sistemas de informação?

Partiremos agora para aprender níveis de atuação, classificação e modalidades de sistemas de informação, mas, para tanto, precisamos entender um pouco mais sobre a estrutura das organizações.

A organização básica de uma empresa tradicional envolve as funções empresariais elementares, desempenhadas pelos departamentos, quais sejam: produção, vendas, contabilidade, recursos humanos, entre outros; e uma hierarquia funcional dividida em níveis, que são: operacional, técnico ou de conhecimento, tático e estratégico (Figura 1.4). Explicando melhor os níveis: no nível operacional, estão os trabalhadores que fabricam os produtos ou fazem a prestação de serviços, os operários; no nível técnico ou de conhecimento, estão os trabalhadores que cuidam dos dados através da documentação, secretárias e auxiliares administrativos, assim como os trabalhadores que projetam os produtos e serviços, engenheiros e arquitetos; no nível tático, estão os gerentes que conduzem as equipes nas atividades diárias para executar as tarefas conforme o planejamento da empresa; e, no nível estratégico, está a alta administração da empresa responsável pelas decisões estratégicas que conduzirão a organização à consecução de seus objetivos (LAUDON; LAUDON, 2007).

Figura 1.4 | Estrutura empresarial básica

Fonte: elaborada pelo autor.

Os sistemas de informação atingem todas as funções e níveis hierárquicos da empresa e, como base nesse preceito, são agrupados por vários critérios.

Os sistemas de informação que atendem às necessidades dos departamentos de uma empresa são, então, **classificados com base nas funções básicas da empresa** e podem ser:

– Sistema de Informação de Vendas e Marketing.

– Sistema de Informação Financeiro.

– Sistema de Informação Contábil.

– Sistema de Informação de Recursos Humanos.

– Sistema de Informação de Produção.

Os sistemas de informação também podem ser **classificados por nível de atuação dentro da estrutura da empresa**. Nesse caso, não importa a que departamento da empresa o sistema está apoiando e sim qual é o nível hierárquico da empresa que está recebendo o suporte do sistema. São classificados em:

- Sistemas de Processamento de Transações (SPT)
  - – Atendem ao nível operacional.
  - – Registram as operações cotidianas necessárias para a execução do negócio da empresa.
  - – Exemplos: processamento de pedidos, controle de materiais, folha de pagamento, contas a pagar e registro de funcionários.
- Sistemas de Automação de Escritório (SAE)
  - – Estão no nível de conhecimento.
  - – Permitem que os trabalhadores dos dados processem os documentos da organização e executem os fluxos de dados.
  - – Normalmente, são pacotes de automação de escritório.
  - – Exemplos: editores de texto, calendários eletrônicos, protocolos eletrônicos.
- Sistema de Trabalho do Conhecimento (STC)
  - – Também atendem ao nível de conhecimento.
  - – São específicos para os engenheiros e arquitetos de produto.
  - – Exemplos: engenharia assistida por computador.
- Sistema de Informação Gerencial (SIG)

– Dão suporte ao nível tático ou gerencial da empresa.

– Reportam as operações básicas da empresa através de relatórios e estatísticas sobre o desempenho da organização, permitindo o acompanhamento e controle dos meios de produção, da produção propriamente dita e dos produtos e serviços gerados.

– Exemplos: administração de vendas, controle de estoque, controle de orçamento, análise de produção.

• Sistema de Apoio à Decisão (SAD)

– Também dão suporte ao nível tático ou gerencial.

– Auxiliam os gerentes a tomarem decisões que estão fora dos procedimentos estruturados da empresa.

– Exemplos: programação da produção, análise de custos e análise de vendas.

• Sistema de Apoio ao Executivo (SAE)

– Enquadram-se no nível estratégico da empresa.

– Disponibilizam todas as informações necessárias ao processo decisório da alta administração da empresa, englobam dados e informações internas e externas da empresa e executam processamentos customizados.

– Exemplos: planejamento de lucros, tendências de vendas por período, pesquisas dos concorrentes.

Os sistemas de informação ainda podem ser **classificados de acordo com a integração dos sistemas** da empresa, que, segundo Franco, Rodrigues e Casela (2013), simplificam os processos de negócio e tornam as organizações mais eficientes. A classificação é a seguinte:

• Sistema de Planejamento de Recursos Empresariais (ERP – Enterprise Resource Planning)

– É o principal integrador de sistemas em uma empresa, englobando desde os sistemas básicos de coleta de dados até os complexos sistemas de apoio ao executivo, reunindo todas as áreas como marketing, produção, recursos humanos e contabilidade.

• Sistema de Gerenciamento da Cadeia de Suprimento (SCM – Supply Chain Management)

– É composto pela integração de todos os sistemas que

envolvem os fornecedores, estoques, transportes, lojas e tudo mais envolvido na cadeia de suprimento, com o objetivo de distribuir produtos e serviços nas quantidades corretas e no prazo, reduzindo, é claro, o custo disso tudo.

• Sistema de Gerenciamento do Relacionamento com o Cliente (CRM – Customer Relationship Management)

– Combina todos os sistemas que estão voltados para os clientes, apoiando a empresa na manutenção do relacionamento com os clientes, visando atender todas as suas necessidades e coletar dados para o aperfeiçoamento e inovação nos produtos.

• Sistema de Gestão do Conhecimento (KM – Knowledge Management)

– São sistemas baseados na integração das informações armazenadas pela empresa, visando disponibilizá-las de forma fácil e rápida, permitindo o compartilhamento do aprendizado entre todos os setores da organização.

• Sistema de Inteligência de Negócio (BI – Business Intelligence)

– Integra os sistemas com foco nos Sistemas de Apoio à Decisão (SAD) e Sistemas de Apoio ao Executivo (SAE), visando fornecer informações para dar suporte ao processo decisório nos níveis tático e estratégico.

Assimile

Classificação dos sistemas de informação

Quanto à área funcional:

- Sistema de Informação de Vendas e Marketing
- Sistema de Informação Financeiro
- Sistema de Informação Contábil
- Sistema de Informação de Recursos Humanos
- Sistema de Informação de Produção

Quanto ao nível hierárquico:

- Sistemas de Processamento de Transações (SPT)

- Sistemas de Automação de Escritório (SAE)
- Sistema de Trabalho do Conhecimento (STC)
- Sistema de Informação Gerencial (SIG)
- Sistema de Apoio à Decisão (SAD)
- Sistema de Apoio ao Executivo (SAE)

Quanto à integração:

- Sistema de Planejamento de Recursos Empresariais (ERP)
- Sistema de Gerenciamento da Cadeia de Suprimento (SCM)
- Sistema de Gerenciamento do Relacionamento com o Cliente (CRM)
- Sistema de Gestão do Conhecimento (SGC)
- Sistema de Inteligência de Negócio (BI)

Encerrando a nossa exposição, veremos agora alguns exemplos de sistemas de informação na segurança pública e privada.

Como exemplo de sistema de informação na segurança pública, podemos citar a Rede Nacional de Integração de Informações de Segurança Pública, Justiça e Fiscalização (Rede Sinesp Infoseg), que tem como objetivo integrar os dados de criminosos, de armas de fogo, de automóveis, de pessoas físicas, de pessoas jurídicas e outros, de todos os estados do País, disponibilizando esses dados para os órgãos de segurança pública e para o judiciário, através da Internet.

A Rede Sinesp Infoseg integra todas as bases de dados de todas as unidades federativas com as bases de dados federais, disponibilizando uma completa massa de dados e possibilitando a integração rápida e confiável entre esses sistemas. Na prática, a Rede Sinesp Infoseg auxilia o trabalho das polícias, do judiciário, dos órgãos de fiscalização e dos órgãos de inteligência no combate ao crime, permitindo a troca de informações entre essas entidades, otimizando e agilizando a execução de investigações, prisões, aplicação de multas, julgamentos e outras atividades.

Pesquise mais

Para ampliar seus conhecimentos sobre essa rede tão importante, procure saber um pouco mais sobre a Rede Infoseg. Disponível em: <http://www.infoseg.gov.br>. Acesso em: 12 abr. 2017.

Na segurança privada, podemos citar como exemplo de emprego dos sistemas de informação os sistemas de controle de acesso que encontramos quando vamos entrar em um banco, um prédio de escritórios, um condomínio de casas, um clube ou em uma empresa. Normalmente, esse tipo de sistema tem a função de liberar, ou não, o acesso de pessoas cadastradas no sistema, mantendo um histórico de circulação e contribuindo sobremaneira para a segurança do local e do patrimônio privado. Em linhas gerais, são compostos por cartões com identificação por proximidade (RFID), leitores biométricos, catracas, cancelas, portões automáticos, centrais de alarme, câmeras, sensores, sirenes, gravadores DVR, interfones e muitos outros equipamentos de segurança, todos eles interligados por sistemas de informação computadorizados, funcionando de forma conjunta na vigilância do perímetro da instalação e permitindo o total controle da circulação no interior da propriedade. O mercado de segurança privada oferece soluções de controle de acesso, tanto na forma de produtos como na de serviços.

Pesquise mais

Saiba mais sobre sistemas de informação na segurança privada pesquisando nos sítios das empresas que comercializam produtos e serviços de segurança na Internet. Seguem alguns como sugestão:

Disponível em: <http://www.k2seguranca.com.br>. Acesso em: 17 abr. 2017.

Disponível em: <http://secticom.com.br>. Acesso em: 17 abr. 2017.

Disponível em: <http://grupozanardo.com.br>. Acesso em: 17 abr. 2017.

Disponível em: <https://www.youtube.com/watch?v=DVhNkK65f6>. Acesso em: 17 abr. 2017.

Como você pode ver, caro aluno, o nosso assunto é bastante extenso. Mas não acaba aqui, não. Ainda temos muito o que estudar. Sigamos em frente!

Sem medo de errar

Vamos à nossa solução, então!? Relembramos que, na posição do João Wanderson, você precisava levantar quais seriam os principais dados para constar no Relatório de Ocorrências e sugerir o que seria relevante para que todo o sistema de informações pudesse ser aperfeiçoado.

Então, primeiramente, vamos enunciar quais seriam os principais dados para constar em um relatório de ocorrências, lembrando que os dados constam do contexto de aprendizagem e são fictícios. Veja eles:

– A empresa prestadora do serviço de segurança. Ex.: EMPRESA: JRW Defender.

– A empresa no qual o serviço está sendo prestado, ou posto de serviço. Ex.: POSTO DE SERVIÇO: Flextram Suporte e Soluções em RH.

– Endereço do posto de serviço. Ex.: ENDEREÇO DO SERVIÇO: Rua Bandeirantes, 345 – Centro – Curitiba/PR, CEP 34.876-945.

– Data do serviço. Ex.: DATA: 17 de outubro de 2017 (segunda-feira).

– Função, nome e identificação dos integrantes da equipe de serviço. Ex.: PESSOAL DE SERVIÇO: vigilante Antônio das Neves, registro: 12345678-9.

– Relação de todo o material de apoio existente no posto de serviço, especificando a numeração de patrimônio se existir. Ex.: MATERIAL: revólver calibre 32 nº 234, rádio comunicador HT nº 23, lanterna, caneta, livro de registro, molho de chaves.

– Nome do responsável pelo turno de serviço anterior e que passou o serviço para o responsável atual. Ex.: RECEBIMENTO DE SERVIÇO: vigilante Carlos Cândido, registro: 56709834-2.

– Relato dos fatos ocorridos durante o turno do serviço, devendo contemplar os dados levantados na seção anterior, ao alinhar com os dados necessários para o BO. Ex.: OCORRÊNCIAS: relate o fato objetivamente, mas com a maior riqueza de detalhes possível (principalmente quando se tratar de algum tipo de documento), buscando responder às perguntas: Quem? Autor do ato; Quê? O fato ocorrido; Quando? Data e hora da ocorrência; Onde? Local exato da ocorrência; Como? O modo pelo qual a ocorrência se desenvolveu; e Para quê? O objetivo da ação.

- Nome do responsável pelo turno de serviço posterior e que recebeu o serviço do responsável atual. Ex.: PASSAGEM DO SERVIÇO: vigilante Demétrio Damasceno, registro: 73561239-5.

Agora, podemos sugerir uma ideia para que o sistema de informações possa ser aperfeiçoado, que poderia ser algo do tipo: seria interessante que esse relatório fosse preenchido em um formulário eletrônico de um sistema de informação específico para essa finalidade, no nível operacional, como um Sistema de Processamento de Transações (SPT). Assim, os dados ali lançados poderiam ser automaticamente disponibilizados para os demais níveis, integrando Sistemas de Informações Gerenciais (SIG) e Sistemas de Apoio à Decisão (SAD), que dariam suporte aos níveis mais altos da organização, agilizando a transmissão dessas informações e facilitando a ação de supervisores, inspetores (como o João Wanderson) e gerentes, que, por sua vez, poderiam dar uma resposta mais rápida e eficiente para o cliente, otimizando os processos da JRW e melhorando o negócio da empresa.

Avançando na prática

Conhecendo os SI em segurança

Descrição da situação-problema

Carlos e Danilo são amigos há muito tempo e se formaram juntos no curso de formação de vigilante da segurança privada. Após a conquista do tão esperado diploma, os amigos seguiram suas vidas e iniciaram suas carreiras profissionais em duas empresas distintas. Carlos foi trabalhar como Analista de Segurança, no Departamento de Segurança Patrimonial da FABTEC (uma indústria de computadores), desempenhando o cargo de auxiliar no planejamento de gerenciamento de risco, que é totalmente suportado por um sistema de informação. Já o Danilo ingressou na Total Seguro (empresa do ramo de segurança privada) como inspetor de segurança, mas presta serviço na Goodmeat (indústria de alimentos), onde a Total Seguro presta serviço de segurança pessoal e patrimonial, e trabalha com um sistema de informação de monitoramento das pessoas que circulam na fábrica.

Pois bem, diante dessas informações e com base nos seus conhecimentos sobre o emprego dos sistemas de informação nas organizações, você seria capaz de classificar os SI utilizados por Carlos e Danilo e citar algumas vantagens que esses SI trazem para as empresas que o utilizam?

Resolução da situação-problema

O SI utilizado por Carlos pode ser classificado quanto à sua função básica na empresa, já que a FABTEC possui um Departamento de Segurança Patrimonial, como Sistema de Informação de Segurança Patrimonial; e também pode ser classificado quanto ao nível de atuação como Sistema de Informação Gerencial (SIG), uma vez que permitirá a um gerente controlar os riscos de segurança da empresa. As vantagens do SI de Planejamento de Gerenciamento de Risco seriam: melhorar a administração da segurança; otimizar a alocação de recursos no tratamento dos riscos; sistematizar a prevenção de incidentes e outros. Falando agora do SI utilizado por Danilo, poderíamos classificá-lo, quanto à sua função básica na empresa, como um Sistema de Processamento de Transações (SPT), já que atende ao nível operacional, ou seja, ao monitoramento das pessoas, nível de coleta de dados e que registra uma atividade cotidiana da empresa. As vantagens desse SI seriam: mitigar problemas na produção dos alimentos, tais como contaminação ou adulteração; evitar eventuais vazamentos de informação, devido à circulação de pessoas por áreas não autorizadas; a assegurar a produtividade no chão de fábrica, restringindo o acesso a essas áreas.

Faça valer a pena

1. Na década de 1990, houve uma verdadeira febre do uso dos pagers ou bips, pequenos aparelhos que permitiam a troca de mensagens de texto entre os usuários. Mas, antes que os anos 2000 chegassem, os pagers já tinham praticamente sido extintos do mercado de telemóveis. Isso devido ao surgimento dos telefones celulares. Processo semelhante ocorreu com os netbooks, aqueles pequenos computadores com poucos recursos de hardware e muita conectividade, que tiverem seu ápice por volta de 2010 e hoje já estão totalmente esquecidos em virtude do aparecimento dos tablets.

Analisando essa situação e refletindo sobre as atividades das empresas fabricantes desses equipamentos, assinale a alternativa que apresenta uma medida tomada por essas empresas para conseguirem sobreviver nesse mercado tecnológico da "Era da Informação".

a) Mudaram de ramo de atividade.

b) Passaram a fabricar pagers e depois tablets.

c) Investiram pesado em sistemas de informação.

d) Demitiram seus funcionários e renovaram seus quadros profissionais.

e) Investiram no mercado financeiro para garantir rentabilidade, mesmo com todas as adversidades do mercado.

2. Os sistemas de informação podem ser classificados de acordo com a função, o nível ou a integração com que atuam nas organizações, ou seja, sua classificação está diretamente relacionada com a estrutura da empresa e com a sua hierarquia. Com base nesses conhecimentos, analise as afirmativas a seguir.

I – Um Sistema de Apoio ao Executivo (SAE) disponibiliza as informações necessárias ao processo decisório da alta administração da empresa e engloba dados e informações internos e externos.

II – Um Sistema de Planejamento de Recursos Empresariais (ERP) pode ser considerado o principal integrador de sistemas em uma empresa, englobando desde os sistemas básicos de coleta de dados até os complexos sistemas de apoio ao executivo.

III – Um Sistema de Informação de Produção recebe essa classificação pelo nível de atuação dentro da estrutura da empresa.

IV – Os Sistemas de Processamento de Transações (SPT) atuam no nível tático das empresas e podem ser exemplificados pelos sistemas de processamento de pedidos e pelos sistemas de controle de materiais.

Está correto somente o que se afirma em:

a) I e II;

b) I e III;

c) I, II e III;

d) II e IV;

e) I, III e IV.

3. No mercado de softwares voltados para a área de segurança, é fácil encontrar sistemas como o GesOper, que é um ERP concebido para maximizar os resultados de empresas de segurança patrimonial e outros ramos por meio da informatização das atividades de marketing, operacional, de recursos humanos, de finanças e gerenciais. Esse tipo de sistema pode trazer benefícios como o controle total sobre as diversas escalas de serviço; comunicação com sistemas da Polícia Federal, agilizando medidas corretivas e eliminando retrabalho de digitação; e operação em *real-time*, garantindo maior presteza e oportunidade das informações (SOLLUÇÃO, 2017).

O GesOper pode ser considerado um exemplo de sistema de informação empregado na:

a) segurança operacional

b) segurança pública

c) segurança pessoal

d) segurança de gestão

e) segurança privada

Seção 1.3

Conceitos de tecnologia da informação e sua aplicação na segurança pública e privada

Diálogo aberto

Muito bem, caro aluno, você está quase finalizando a solução de todos os desafios vivenciados por João Wanderson, mas a problemática principal ainda não foi solucionada. Embora João tenha obtido na delegacia as informações necessárias para realização de um Boletim de Ocorrência – BO e, ainda, tenha confeccionado um completo Relatório de Ocorrências que muito servirá para elucidar o furto de materiais particulares dos funcionários no banheiro masculino da Flextram Suporte e Soluções em RH, ainda falta a elaboração do BO, propriamente dito.

João não é nenhum *nerd* em informática, mas tem ouvido falar bastante sobre esse negócio de tecnologia de informação e sabe que, cada vez mais, ela está presente na vida das pessoas. Sabe, também, que a JRW Defender está implantando um monte de novas tecnologias, como softwares, aplicativos e sistemas. João escutou outro dia do seu diretor regional, que a empresa iria investir pesado em novos computadores e bancos de dados, aumentando até a banda larga da companhia, para que a comunicação fosse realizada pela rede mundial de computadores, que todo mundo tem acessado ultimamente.

João tem procurado aprender sozinho o que pode para se atualizar nessas questões de tecnologia, acessando todos os dias os portais de busca. Como ele tinha de registrar o BO do furto dos funcionários, foi até o Google e verificou que poderia ser realizado pela Internet, caso cada pessoa envolvida realizasse o seu próprio registro. O que facilita é que, no escritório da Flextran, todos os colaboradores têm acesso à rede. João pensou em facilitar esse registro sem que todos tivessem de ir à delegacia, mas ele teria de conhecer em detalhes todos os dados e passos para orientar cada colaborador a como realizar o registro do BO em uma Delegacia Eletrônica.

Pois bem, o desafio final de João Wanderson será elaborar um formulário para o Boletim Eletrônico disponível na Internet. A finalidade desse formulário será facilitar e orientar o processo de registro de cada funcionário. João, fazendo com que o funcionário preencha o formulário e indicando o link da Internet da Delegacia Eletrônica, em que o colaborador realizará o seu registro individual, permitirá que sejam efetuados todos os registros em BO, relativos ao furto que ocorreu com os funcionários da Flextram.

Para a confecção desse formulário para o Boletim Eletrônico disponível na Internet, o qual finalizará a elaboração do seu produto entregável, você, aluno, necessitará conhecer conceitos sobre aplicativos e software, bem como as aplicações de TI na segurança pública e privada. Vamos lá finalizar nossa tarefa?

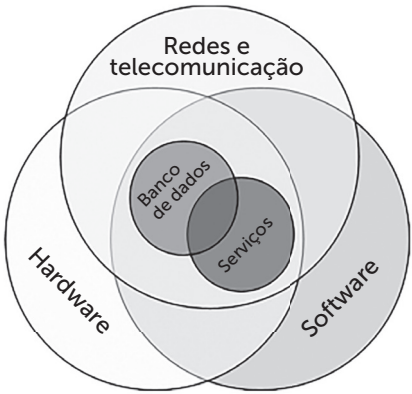
Não pode faltar

A partir de agora, iremos estudar conceitos relacionados às tecnologias da informação (TI) e à aplicação das TI na segurança pública e privada. Para tanto, vamos inicialmente entender o que é TI e o que é uma infraestrutura de TI, para depois ver a aplicação de TI na segurança.

O conceito de TI é muito simples: denomina-se TI o conjunto de todos os recursos tecnológicos necessários para produzir, armazenar e transmitir informação. É lógico que esse conjunto de recursos tecnológicos envolve determinados tipos de tecnologia e são justamente esses tipos de tecnologia que compõem uma infraestrutura de TI, que dá suporte às aplicações que fornecem sustentação aos processos informacionais de uma organização. Uma infraestrutura de TI bem planejada permite que uma organização realize suas tarefas – baseadas em informação – com eficiência e agilidade, proporcionando um equilíbrio entre processos, pessoas e tecnologia (ARAÚJO, 2010).

Segundo Laudon e Laudon (2007), os elementos que compõem a infraestrutura de TI são: hardware, software, telecomunicações e redes, bancos de dados e serviços de tecnologia (vide Figura 1.5).

Figura 1.5 | Elementos da infraestrutura de TI



Fonte: elaborada pelo autor.

Agora que você entendeu o conceito, vamos ver o que significa cada um dos elementos da infraestrutura de TI.

O **hardware** tem a finalidade de executar o processamento computacional, armazenamento e entrada e saída de dados. É composto pelos computadores, servidores, notebooks, celulares, palmtops, GPS, impressoras, pen drives, cancelas, catracas, sensores, câmeras e muitos outros.

O **software** é aquele programa que permite que um computador realize uma tarefa, sendo composto por um conjunto de instruções ou comandos organizados em uma sequência lógica, que visam instruir o computador.

As **telecomunicações e redes** propiciam a conexão entre computadores distribuídos geograficamente, de maneira a permitir a comunicação entre eles, possibilitando a troca de informações e de processamento. Um dos maiores benefícios das redes de computadores é o compartilhamento de recursos, tais como impressoras, dados, aplicações, acesso à Internet e outros (MARÇULA; FILHO, 2008).

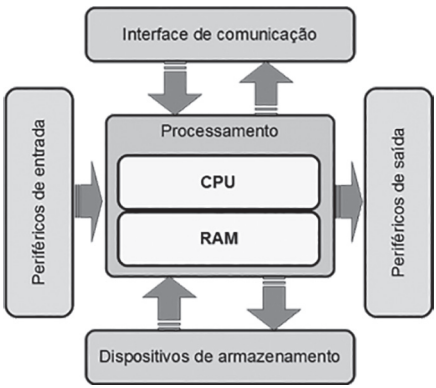
Os **bancos de dados**, por sua vez, têm a finalidade de organizar, gerenciar, processar e recuperar os dados e as informações de uma organização, permitindo acessá-las de forma rápida e segura.

Por fim, os **serviços de tecnologia** permitem aos usuários aproveitarem os recursos tecnológicos para sua produção e execução

de seus processos de trabalho, por exemplo, correio eletrônico (e-mail), acesso à Internet, páginas web, segurança (*firewall* e antivírus), armazenamento (servidor de arquivos e backup), aplicação (sistemas corporativos), dentre vários outros.

Muito bem. Passaremos a estudar cada um desses elementos separadamente, exceto os serviços de tecnologia. Começaremos pelo hardware, que podemos definir como sendo todos os equipamentos usados para entrada, processamento e saída de dados em um sistema de informação. Normalmente, o hardware pode ser entendido como um sistema computacional, possuindo uma unidade de processamento, unidades de entradas e saída de dados, dispositivos de armazenamento e um meio de comunicação com a rede. Comumente, chamamos de periféricos aqueles dispositivos que fazem entrada e saída de dados no sistema computacional (vide Figura 1.6).

Figura 1.6 | Esquema simplificado de um sistema computacional



Fonte: adaptada de Stair e Reynolds (2015, p. 101).

Com base nesse esquema de um sistema computacional, podemos estudar os equipamentos de hardware, que são:

Processadores: também chamados de microprocessador ou CPU (Central Processing Unit ou Unidade Central de Processamento), são responsáveis por processar os dados e informações, obedecendo aos comandos e instruções contidas no programa, que podem fazer a CPU somar dois números ou enviar uma informação para a placa de rede, por exemplo. Via de regra, o desempenho dos processadores é definido pelo seu

clock, que indica a frequência de bits processados, ou seja, quanto maior for o clock, mais rápido é o processador. Ex.: AMD Ryzen R7 1800X 3,6GHz ou o Intel Core i7-7920HQ 4,1Ghz.

Memórias RAM: conhecidas como memória principal ou memória de acesso rápido, as memórias RAM (Random Acess Memory) são encarregadas de armazenar as informações que estão em uso pelo processador, proporcionando um rápido acesso aos dados, isto é, quando abrimos um aplicativo gravado no HD do computador, ele é "carregado" na RAM, permitindo que o processador "leia" esse aplicativo a partir da memória rápida. A RAM é uma memória dita volátil, porque os dados gravados nela são perdidos quando o computador é desligado. As RAM variam de acordo com o seu tipo, capacidade e clock. Ex.: DDR3 8GB 1866Mhz, DDR3 4GB 1333Mhz.

Dispositivos de armazenamento: armazenam dados mesmo com o sistema computacional desligado. Também são conhecidos como memória secundária e são muito mais lentos que a memória principal. Existem diversas tecnologias para armazenamento de dados, variando em tipo, capacidade e velocidade de leitura/escrita. Ex.: HD (disco rígido), SSD (disco de estado sólido), pen drives, cartões SD, unidades de fita, DVD/CD/BluRay, *storage* e muitos outros.

Periféricos de entrada: a missão desses dispositivos é coletar dados e informações e introduzi-los no sistema computacional, convertendo os dados do homem para a máquina e vice-versa e, também, recuperar informações dos dispositivos de armazenamento. Ex.: teclado, mouse, microfone, scanner, câmera, sensor de infravermelho, leitor de RFID, leitor de código de barras, leitor biométrico etc.

Periféricos de saída: a função deles é mostrar os resultados do processamento, fazendo uma interface com o usuário ou outros sistemas. Ex.: monitor, impressoras, caixas de som, fones de ouvido, cancelas, alarmes, sirenes e por aí vai.

Periféricos de entrada/saída: existem periféricos que podem fazer as duas funções, enviando e recebendo dados e normalmente

são as tecnologias mais modernas. Ex.: impressoras multifuncionais (imprimem e scaneiam), telas touch (exibem imagens e capturam o toque), discadora digital (recebe um número e disca para um telefone) e catracas (leem cartões e liberam acesso).

Interface de comunicação: possibilitam a comunicação de dados entre sistemas computacionais ou dispositivos distintos, através de uma rede de telecomunicações. Ex.: placa de rede, *hub, switch*, roteador, cabos, conectores, e assim por diante.

Computadores/similares: são sistemas computacionais completos, mas que podem ser integrados a outros sistemas computacionais maiores ou mais complexos. Ex.: tablets, smartphones, PDAs e outros.

Obs.: Existe também um tipo de hardware que é integrador entre todos os outros dispositivos, possibilitando que os bits de dados circulem de um para o outros; são as conhecidas " placas-mãe" ou "motherboard" ou ainda "mainboard", responsáveis pela interconexão de todas as partes que formam um sistema computacional, ou seja, HD, RAM, teclado, mouse, placa de vídeo, placa de rede, scanner, impressora, leitor de SD, enfim, todos os periféricos precisam ser conectados à "placa-mãe".

Prosseguindo, estudaremos os softwares, que são a parte lógica de um sistema computacional e são compostos por (i) um conjunto de instruções ou programas, escritos em alguma linguagem de programação, (ii) por estruturas de dados que manipulam as informações e (iii) pela documentação que especifica os programas e descreve a sua operação (MARÇULA; FILHO, 2008).

Assimile

Linguagem de programação é o vocabulário de expressões codificadas utilizadas para determinar as operações a serem realizadas pelo sistema computacional. Um conjunto de instruções em uma sequência lógica forma o código-fonte de um software, que, após ser compilado ou interpretado, dará origem ao programa executável. Exemplos: C++, Java, PHP, ASP, Delphi e Visual Basic.

Uma questão muito importante que envolve o mundo dos softwares e a licença de uso. Pode-se dividi-los praticamente em dois grupos, a saber:

Softwares livres: são softwares licenciados sob a GPL (Generic Public License ou Licença Pública Genérica), que determina 4 (quatro) liberdades do usuário para com o software, as quais definem o conceito de software livre, ou seja, software livre é o software que possui as quatro liberdades da GPL.

Pesquise mais

Saiba tudo sobre a GPL, acessando *Licenças*, disponível em: <https://www.gnu.org/licenses/licenses.pt-br.html>. Acesso em: 20 abr. 2017.

Softwares proprietários: são aqueles em que o software está licenciado com direitos exclusivos para o produtor (direitos autorais ou copyright); seu uso, redistribuição ou modificação não são livres, requerendo permissão do produtor, que normalmente é concedida por meio de pagamento.

Afora o tipo de licença, os softwares podem ser classificados em duas grandes categorias: software de sistema, que é um programa responsável pelo correto funcionamento e pelo gerenciamento de todos os componentes de um computador; e software aplicativo, um programa que permite ao usuário realizar uma ou mais tarefas específicas.

Os aplicativos e os sistemas operacionais estabelecem um relacionamento muito íntimo com o sistema computacional, em que o sistema operacional trabalha diretamente com o hardware, fazendo todas as interfaces necessárias aos aplicativos (vide Figura 1.7).

Figura 1.7 | Hardware, sistema operacional e aplicativos

Fonte: elaborada pelo autor.

A função básica de um software aplicativo é auxiliar os usuários na realização de suas tarefas, proporcionando suporte para a sua produtividade individual e aumentando a quantidade e a qualidade do seu trabalho, e varia de editores gráficos a navegadores web, passando por planilhas eletrônicas e banco de dados, apresentando-se, às vezes, como um pacote completo de soluções integradas.

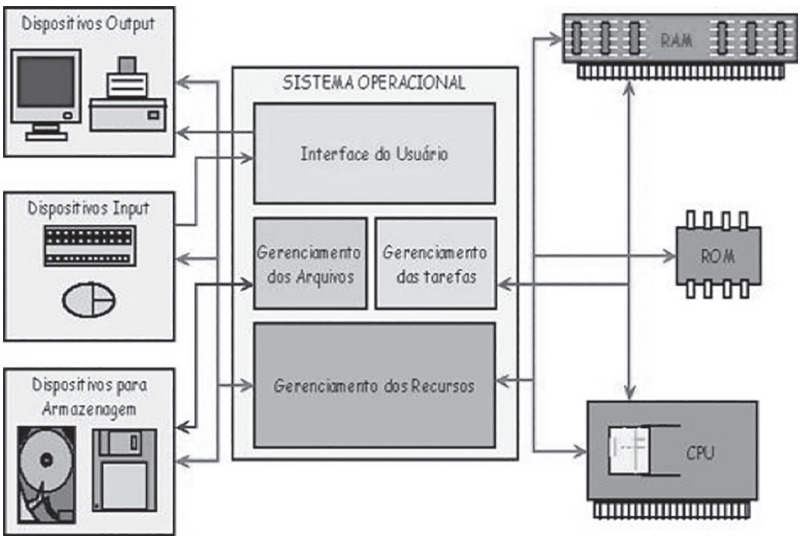
Exemplificando

- Navegadores web: permitem aos usuários acessarem conteúdos na Internet ou páginas www. MS-Explorer, FireFox, Safari, Chrome etc.
- Editores gráficos: permitem a criação e edição de imagens digitais. GIMP, Corel Draw, Photoshop, 3DMax, Draw-LibreOffice.
- Suíte de escritório: são pacotes especiais de softwares aplicativos, compostos por editores de texto, planilha e apresentação; oferecendo uma interface comum a todos os aplicativos; e proporcionando interoperabilidade entre eles. MS-Office (Word, Exel, PowerPonit), LibreOffice, Lotus Symphony e Apple iWork.
- Corporativos: aplicações diversas que atendem as necessidades de organizações: SPT, CRM, SIG, BI, SAD, SAE, KM etc.

Ao contrário dos aplicativos, os sistemas operacionais (SO) são softwares que atuam em contato com o hardware e não com o usuário, servindo como intermediário entre o usuário (pessoa ou aplicativo) e o hardware do computador (vide Figura 1.7) e tem como

missão principal administrar os recursos do sistema computacional, ou seja, processador, memória, arquivos, dispositivos de entrada/saída (E/S ou I/O) e outros (vide Figura 1.8).

Figura 1.8 | Sistema operacional



Fonte: <http://www.coladaweb.com/wp-content/uploads/2014/12/sistema-operacional.jpg>. Acesso em: 14 jun 2017.

A tabela a seguir mostra os principais sistemas operacionais utilizados no mundo e algumas informações sobre esses softwares.

Tabela 1.1 | SO mais utilizados

SO	Fabricante	Ícone	% Usuários	Usuários
Windows	Microsoft		89%	400 milhões
Mac OS X	Apple		6%	23 milhões
GNU/Linux	Vários		2%	9 milhões

Fonte: elaborada pelo autor.

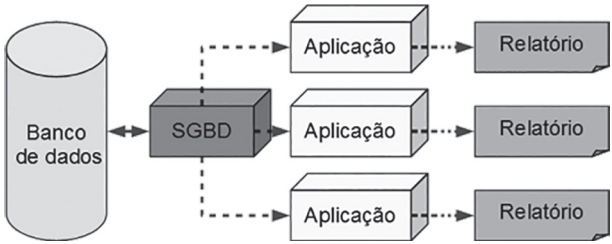
Para finalizar a parte de software, não poderíamos deixar de comentar um tipo especial de software que é o **SISTEMA EMBARCADO**. Um sistema embarcado é um software desenvolvido para uma tarefa específica, que não pode ser alterada e é totalmente dedicada ao dispositivo que controla. Esse software também recebe o nome de **FIRMWARE**, pois é um conjunto de

instruções operacionais programadas diretamente no hardware do equipamento. Esses sistemas são empregados em quase todos os equipamentos eletrônicos da atualidade, como CD/DVD players, GPS, câmeras, impressoras, centrais de alarme, televisores e muitos outros.

Abordaremos agora os bancos de dados, que nada mais são do que um conjunto de dados organizados de forma estruturada, possibilitando o acesso aos dados e informações de forma rápida, precisa e oportuna. Os bancos de dados dão suporte para que as organizações gerem informações que lhes permitirão otimizar seus recursos, diminuindo gastos, aumentando os lucros, facilitando a gestão das rotinas de produção, formulando tendências de mercado e outras inúmeras vantagens.

Para entendermos o que é um banco de dados na prática, vamos pensar que nossos dados (nome, endereço, CPF, salário etc.) são guardados como registros em campos de uma tabela, que várias tabelas são armazenadas em diversos arquivos, e esses arquivos, por sua vez, são concentrados em um banco de dados, ou seja, uma coleção de dados de todos os setores e níveis da organização, gerando o que chamamos de massa de dados, que, dependendo do tamanho, pode virar um *Big Data* ou *Data Warehouse* (bancos de dados gigantescos). Note que cada dado armazenado foi guardado dentro de uma estrutura própria, como se fossem folhas dentro de uma pasta, dentro de uma gaveta, em um armário, numa determinada sala de um prédio específico. Essa forma de guardar os dados é que permite o acesso a eles, que normalmente é feito através de um Sistema Gestor de Banco de Dados (SGBD), uma ferramenta a qual tem a missão de guardar e recuperar dados em um banco de dados e faz isso gerenciando todos os locais possíveis de se arquivar dados, ou seja, todos os prédios, salas, armários, gavetas, pastas e folhas. Um SGBD é um especialista em manipular dados, fornecendo serviços para usuários através das aplicações, como a geração de um relatório de compras, de modo que todos os dados necessários para o relatório serão manipulados pelo SGBD. No entanto, o formato e a apresentação do relatório serão feitos pela aplicação (Figura 1.9).

Figura 1.9 | Esquema de banco de dados



Fonte: adaptada de Stair e Reynolds (2015, p. 210).

Passaremos para o estudo das telecomunicações e redes, começando com o conceito de telecomunicações, que é a ciência que tem como objeto de estudo as formas de comunicação a distância. Como tal, a telecomunicação é uma técnica que consiste na transmissão de uma mensagem de um ponto para outro. A telefonia, o rádio, a televisão e a transmissão de dados através de computadores fazem parte das telecomunicações. Essa comunicação a distância, em se tratando de um sistema computacional, é feita através das redes de computadores, que podem ser definidas como sendo um conjunto de dispositivos conectados por um canal de comunicação (ou link) que permitem compartilhar recursos físicos e lógicos, como dados, periféricos, mensagens e imagens, dentre outros. As redes de computadores abrangem vários segmentos da sociedade e, hoje em dia, são essenciais em cada um deles. As redes melhoraram as escolas, as empresas, os governos e a vida das pessoas, porque possibilitaram uma comunicação rápida e eficiente, além de um compartilhamento generalizado de recursos (impressoras, CD/DVD, *storages*) e informações (registros de clientes, estoques e comunicação entre as pessoas) (FOROUZAN, 2008).

A transmissão de dados de um ponto para outro em uma rede pode ser feita através de cabeamento, ditos meios guiados, tais como o UTP (cabo par trançado), a fibra ótica ou o cabo coaxial; ou pode ser feita sem fio, meios não guiados, com o emprego de equipamentos de radiofrequência (comunicações via ondas de rádio), de comunicações via infravermelho, wi-fi e outros. Já o tráfego de dados, ou seja, o significado daqueles impulsos que são transmitidos, deve seguir um conjunto de protocolos específicos para serem entendidos por todos os dispositivos interconectados.

Normalmente, esse conjunto de protocolos é o **TCP/IP**, que implementa uma série de camadas para operacionalizar o tráfego de dados na rede, garantindo o envio e recebimento das mensagens.

As redes são categorizadas, dependendo do seu alcance, em:

– **PAN** (Personal Area Network – Rede Pessoal): usada para que dispositivos se comuniquem dentro de uma distância bastante limitada, normalmente de dispositivos que cercam uma pessoa.

– **LAN** (Local Area Network – Rede Local ou Privada): interliga computadores presentes dentro de um mesmo espaço físico, via de regra, uma empresa, uma escola ou dentro da sua própria casa.

– **MAN** (Metropolitan Area Network – Rede Metropolitana): permite a interligação de redes e equipamentos numa área metropolitana (locais situados em diversos pontos de uma cidade).

– **WAN** (Wide Area Network – Rede de Longa Distância): possibilita a interligação de redes locais, metropolitanas e equipamentos de rede, numa grande área geográfica (país, continente etc.). Ex.: Internet.

Dessa forma, fornecendo uma maneira para que os dados e informações possam transitar de um lado para outro, por toda a organização e também entre as outras organizações, é que as redes de computadores se tornaram essenciais na infraestrutura de TI das empresas.

Reflita

Diuturnamente mantemos contato com algum hardware, software ou rede de computadores. Você é capaz de identificar e anotar todos esses elementos que aparecem cotidianamente na sua vida? E depois relacioná-los com o que você aprendeu nesta seção?

Para finalizar os nossos estudos, nesta seção, vamos ver algumas aplicações da TI na segurança pública e privada.

Começando pela segurança privada, podemos identificar claramente o emprego da TI em um circuito fechado de televisão (CFTV) que envolve câmeras, cabos, gravadores, computadores, bancos de dados de vídeos,

monitores, aplicativos de exibição, gravação, recuperação e editoração de vídeos e uma rede de comunicação entre todos esses dispositivos; ou em um sistema de controle de acesso, contendo cancelas, catracas, sensores de barreira eletrônica, computadores, sirenes, alarmes, cartões de identificação, banco de dados de pessoas e instalações, rede de comunicação cabeada e sem fio e tudo mais; ou ainda em um sistema de inteligência, que possui um vasto banco de dados, alimentado por agentes de inteligência e analisados por especialistas, que montam diversos relatórios, buscando informações sobre ameaças, vulnerabilidades e riscos de segurança; ou até mesmo em um sistema de monitoramento de frota, com o emprego de GPS, comunicação por celular, e softwares de posicionamento geográfico e controle de itinerário, horário e combustível, que coletam dados constantemente dos veículos, alimentando um banco de dados capaz de gerar relatórios precisos sobre a operação de toda a frota da empresa.

Na segurança pública não poderia ser diferente, pois, hoje em dia, os órgãos de segurança estão empregando largamente a TI e os sistemas de informação no combate ao crime. Como é o caso, por exemplo, do Centro de Operações da Polícia Militar de São Paulo (COPOM), que é totalmente informatizado para combater o crime, monitorando várias regiões através de câmeras de segurança e recebendo denúncias de cidadãos pelo telefone. Em ambos os casos, um policial que opera um sistema de informação em seu computador recebe as informações e as cadastra no banco de dados; a partir daí, o próprio sistema envia as informações para outro policial, que aciona através de rádio ou mensagem uma equipe de policiamento em uma viatura, passando os dados da ocorrência; e essa equipe desloca-se para atender a ocorrência. Dessa maneira, a reação policial passou a ser muito mais rápida e o crime passou a ser combatido com maior sucesso. Chegamos ao final de mais uma seção. Vamos responder a nossa situação-problema?

Sem medo de errar

Vamos voltar à nossa situação-problema e procurar solucionar todos os desafios vivenciados por João Wanderson. Veremos agora que, para elaborar o formulário para o Boletim Eletrônico disponível na Internet, nosso amigo João Wanderson teve de utilizar um computador (hardware) com acesso à Internet (Telecomunicações e Rede) e, utilizando um

navegador (software), acessar o sítio da Delegacia Virtual na web, em que é disponibilizado o sistema de Boletim Eletrônico (software), no qual um comunicante deve preencher um formulário eletrônico, enviando os dados para o banco de dados da polícia. Veja que João Wanderson manteve contato com os elementos da infraestrutura de tecnologia da informação presentes na sua rotina de trabalho na segurança privada e no sistema da Delegacia Virtual, que é um órgão da segurança pública. Vamos ao formulário, então:

FORMULÁRIO PARA PREENCHIMENTO DE BOLETIM DE OCORRÊNCIA ELETRÔNICO

Link para registro da ocorrência: <http://www.ssp.sp.gov.br/nbo/>. Acesso em: 20 abr. 2017.

- Localização Provável da Ocorrência

Estado: _____ Município: _____

Bairro: _____ Quadra: _____

Tipo: _____ Logradouro: _____

Número: _____ Lote: _____ CEP: _____

Complemento: _____

Referência: _____

- Data / Hora do Fato

Data do Fato: _____ Hora aproximada: _____

- Comunicante

Nome: _____ Sexo: ( ) M / ( )F

Telefone Residencial: (___) _____-_____

Celular: (___) _____-_____

E-mail: _____

CPF: _____ RG: _____

Órgão Expedidor: _____

Data de Nascimento: ___/___/___ Nacionalidade: _____

Naturalidade: _____

Estado Civil: _____

Profissão: _____

Nome da Mãe: _____

Nome do Pai: _____

- Endereço do Comunicante

Meu endereço é o mesmo do local da ocorrência?

( ) SIM ( ) NÃO

Estado: _____ Município: _____

Bairro: _____ Quadra: _____

Tipo: _____ Logradouro: _____

Número: _____ Lote: _____

CEP: _____

Complemento: _____

Referência: _____

- Detalhes da Ocorrência

Tipo de Ocorrência: ( ) Furto ( ) Perda

Descreva o que aconteceu: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

- Relação de Documentos

Tipo	Informações:	
CPF	Número:	( ) não sei
RG	Número e órgão:	( ) não sei
CNH	Número de registro:	( ) não sei
Outro:	Descrição:	( ) não sei
Outro:	Descrição:	( ) não sei

Bom trabalho, que tal exercitar mais um pouco?

Avançando na prática

Sistema de segurança na lavanderia

Descrição da situação-problema

Vamos conhecer um pouco da rotina de vida de Eduardo, que é um pequeno empresário, dono de uma lavanderia no bairro onde mora, mas que ultimamente tem visto a criminalidade crescer na circunvizinhança e também tem acompanhado o revés de alguns colegas que tiveram seu comércio invadido e roubado nos últimos tempos. Pensando em se precaver para tal situação, Eduardo resolveu instalar um sistema de segurança em sua loja e, para tanto, contatou um representante de uma empresa que presta serviços nessa área e instala sistemas completos de vigilância, inclusive permitindo ao proprietário que acompanhe tudo pela Internet quando seu comércio estiver fechado. Muito bem. Assumindo o papel do representante da empresa de segurança, você deve propor para o Eduardo que itens serão necessários para construir o sistema que ele deseja. Faça isso pesquisando um pouco na Internet e com base nos conhecimentos adquiridos nesta seção. Faça também a correlação de cada item do sistema de segurança com o seu respectivo item na infraestrutura de TI. Bom trabalho e mãos à obra!

Resolução da situação-problema

Como vimos anteriormente, trata-se de uma pequena loja, que é uma lavanderia, e pode ser instalado um sistema de

segurança sem muita complexidade, mas com bastante eficiência e tecnologia. Para tanto, será necessário empregar basicamente alguns hardwares, como: central de alarme, que é praticamente um computador e comandará o funcionamento de todo sistema, inclusive a comunicação com o celular do Eduardo e acionamento da Polícia Militar através do 190; câmeras, que servirão como periféricos de entrada, capturando as imagens do interior da loja; sensores de movimento, que também são periféricos de entrada, enviando dados do status da movimentação; sensores de porta e janela, periféricos de entrada, que coletam e enviam dados se houve abertura ou não; uma sirene, periférico de saída, que tocará um alarme sonoro em caso de invasão; e cabeamento, necessário para interligar tudo com a central de alarme e essa com a Internet e com a linha telefônica. Será utilizado, além do software embarcado na central de alarme – que possui um pequeno banco de dados para guardar as informações coletadas pelas câmeras e pelos sensores –, um software aplicativo no celular do Eduardo, para que ele possa ver as imagens das câmeras on-line. E, para completar tudo isso, também será utilizada uma conexão com a Internet e uma linha de telefone, que são assinadas pelo Eduardo, para viabilizar a comunicação do sistema com o celular, tablet ou desktop dele.

Ótimo trabalho! Mas, já que estudamos bastante, que tal verificarmos o que aprendemos, respondendo a algumas questões? Vamos lá!

Faça valer a pena

1. Uma câmera de vigilância é um dispositivo largamente empregado na segurança, tanto em circuitos fechados de televisão (CFTV) em uma empresa privada ou em uma organização pública quanto no monitoramento de veículos, vias públicas, linhas de produção e toda ordem de atividades. Dessa maneira, hoje em dia, quase não dá mais para fugir da ação dessas espiãs eletrônicas.
Considerando uma câmera como um hardware que faz parte de um sistema computacional dentro de uma infraestrutura de tecnologia da informação, a alternativa que melhor a descreve é:

a) Periférico de entrada
b) Interface de comunicação
c) Periférico de saída
d) Processador
e) Dispositivo de armazenamento

2. Os softwares são a parte lógica de um sistema computacional e definem, basicamente, um conjunto de instruções chamado de programa, escritos em linguagem de programação e que descrevem as tarefas que o computador deverá executar.

Sabendo que os softwares dividem-se em duas grandes categorias, avalie as afirmativas a seguir:

I – Software de sistema é aquele que ajuda o usuário nas tarefas específicas.

II – Um exemplo de software aplicativo é o Google Chrome.

III – Um sistema operacional é responsável por gerenciar os recursos do hardware.

IV – O software aplicativo faz interface direta com os usuários e manipula o hardware através de sistema operacional.

Estão corretas somente as afirmações:

a) I, II e III.
b) I e II.
c) II, III e IV.
d) III e IV.
e) I, III e IV.

3. Os bancos de dados são conjuntos de dados organizados de forma estruturada, ou seja, obedecendo a uma formatação padronizada de organização dos dados, como os descritos a seguir:

1. Arquivos

2. Registros

3. Banco de dados

4. Dados

Assinale a alternativa que apresenta a ordem correta da estruturação de um banco de dados.

a) 3-1-4-2
b) 4-2-3-1
c) 2-1-3-4
d) 4-2-1-3
e) 1-3-2-4

Referências

ARAÚJO, A. P. F. de. **Infraestrutura de tecnologia da informação** (Notas de Aula). 2009/2011. 2010. 40 f. Curso de Especialização (Gestão da Segurança da Informação e Comunicações) – Departamento de Ciências da Computação da Universidade de Brasília, 2010.

B2W DIGITAL (Rio de Janeiro). B2W – Companhia Digital. **Comércio Eletrônico no Brasil**. 2016. Disponível em: <https://www.b2wdigital.com/institucional/comercio-eletronico-no-brasil>. Acesso em: 17 mar. 2017.

CARUSO, Carlos A. **A Segurança em Microinformática e em redes locais**. São Paulo. Editora: LTC, 1995.

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

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerencial**. Tradução de Thelma Guimarães; revisão técnica de Belmiro N. João. 7. ed. São Paulo: Pearson Prentice Hall, 2007.

MARÇULA, M.; FILHO, P. A. B. **Informática**: conceitos e aplicações. 3 ed. rev. São Paulo: Érica, 2008.

STAIR, R. M.; REYNOLDS, G. W. **Princípios de sistemas de informação**. Tradução Noveritis do Brasil; revisão técnica Tânia Fátima Calvi Tait. 11. ed. São Paulo: Cengage Learning, 2015.

VON BERTALANFFY, Ludwig. **Teoria Geral dos Sistemas**. 6. ed. Petrópolis: Vozes, 2012.

A gestão e a segurança da informação

Convite ao estudo

Caro aluno, na unidade anterior vimos como os sistemas de informação e as tecnologias da informação e comunicações transformaram o mundo moderno. Vimos também a importância da informação e seus impactos nas organizações e na segurança pública e privada. Neste momento, prosseguiremos no nosso aprendizado, buscando conhecimentos sobre a gestão desses sistemas de informação, que processam o bem mais valioso das organizações atualmente, ou seja, a informação. Além disso, discutiremos sobre como é relevante que a informação que tramita nesses sistemas e tecnologias seja protegida contra a ação indevida de agentes maliciosos, porque a segurança da informação deve ser encarada como uma necessidade vital para as pessoas, organizações públicas e privadas e, principalmente, para os órgãos de segurança pública e as empresas e os agentes da segurança privada.

Dentro da ideia de contextualizar nossa aprendizagem, vamos pensar na situação a seguir que começa pela frase: "Futuro conectado compromete segurança na rede". Foi a chamada que Fernando Bezerra leu na coluna Link, do Jornal "O Estado de São Paulo" (disponível em: <https://goo.gl/H3ANpQ>. Acesso em: 16 abr. 2017).

Fernando trabalha na Secretaria de Segurança do Governo do Estado de Minas Gerais - SSPMG, cuja função é analisar os riscos da rede e dos sistemas de segurança pública, que, atualmente, disponibilizam o acesso a diversos dados aos cidadãos e órgãos pela internet. Fernando Bezerra não ficou muito surpreso com a notícia que leu no site desse jornal de grande circulação, porque tem bastante conhecimento do assunto. Ele sabe das

dificuldades e tem a exata noção de que a Rede Internacional de Computadores traz vários benefícios, mas carrega consigo riscos ilimitados aos usuários, às organizações e às corporações. Sua missão, como especialista em segurança de redes, é analisar todos os sistemas da SSPMG, a maioria destes voltados para a segurança pública, e levantar os acessos indevidos, as tentativas de invadir a privacidade dos agentes públicos, as invasões para obtenção dos dados diversos dos cidadãos e, ainda, as ações deliberadas aos servidores (grandes computadores) para provocar a queda e a inoperância dos sistemas.

Fernando Bezerra lida com vários sistemas alimentados pelas ocorrências dos órgãos policiais civil e militar, com os dados advindos dos Conselhos Comunitários de Segurança – CONSEG e com as informações oriundas dos órgãos de inteligência diversos, como a Rede Nacional de Integração de Informações de Segurança Pública, Justiça e Fiscalização – Rede INFOSEG. Seu desafio, o de gerenciar o fluxo da informação e evitar os acessos não autorizados, é grande.

Pelo visto, a missão de Fernando não é fácil. E realmente não é simples trabalhar diretamente com a informação, seja fazendo a gestão dela ou sua segurança. Mas será que esta é uma missão impossível? Qual será a forma correta de se administrar a informação? Como conseguir manter uma informação segura nessa era da internet? E como fica o papel da segurança pública e privada nesse contexto?

Para cada questão que possa ser levantada sobre este assunto, existirá uma resposta adequada e, nesta unidade, tentaremos buscar um pouco das nossas respostas, estudando a Gestão Estratégica da Informação; a Segurança da Informação; e a Segurança na Era da Internet. Sem sombra de dúvidas, vamos cursar um conteúdo instigante e muito atrativo, por isso, precisamos começar com firmeza e determinação.

Boa jornada e bom estudo!

Seção 2.1

A gestão estratégica da informação

Diálogo aberto

Dentro do nosso contexto de aprendizagem – Fernando, que trabalha na Secretaria de Segurança do Governo do Estado de Minas Gerais, cuja função é analisar os riscos da rede e dos sistemas de segurança pública utilizados em Minas Gerais – imagine agora que o Cabo Abreu, que trabalha há mais de vinte anos em um dos Pelotões de Polícia do 62º BPM da cidade de Caratinga – MG estava indignado logo em uma segunda-feira, porque sua mesa estava cheia de fichas de ocorrências dos plantões policiais do final de semana, as quais deveriam ser conferidas e lançadas no livro de ocorrência para que pudessem se transformar em boletins de ocorrência. A experiência do Cabo Abreu diz que ele deve ser criterioso com o registro oficial das ocorrências, pois caso insira um fato, uma pessoa envolvida ou o nome incorreto do policial que atendeu à ocorrência, podem acontecer desdobramentos diversos e, até mesmo, inviabilizar a ocorrência formal. Quando iniciou seus trabalhos na PM, Caratinga era uma cidade menor, mas com o crescimento da população veio a evolução dos crimes e, consequentemente, das ocorrências.

O Cabo Abreu já não estava muito satisfeito com aquela papelada que não acabava mais e, justo na segunda-feira, veio uma moça solicitando o boletim de ocorrência policial de um acidente envolvendo veículos e vítimas com lesões corporais, para dar entrada na solicitação do seguro. Aquele foi o estopim. Ele ficou pensando, será que não existe um sistema que possa agilizar a inserção dos dados diversos? Seria bom se a SSPMG se lembrasse das pessoas de Caratinga. Mas como seria este sistema em uma cidadezinha do interior? É possível que não chegue até nós. O melhor seria se eu lançasse a identidade e o CPF e já puxasse os dados do cidadão, dessa forma ajudaria muito a reduzir a papelada. Auxiliaria até mesmo os policiais no atendimento das ocorrências. Mas isso parece que é muito difícil!

Para ajudar a resolver os problemas do Cabo Abreu, você deverá elaborar um relatório contendo respostas para os seguintes

questionamentos: o que seria necessário a SSPMG implementar em termos de sistemas? E como garantir a segurança de um sistema de ocorrências e registro de dados? É possível a Secretaria de Segurança Pública disponibilizar, integrar e proteger um sistema de ocorrências policiais em um local remoto?

Para ajudar o Cabo Abreu, precisaremos compreender o que é o mundo digital, onde as coisas acontecem on-line, facilitando a vida de todo mundo, e também saber como é feito o gerenciamento da informação que circula nesses sistemas, além de entender um pouco mais sobre esses próprios sistemas de informações gerenciais e de negócio. Não podemos perder tempo, vamos ao conhecimento!

Não pode faltar

Caro aluno, vamos dar início a mais uma seção de estudo buscando conhecer os Sistemas de Informação em Segurança e, desta vez, abordaremos a Gestão Estratégica da Informação. Para tanto, começaremos com a identificação da Era da Informação para prosseguirmos com a aprendizagem de como pode ser feita a gestão da informação, além de nos aprofundarmos um pouco mais nos Sistemas de Informações Gerenciais (SIG) e nos Sistemas de Inteligência Empresarial (BI). Vamos lá!

A Era da Informação ou Era Digital, também conhecida como Era Pós-Industrial, é o novo ciclo que a humanidade está vivendo desde o final do século passado, com o término da Revolução Industrial. Esta nova era pode ser caracterizada pelo papel transformador assumido pela informação na vida das pessoas, na sociedade, nas organizações. Neste meio tempo, o grande avanço da informática, da computação e das telecomunicações, originando o espaço cibernético, acelerou sobremaneira essa transição, acentuando ainda mais a projeção da informação como mola propulsora dessa revolução. Dessa forma, a Era da Informação passou a ser mais uma etapa na evolução da vida humana.

Nessa nova fase, os sistemas de informação ganharam popularidade e assumiram papéis desempenhados privativamente pelo homem, por causa da sua capacidade de raciocínio. A tecnologia tomar o lugar do homem não é novidade, pois isso já havia acontecido quando a automação industrial substituiu o operário no chão de fábrica, só que

agora o computador está substituindo a capacidade do homem de processar informações e isso é muito impactante. É claro que o homem ainda ficou com o papel de detentor do conhecimento e da sabedoria (e estes conceitos você já aprendeu na Seção 1.1, da Unidade 1), através da sua criatividade e imaginação; detalhes que o computador ainda não é capaz de fazer. Por esse motivo, vem crescendo a importância do estudo e da qualificação profissional na vida do ser humano.

A tecnologia assumiu o controle da informação porque cresceu muito a capacidade da TI em gerar, armazenar, manipular e difundir informação de forma automática. Essa evolução transcendeu a capacidade humana, pois a informação passou a ser gerada, processada e transmitida de forma muito rápida e em grandes volumes, e essa velocidade e quantidade foram crescendo exponencialmente, sendo humanamente impossível realizar essa tarefa. Atualmente, por causa dessa velocidade da informação, tudo está mais rápido. O que era novidade em um momento, vira passado no instante seguinte. Foi o que aconteceu do *pager* ao smartphone, do disco de vinil ao *stream* de áudio e da televisão de tubo a *smart TV*, ou seja, as transformações são diversas e muito rápidas, sendo difícil de acompanhá-las.

Exemplificando

Para ilustrar essa aceleração e transformação promovida pela informação nos produtos e serviços comercializados pelas empresas, vamos tomar como exemplo dois modelos de automóveis muito conhecidos por todos: o Fusca e o Gol. O Fusquinha, um dos carros mais populares já comercializados pela indústria automobilística, reinou isolado no Brasil por mais de 25 anos, desde seu lançamento em 1959, até sair de linha em 1986. Detalhe, com o mesmo modelo! Em seguida, veio o substituto do Fusca, o também muito popular e conhecido Gol, lançado em 1980, sendo o primeiro modelo denominado pela Volkswagen (VW) como Geração 1 (G1), e durou até 1994. Portanto, 14 anos no mercado, quando foi lançado o Gol G2, em 1994, conhecido como "bola", que já durou apenas cinco anos, até ser substituído pelo Gol G3, em 1999. Este teve o mesmo tempo de vida do Gol G2, ou seja, 5, quando deu lugar para o Gol G4, em 2004. E agora estamos no Gol G5, desde 2007, isto é, o Gol G4 durou apenas 3 anos (MOTOR1.COM, 2015). Embora o Gol G5 ainda esteja em atividade passados mais de 10 anos, pode ser justificado porque a partir daí as maiores mudanças foram feitas no embarque de tecnologias nos automóveis, ou seja, o diferencial deixou de ser o modelo em si, mas sim a tecnologia à disposição do condutor, como conectividade, informação e entretenimento.

Essa informação toda é propulsora da integração mundial que se vive atualmente, porque as notícias correm o mundo em segundos e os acontecimentos são narrados, às vezes, em tempo real, como se a história fosse contada dia a dia, além de permitir uma troca muito intensa de conhecimento provocando a rápida evolução de diversos setores da sociedade, como educação, cultura, lazer, economia, política e outros. Graças à integração promovida pela comunicação, as distâncias diminuíram, a sociedade ficou mais coesa e surgiu a globalização, um movimento de integração da sociedade mundial em torno da economia e da cultura, com o intercâmbio de produtos e de conhecimento. Na direção oposta desta integração mundial está o isolamento social do indivíduo, um fenômeno do mundo moderno que atinge um grande número de pessoas. Motivadas pelo fácil acesso à informação através das redes sociais e dos aplicativos, muitas pessoas vivem escondidas atrás de sua timidez e, apesar de estarem isoladas socialmente, interagem vigorosamente com a internet, ora com outras pessoas, ora com elementos virtuais e até mesmo trabalhando, e isto tudo sem nenhum contato físico com outra pessoa. Este é um sério problema da Era Digital.

Reflita

Imagine um profissional de segurança que passa seus dias a fio olhando para monitores de computador que exibe imagens sobre aquilo que se deseja manter seguro. Será que ele está mais propício ao isolamento social? Como evitar essa tendência? Você já se preocupou com isso? Essas questões também afligem os profissionais de segurança e não somente os adolescentes *nerds* e as pessoas introvertidas.

Prosseguindo, podemos dizer que este momento da civilização também trouxe uma democratização da informação, porque praticamente todo mundo pode divulgar informações na internet e muitas delas ganham notoriedade rapidamente, são as conhecidas "**viralizadas**", isto é, informações que ganham o mundo em poucos minutos na internet. Essa facilidade também tem seus revezes, porque existe muita informação não confiável, tendenciosa e fraudulenta circulando pela rede, tendo de cada um saber selecionar o conteúdo adequado. Note que somente os meios de comunicação convencionais, como a televisão, o rádio, o jornal, as revistas e outros,

tinham o poder de selecionar as informações que se tornariam públicas, e agora isso não ocorre mais. Por um lado, é bom porque fica mais difícil de se manipular a opinião pública apresentando conteúdos pré-selecionados, por outro, surgem muitas informações desqualificadas e improcedentes para processarmos. O fato é que a internet trouxe à tona um aglomerado incontrolável de informações onde se pode achar de tudo, desde a receita de um bolo até o manual de bombas caseiras, e da mais divina evangelização até a apologia ao nazismo e à violência.

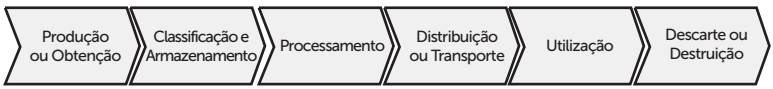
Ainda sobre essa nova era, temos também o surgimento do conceito de cibernética como sendo uma ciência baseada nos sistemas de processamento das informações e que estuda a comunicação e o controle dentro da abordagem sistêmica da informação, onde a comunicação integra os sistemas de informação e o controle governa o desempenho destes no processamento e na transformação da informação (CHIAVENATO, 2004). Como desdobramento deste conceito, surgiram novas concepções e dimensões no ambiente de vida humana, como o espaço cibernético ou ciberespaço, que é justamente este universo de sistemas integrados pela comunicação em rede, que ninguém consegue ver ou pegar, mas onde ocorrem diversos fatos que geram impactos concretos e muito significativos na vida real. É a chamada Era Virtual, na qual o meio físico não existe mais, e tudo acontece de forma intangível e on-line, contudo, gerando consequências verdadeiras e efetivas.

Finalizando, esta é a nova era da civilização, na qual a comunicação passou a ser a essência da atividade humana, surgindo um novo tipo de sociedade, a conectada ou em rede, com novos universos, comportamentos, oportunidades, adversidades e desafios.

Compreendida a complexa Era da Informação, na qual a informação é o bem mais valioso da sociedade, constituída pelas pessoas e organizações, é claro que esse bem deve receber um tratamento específico para manter sua utilidade e, principalmente, seu valor. Esse tratamento é conhecido como Gestão da Informação, que podemos conceituar como sendo a capacidade que uma organização deve ter para administrar ou gerenciar a informação durante todo o ciclo de vida dela. O ciclo de vida da informação é descrito de várias maneiras por diversos autores, porém, podemos considerar que compreende sua produção, obtenção ou coleta; sua classificação

e seu armazenamento; seu processamento ou manipulação; sua transmissão, distribuição ou transporte; sua utilização; e, por fim, seu descarte ou destruição (Figura 2.1)

Figura 2.1 | Ciclo de vida da informação



Fonte: elaborada pelo autor.

Assimile

Vamos entender o que significa cada conceito apresentado na Figura 2.1?

- **Produção ou busca**: gerar informação ou adquiri-la de alguma fonte, atendendo aos requisitos de necessidade da informação.
- **Classificação e armazenamento**: conservar a informação de forma estruturada em bancos de dados, categorizadas por características e critérios, principalmente, determinando que usuários terão acesso à informação.
- **Processamento**: transformação feita na informação para agregar significado e formatar sua apresentação.
- **Distribuição**: disponibilização da informação para os usuários autorizados.
- **Utilização**: empregar a informação de forma que produza os resultados desejados.
- **Descarte**: deixar de guardar a informação ou destruí-la.

Geralmente, as organizações fazem gestão da informação com o objetivo de permitir que a informação permaneça segura e esteja disponível no momento certo para ser utilizada com oportunidade pelos usuários que necessitem da informação e estejam credenciados a acessá-la.

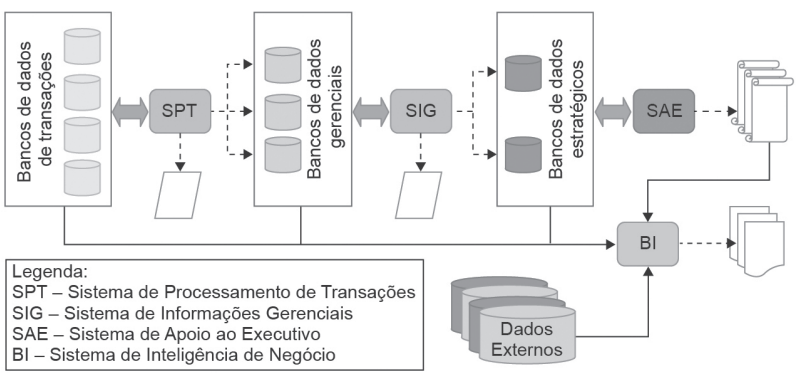
Vimos que a informação é a mola propulsora da atividade humana atualmente, por isso, as pessoas e as organizações precisam das informações em suas tarefas e processos, principalmente, aquelas que envolvam algum tipo de decisão. Fruto dessa necessidade de informação, surge a exigência de se administrar ou gerir este tão valioso ativo da sociedade digital.

As organizações que fazem gestão da informação buscam também:

- Produzir informação sobre seus processos internos.
- Coletar informações externas que de alguma forma influenciam ou interferem na sua atividade.
- Manipular suas informações através de sistemas de processamento de informações, buscando obter vantagem competitiva. Sistemas como o SIG que já conhecemos e veremos mais detalhadamente adiante.
- Promover uma comunicação ágil e segura para troca de informações entre suas repartições internas e com seus participantes externos.
- Utilizar informação nos seus processos de tomada de decisão, na arquitetura de novos produtos e no relacionamento com o cliente.
- Configurar cenários prospectivos do mercado e da economia, visando valer-se de decisões estratégicas e proativas que podem definir a sobrevivência da empresa.

A gestão da informação em uma empresa ou organização perpassa pelos sistemas de informação que a empresa utiliza, simplesmente porque estes participam diretamente da existência da informação, desde sua produção ou coleta; passando por seu armazenamento e processamento; e chegando à sua utilização e descarte (Figura 2.2).

Figura 2.2 | Sistemas de informação nas organizações



Fonte: elaborada pelo autor.

Vendo por esta perspectiva, logo se nota que fazer gestão da informação não é uma tarefa simples nem pode ser desenvolvida ou executada por um profissional sem a devida habilitação técnica para levar a efeito esta delicada atividade dentro de uma empresa ou organização. Na verdade, esta é uma tarefa para um profissional específico, o Gestor da Informação. Esta profissão envolve a realização de todas as atividades que acabamos de aprender, além de participar de outras que envolvam informação dentro da empresa, tais como realizar pesquisa de informações estratégicas para os negócios da empresa, compor times de análise de cenários de mercado, estudar e otimizar fluxos de informação e gerenciar os bancos de dados internos e as fontes de dados externos. Em virtude do largo emprego de tecnologias da informação e comunicação na sua atividade, este profissional atua intimamente ligado com a área de TI da empresa, fazendo todas as interfaces necessárias para que sua missão obtenha sucesso.

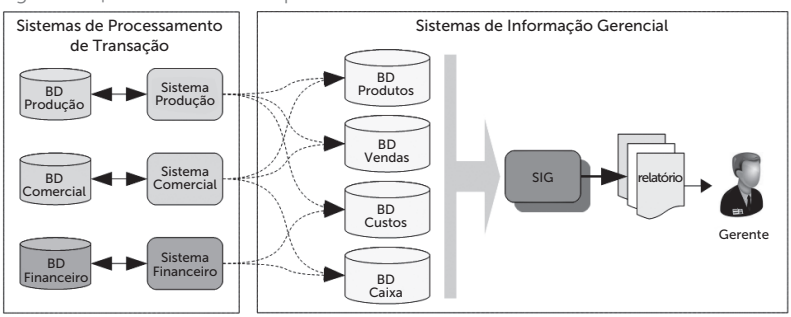
Vimos, portanto, como fazer a gestão da informação em uma organização e que, além de ser uma atividade vital para o negócio da empresa, está longe de ser uma tarefa fácil, principalmente porque envolve grande parte dos sistemas de informação empregados na organização, e somente promover essa integração já é motivo de bastante trabalho. Particularmente dois sistemas utilizados pelas empresas, em geral, são muito importantes para a gestão estratégica da informação, são eles: os Sistemas de Informações Gerenciais (SIG) e os Sistemas de Inteligência de Negócio (BI). Passaremos, então, a estudar detalhadamente cada um deles.

Começaremos pelos Sistemas de Informações Gerenciais (SIG), os quais já sabemos que recebem essa classificação porque atuam no nível tático ou gerencial dentro da estrutura da empresa e que reportam as operações básicas dela, através de relatórios e estatísticas sobre o desempenho da organização, permitindo o acompanhamento e o controle dos meios de produção, da produção propriamente dita e dos produtos e serviços gerados. Na verdade, um SIG é um sistema que envolve diversas tarefas reunidas em torno de um objetivo comum, ou seja, fornecer as informações necessárias para que os gerentes possam acompanhar e controlar o andamento do negócio da empresa, possibilitando intervenções e ajustes, quando necessário, visando a consecução

dos objetivos do negócio e promovendo vantagem competitiva para a organização (LAUDON; LAUDON, 2007).

A operação básica de um SIG compreende o processamento de dados para a produção de informações que serão empregadas no sistema decisório de nível gerencial da empresa (FRANCO; RODRIGUES; CASELA, 2013). Esse processo se inicia com a coleta de dados pelos SPTs que resultam na manutenção de bancos de dados operacionais, geralmente, contento dados sobre a produção, o volume de vendas, a contabilidade e outros. Os SPTs, por sua vez, se interligam com o SIG, fornecendo dados para os bancos de dados gerenciais. Dessa forma, o SIG pode realizar consultas estruturadas e processamentos nestes dados, buscando agregar significado a eles, isto é, transformando-os em informações, regularmente apresentadas em formato de relatórios que serão utilizados pela gerência (Figura 2.3). Os relatórios podem se apresentar de diversas formas, a critério da gerência e dentro das possibilidades de customização do sistema, podendo ser programados (semanal, mensal, anual); eventuais, sob demanda dos gerentes, em um momento de necessidade ou imposição; de indicadores, resumem índices de atingimento de metas; de adversidades ou exceções, quando ocorre algum evento ou comportamento anormal em alguma rotina; e outros (a Tabela 2.1 mostra um exemplo fictício de relatório de um SIG).

Figura 2.3 | Funcionamento típico de um SIG



Fonte: adaptada de Laudon e Laudon (2007).

Um sistema tipicamente SIG deve apresentar algumas peculiaridades que o caracteriza discriminativamente de outros. Vejamos algumas delas (STAIR; REYNOLDS, 2015):

- Baseiam-se geralmente em dados internos da empresa.
- Executam operações e processamentos relativamente simples do ponto de vista matemático e estatístico.
- Processam dados históricos e atuais da atividade da organização, mas usualmente não projetam informações futuras.
- Servem exclusivamente para o ambiente interno da empresa, mais precisamente no que diz respeito à rotina interna da organização.
- Usualmente emitem relatórios padronizados.

Tabela 2.1 | Exemplo de relatório gerado pelo SIG

COD PROD	DESCRIÇÃO	CUSTO	VENDAS	LUCRO	META
2584	Amaciante 1,5l	R$ 2,97	711.695	R$ 634.120,00	R$ 600.000,00
2365	Detergente 500ml	R$ 0,58	1.865.259	R$ 324.556,00	R$ 400.000,00
9841	Sabão em Pó 800g	R$ 1,64	1.543.684	R$ 759.492,00	R$ 1.000.000,00
2478	Água Sanitária 2l	R$ 1,36	2.684.532	R$ 1.095.289,00	R$ 1.000.000,00
8745	Cera líquida 800g	R$ 3,42	568.265	R$ 583.039,00	R$500.000,00
			TOTAL	R$3.396.496,00	R$ 3.500.000,00

Fonte: elaborada pelo autor.

Outro importante sistema, dentro do contexto de gestão estratégica da informação, é o Sistema de Inteligência de Negócio (BI), que também já estudamos e conhecemos como sendo resultado da integração dos sistemas da empresa com foco no processo decisório, primordialmente, no nível estratégico da organização. É exatamente isso, um sistema de BI também tem a finalidade de dar suporte ao processo decisório de uma empresa, assim como o SIG, porém voltado para o nível estratégico da organização. Por se tratar do nível estratégico, as informações a serem analisadas e os cenários a serem elaborados são muito mais complexos, por isso, em um sistema de BI são processados enormes volumes de dados, coletados de diversas fontes internas e externas a empresa, e são produzidas informações capazes de permitir uma clara interpretação do significado desses dados pela gerência estratégica da empresa.

Um sistema de BI é capaz de (i) extrair dados de múltiplos bancos de dados simultaneamente (Figura 2.2), por meio

de ferramentas específicas, como OLAP (*On-line Analytical Processing* ou processamento analítico on-line), EIS (*Executive Information System* ou sistema de informação do executivo), Data Mining (Mineração de Dados) e outros; (ii) processar toda essa massa de dados, considerando um contexto de análise, buscando estabelecer relações entre os dados e projetando hipóteses e tendências futuras neste contexto; e (iii) emitir relatórios, gráficos e composição de cenários de negócio. Tudo isso para permitir a empresa tomar medidas proativas para manutenção de suas estratégias de negócio, como prever tendências do mercado consumidor, antevendo o lançamento de produtos e até mesmo antecipando estratégias dos concorrentes (BROGNOLI, 2010).

Pesquise mais

Para ampliar seus conhecimentos sobre Sistemas de BI, leia o artigo de Alvaro Brognoli, especialista em Gestão Estratégica Empresarial, disponível em: <http://alvarobrg.blogspot.com.br/2010/04/implementacao-de-um-sistema-de.html>. Acesso em: 20 abr. 2017.

Chegamos ao final de mais uma seção dos nossos estudos, espero que tenhamos conseguido aprender um pouco mais sobre os sistemas de informação e a gestão estratégica da informação. Dessa forma, poderemos prosseguir na resolução da nossa situação-problema.

Sem medo de errar

Caro aluno, vamos a solução da nossa situação-problema. Você se lembra das reclamações do Cabo Abreu sobre o sistema de registro de ocorrências?

Para ajudar o nosso amigo, a SSPMG poderia implementar um sistema de informações de registro de ocorrências, disponibilizando acesso pela internet, podendo assim viabilizar o acesso para as mais remotas unidades de polícia do Estado de Minas Gerais, aproveitando o espaço cibernético de nossa Era Digital. Este sistema teria a finalidade de preencher bancos de dados de ocorrências, possibilitando o armazenamento destes,

sua transmissão pela grande rede, sua utilização por agentes públicos de segurança e outros órgãos de interesse, mediante credenciamento de acesso, além do processamento dos dados por outros sistemas que possibilitem ações policiais mais eficazes contra o crime, advindas de sistemas de informações gerenciais da SSPMG.

Mas claro que nem tudo seria fácil assim, para garantir a eficiência do sistema e a segurança dos dados ali presentes, torna-se necessário a implantação de uma rotina de gestão das informações circulantes no sistema, desde sua produção, passando pelo seu armazenamento e transmissão, até sua utilização e descarte. Tudo isso pode, tranquilamente, ser integrado com outros sistemas da Secretaria de Segurança Pública, como citado anteriormente, para que seja feita uma análise e um cruzamento dos dados do sistemas de registro de ocorrências com os dados de outros sistemas, visando o levantamento de informações que seriam usadas nos processos decisórios dos órgãos de segurança pública – dentro da ideia dos SIG e BI –, permitindo um combate mais eficaz contra a criminalidade e até mesmo antecipando as ações criminosas, provendo uma segurança de melhor qualidade para a população. E, antes que esqueçamos, facilitando, é claro, o trabalho do Cabo Abreu, em Caratinga – MG, que não precisaria mais daquela papelada interminável e ineficiente. O que você achou da nossa solução? Tenho certeza de que ficou bem parecida com a sua. Vamos praticar mais um pouco?

Avançando na prática

Segurança na Era Digital

Descrição da situação-problema

Agora que já auxiliamos o Cabo Abreu com nossas sugestões de implantação de sistemas de informações na SSPMG, vamos continuar nossa prática colaborando com o Marcelo Martins, um agente da guarda municipal de Propriá, no Sergipe, que diariamente faz rondas pela cidade monitorando a segurança dos prédios públicos e do patrimônio da prefeitura. Certo dia, o agente foi chamado para verificar uma chamada do almoxarifado da Secretaria de Saúde do

município. Chegando lá, o diretor do almoxarifado, Sr. Waldir, relatou para Marcelo que ele estava suspeitando de um veículo que estava parado em frente ao portão de carga e descarga do almoxarifado e que já há alguns dias vinha permanecendo várias horas estacionado no mesmo lugar, mas que não dava para ver nada dentro do carro por causa dos vidros escuros.

Como aquela instalação já havia sido vítima de assalto por quadrilhas especializadas em roubo de medicamentos de alto valor, ele estava muito preocupado com aquele veículo e já havia, inclusive, anotado a placa, QRM-2017. Diante desse relato, o Sr. Waldir solicitou que Marcelo tomasse alguma providência para dirimir sua suspeita. E agora? O que Marcelo Martins pode fazer? Será que a desconfiança do Sr. Waldir tem fundamento ou é apenas uma cisma? Como Marcelo pode se valer da vasta quantidade de informações que existem no espaço cibernético para resolver essa questão? Será que existe algum sistema de informação que pode ajudá-lo? Se existe, que tipo de sistema é esse? Você pode ajudar o GM Marcelo Martins? Nesse contexto, vamos ver como?

Resolução da situação-problema

Já que o Marcelo Martins possui somente a placa do veículo e o relato do Sr. Waldir para proceder seu trabalho, ele poderia, por exemplo, consultar a situação do veículo no Aplicativo Sinesp Cidadão, disponibilizado na internet pela Secretaria Nacional de Informações de Segurança Pública, um sistema de informações gerenciais, integrando bancos de dados de informações sobre veículos e mandados de prisão para ajudar os agentes de segurança no combate ao crime. Neste aplicativo ele poderia verificar se não se trata de um veículo roubado ou coisa do tipo, ou ainda mesmo verificar a situação dos integrantes do veículo em relação à justiça. Feitas essas consultas e a abordagem dos integrantes do veículo, o GM Marcelo Martins teria condições de confirmar, ou não, a suspeita do Sr. Waldir, fazendo seu trabalho com o auxílio de informações precisas, seguras e disponíveis no momento certo. Lembre-se de que este sistema tem um aplicativo voltado para o cidadão, o Sinesp Cidadão, que pode ser baixado de graça no seu smartphone.

Ótimo, que tal respondermos algumas perguntas agora?

Faça valer a pena

1. A Era da Informação ou Era Digital, também conhecida como Era Pós-Industrial, é o novo ciclo que a humanidade está vivendo desde o final do século passado, com o término da Revolução Industrial. Esta nova era pode ser caracterizada pelo papel transformador assumido pela informação na vida das pessoas, na sociedade e nas organizações.

A respeito da Era da Informação, avalie se são (V) verdadeiras ou (F) falsas as afirmativas a seguir:

( ) A tecnologia assumiu o controle da informação porque a capacidade da TI em gerar, armazenar, manipular e difundir informação de forma automática transcendeu a capacidade humana.

( ) Os sistemas de informação ganharam muita popularidade e assumiram um papel importantíssimo, o de substituir o homem e sua capacidade criativa.

( ) O grande avanço da informática, da computação e das telecomunicações, dando origem ao espaço cibernético, acentuaram ainda mais a projeção da informação como mola propulsora dessa nova era.

( ) Na contramão da integração mundial vivida na Era Digital está o isolamento social do indivíduo, um mal que aflige grande parcela dos indivíduos conectados.

Assinale a alternativa que apresenta a sequência CORRETA, respectivamente.

a) V-F-F-V.

b) F-F-V-V.

c) V-F-V-F.

d) F-V-V-V.

e) V-F-V-V.

2. A Gestão da Informação pode ser conceituada como a capacidade que uma organização deve ter para administrar a informação durante todo seu ciclo de vida. Este ciclo basicamente compreende as atividades a seguir:

1 – Classificação e armazenamento.

2 – Utilização.

3 – Transmissão.

4 – Produção ou coleta.

5 – Processamento.

Assinale a alternativa que contém a ordem correta das fases do ciclo de vida da informação.

a) 4-1-5-3-2.

b) 1-4-3-2-5.

c) 4-5-1-2-3.

d) 2-3-1-5-4.

e) 4-1-5-2-3.

3. Tanto os Sistemas de Informações Gerenciais (SIG) quanto os Sistemas de Inteligência de Negócio (BI) são empregados para dar suporte ao processo decisório das empresas, com o objetivo de obter uma vantagem competitiva contra a concorrência, mas esses sistemas apresentam algumas diferenças entre si.

Um SIG coleta somente dados _____ para apoiar o nível _____, enquanto que o BI coleta dados _____ e visa apoiar o nível _____ da organização.

A partir da frase anterior, assinale a alternativa que contém as palavras adequadas às lacunas.

a) Interno-estratégico-externo-tático.

b) Externo-tático-externo-estratégico.

c) Interno-tático-externo-estratégico.

d) Externo-estratégico-interno-tático.

e) Tático-interno-estratégico-externo.

Seção 2.2

A segurança da informação

Diálogo aberto

Caro aluno, depois de ajudar o nosso amigo Fernando Bezerra, aquele analista de riscos da rede e dos sistemas de segurança pública da SSPMG, a resolver os problemas do pequeno município de Caratinga, ele pensou que poderia conduzir sua rotina normalmente, mas não foi bem assim. Logo no dia seguinte, ele recebeu uma mensagem pelo WhatsApp de seu amigo da Faculdade de Sistemas de Informação, Flávio Damasco, que trabalhava na mesma função que Fernando só que na iniciativa privada. Flávio comentava que o sistema de controle de acesso e cadastro de funcionários, visitantes e prestadores de serviços do Condomínio de Escritórios Inteligentes Gallery, na cidade de Vespasiano – MG, havia sido invadido por hackers. Flávio Damasco ligou para Fernando para que juntos pudessem analisar o tipo de invasão. Fernando ficou preocupado, matutando os seguintes questionamentos: se o sistema do Condomínio de Escritórios Gallery, que tem uma quantidade imensa de recursos, foi invadido, será que os sistemas da SSPMG também poderiam sofrer os mesmos ataques? Será que não existe nenhum sistema totalmente seguro? Essa invasão de sistemas que tem dados de altos executivos poderia causar alguma consequência maior para os resultados da criminalidade? O que teria de ser analisado e implantado por Fernando e Flávio para garantir a segurança? Essa missão não será fácil e, para cumpri-la, você precisará ter entendido muito bem os conceitos básicos de segurança da informação, conhecido as normas e padronizações referentes à segurança da informação, conseguido identificar as ameaças mais comuns à segurança da informação e empregado corretamente os mecanismos de defesa e segurança da informação na Segurança Pública e Privada. Nesse contexto, vamos ajudar nossos personagens, Fernando e Flávio, a resolverem seus conflitos? Perceba que, ao responder os questionamentos aqui apresentados, você estará promovendo uma

análise de alguns problemas encontrados na Segurança Pública, relativos aos aspectos da Segurança da Informação. Apresente esta análise através de um relatório.

Agora estudaremos alguns conceitos.

Não pode faltar

Após termos aprendido a Gestão Estratégica da Informação, prosseguiremos na nossa missão, estudando a Segurança da Informação, um tema bastante latente atualmente, que indica a crescente importância desta atividade na manutenção da informação e na rotina das pessoas e empresas. Vamos começar compreendendo alguns conceitos fundamentais em Segurança da Informação, o primeiro deles será o próprio conceito de Segurança da Informação e Comunicações (SIC), que nada mais é do que a proteção da informação, no sentido de preservar o valor que ela representa para um indivíduo ou uma organização. Além disso, segundo a Norma ABNT ISO/IEC 27002 (2013), Segurança da Informação é a proteção da informação das várias ameaças, para garantir a continuidade do negócio, diminuir o risco e aumentar os lucros e as oportunidades de negócio. A segurança da informação é obtida por meio da implantação de um conjunto de medidas que envolve pessoas, processos e tecnologias, visando garantir a disponibilidade, integridade, confidencialidade, autenticidade e irretratabilidade ou não-repúdio da informação. Essas características são conhecidas também como atributos de uma informação segura ou princípios de segurança da informação. A seguir, detalharemos cada um deles:

- **Disponibilidade**: é a qualidade da informação estar sempre acessível e em condições de ser utilizada pelo usuário autorizado.

- **Integridade**: é a garantia de que a informação não foi alterada, mantendo suas características originais.

- **Confidencialidade**: é a propriedade de que a informação será acessada somente por usuários autorizados, evitando seu conhecimento ou sua divulgação a pessoas sem permissão.

• **Autenticidade**: é a garantia de que a informação foi originada na fonte anunciada, ou seja, que a informação foi produzida por quem diz tê-la produzido.

• **Irretratabilidade ou não-repúdio**: é a característica de não poder negar ações referentes à informação, isto é, o usuário não conseguir negar que enviou a informação, ou a acessou, ou a modificou, ou a copiou, ou a destruiu, ou etc.

Assimile

Segurança da Informação e Comunicações (SIC) significa proteger a informação preservando seu valor e garantindo os princípios da disponibilidade, integridade, confidencialidade, autenticidade e irretratabilidade.

Fazer a segurança da informação (SIC) envolve reconhecer exatamente o valor da informação e como está sendo feita sua gestão (GI) para identificar possíveis vulnerabilidades ou fragilidades nesse processo; como essas vulnerabilidades podem ser exploradas; e quais ameaças podem investir sobre a informação, valendo-se das vulnerabilidades, podendo causar um evento, um incidente ou uma catástrofe de segurança da informação. Dessa forma, conceituaremos melhor o que vem a ser estas três situações decorrentes da ação das ameaças sobre as informações.

• **Evento de segurança da informação**: qualquer fato ocorrido em relação à informação que infringe um princípio da segurança, mas sem causar maiores consequências para a empresa. Ex.: uma falta de energia elétrica deixa a informação indisponível temporariamente.

• **Incidente de segurança da informação**: é uma ocorrência que viola um ou mais princípios da segurança da informação, via de regra, intencionalmente, e que compromete o negócio ou a atividade da organização gerando consequências indesejáveis e prejudiciais. Ex.: um ataque de negação de serviço a um site de comércio eletrônico, interrompendo propositalmente as vendas pela internet e gerando prejuízos.

• **Catástrofe de segurança da informação**: é um incidente de grandes proporções, inviabilizando quase ou permanentemente a atividade da organização. Ex.: o atentado de 11 de setembro de 2001 às Torres Gêmeas, nos EUA, causou a destruição dos principais bancos de dados (Data *Warehouse*) de uma ou duas grandes financeiras americanas, simplesmente extinguindo as atividades delas no mercado.

Ainda sobre os conceitos de SIC, o conjunto de medidas para obter a segurança da informação, citado anteriormente, envolve a Segurança física ou do ambiente, a Segurança lógica ou Controle de acesso, a Segurança da rede ou da transmissão, e a Segurança do armazenamento. A saber:

• **Segurança física**: preocupa-se em evitar o acesso físico às instalações e informações da organização por indivíduos não autorizados ou estranhos à empresa.

• **Segurança lógica**: visa garantir que o acesso à informação eletrônica seja feito dentro dos princípios da SIC. É implementado através de senhas, níveis de acesso e privilégios, etc.

• **Segurança da rede**: consiste em estratégias e políticas – implementadas através de softwares, hardwares e procedimentos – adotadas para impedir o acesso não autorizado, o uso indevido, a modificação ou a negação de serviço durante a transmissão da informação pela rede.

• **Segurança no armazenamento**: é um conjunto de medidas que visa preservar a informação que estiver guardada, envolvendo cópias de segurança (backup), dispositivos de armazenamento (fitas, discos, cartões SD, nuvem, CD/DVD) e redundância de dados.

Para finalizar essa primeira parte da nossa seção, cabe destacar que, em uma organização, deve existir um documento que registre as diretrizes de SIC a serem adotadas pela empresa e que devem ser observadas por todos seus integrantes e colaboradores e, inclusive, aplicada a todos seus sistemas de informação e

processos corporativos. Este documento é chamado de **Política de Segurança da Informação (POSIC)** e estabelece o conjunto de regras e critérios para implantação da SIC na organização, sendo o documento mais importante dentro do sistema de segurança da informação, justamente por estabelecer o que será segurado e como a segurança será realizada.

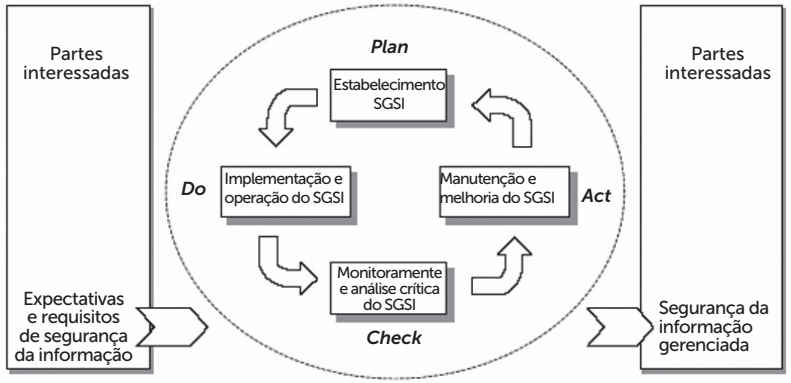
Tudo que nós aprendemos até agora está previsto, descrito e detalhado em uma série de normas e padronizações sobre a Segurança da Informação. As principais normas são as ABNT NBR ISO/IEC da família 27000, que praticamente padronizam toda a atividade relativa à SIC, no Brasil, e cujo estudo, de pelo menos algumas delas, é obrigatório para os profissionais de segurança da informação.

Neste aspecto é importante informar que não existe nenhuma distinção sobre a aplicação das normas na Segurança Pública ou Privada, mas, na verdade, elas são seguidas por quase todas as pessoas e organizações que praticam a SIC de forma séria e consciente. Além das certificações emitidas pela ABNT, é claro, que sempre agregam valor às práticas da empresa, projetando seu nome no mercado e ampliando sua vantagem competitiva.

A família ABNT NBR ISO/IEC 27000 é composta por mais de quarenta normas, sendo a maioria delas direcionada a objetivos específicos dentro da SIC. Contudo, duas delas formam a base para uma SIC bem estruturada e eficiente, são as normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, as quais veremos suscintamente.

A ABNT ISO/IEC 27001:2013 define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI), apresentando um modelo para estabelecer; implementar e operar; monitorar e analisar criticamente; e manter e melhorar um SGSI. O SGSI deve também atender às necessidades, aos objetivos, aos requisitos de segurança, aos processos e ao tamanho e à estrutura da organização. A 27001 se baseia no ciclo PDCA (*Plan-Do-Check-Act* ou Planejar-Executar-Verificar-Atuar) para organizar os processos do SGSI (Figura 2.4 e Tabela 2.2) (ABNT 27001, 2013).

Figura 2.4 | Modelo PDCA aplicado aos processos do SGSI



Fonte: ABNT NBR ISO/IEC 27001 (2013).

Tabela 2.2 | Descrição do ciclo PDCA no SGSI

Plan (planejar) (estabelecer o SGSI)	Estabelecer a política, os objetivos, os processos e os procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e os objetivos globais de uma organização.
Do (fazer) (implementar e operar o SGSI)	Implementar e operar a política, os controles, os processos e os procedimento do SGSI.
Check (checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, aos objetivos e à experiência prática do SGSI, apresentando os resultados para a análise crítica pela direção.
Act (agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Fonte: ABNT NBR ISO/IEC 27001 (2013).

Já a norma ABNT NBR ISO/IEC 27002:2013 apresenta um Código de Prática para a Gestão da Segurança da Informação, ou seja, a norma é um guia para implantação da segurança da informação na organização, operacionalizando o SGSI descrito na 27001 e estabelecendo os objetivos de controle e controles

para o tratamento dos riscos que deverão ser gerenciados. Esses objetivos e controles são descritos em onze seções da 27002, a saber:

- Política de Segurança da Informação.
- Organização da Segurança da Informação.
- Gestão de Ativos.
- Segurança em Recursos Humanos.
- Segurança Física e do Ambiente.
- Gestão das Operações e Comunicações.
- Controle de Acesso.
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.
- Gestão de Incidentes de Segurança da Informação.
- Gestão da Continuidade do Negócio.
- Conformidade.

Pesquise mais

Conheça mais sobre as normas e certificações na área de Segurança da Informação no sítio da ABNT, disponível em: <http://www.abnt.org.br>. Acesso em: 26 abr. 2017.

Complementando essa parte sobre normas e padronizações de Segurança da Informação, existem legislações que tratam especificamente deste assunto no âmbito da Administração Pública Federal (APF), e todas elas estão citadas na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018: versão 1.0. Este documento estabelece objetivos e metas estratégicas de SIC e Defesa Cibernética para os órgãos públicos federais até 2018. Dentre todas as legislações citadas na Estratégia, duas merecem destaque, são elas o Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, e a Instrução Normativa (IN) GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal. Em linhas

gerais, o Decreto nº 3505 determina a implantação da POSIC em todos os órgãos e entidades da APF, com o objetivo básico de garantir o direito à inviolabilidade da intimidade das pessoas e do sigilo das suas comunicações, desenvolvendo e empregando meios de segurança da informação, como forma de manter a soberania do Estado Brasileiro; e a IN nº 1 veio para regulamentar a Gestão de Segurança da Informação e Comunicações (GSIC) da APF, padronizando procedimentos e atribuindo responsabilidades e competências a órgãos específicos. A IN tem ainda várias Normas Complementares (NC) que definem procedimentos específicos em relação à SIC na APF, por exemplo, a NC nº 2, que trata da Metodologia de Gestão de Segurança da Informação e Comunicações.

Como vimos, existem as normas ABNT que padronizam procedimentos em relação à SIC, como forma de apontar as melhores práticas nessa atividade, mas não são de cunho obrigatório; e existem legislações que tratam do assunto no âmbito da Administração Pública Federal e estas sim são determinações que devem impositivamente serem cumpridas por esses órgãos.

Agora que conhecemos algumas normas e padronizações, faremos uma abordagem sobre as ameaças mais comuns. Como dito anteriormente, a SIC será comprometida sempre que uma ameaça conseguir explorar uma vulnerabilidade da informação, violando seus atributos de segurança. De forma geral, existem quatro formas de ataque à segurança da informação (Figura 2.5):

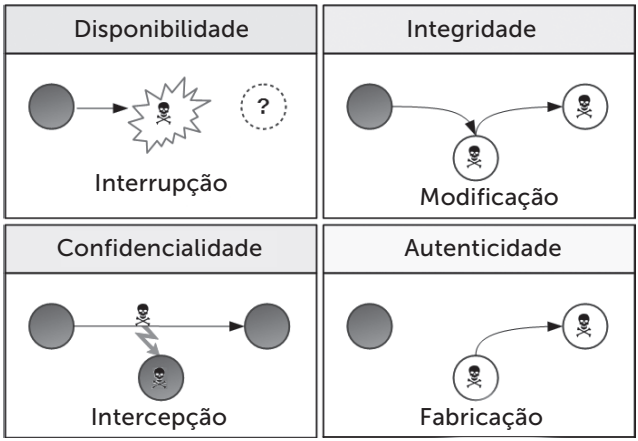
- **Interrupção**: deixa a informação indisponível, não sendo possível acessá-la.

- **Modificação**: quando a informação sofre algum tipo de alteração não autorizada, violando sua integridade.

- **Interceptação**: quando o sigilo da informação é quebrado, ou seja, quando usuários não autorizados acessam a informação.

- **Fabricação**: quando uma informação é "plantada" por uma fonte ilícita, fazendo se passar por uma fonte fidedigna.

Figura 2.5 | Tipos de ataques



Fonte: elaborada pelo autor.

Quando se fala em ameaças à segurança da informação aparece um emaranhado de palavras que, por si só, parecem assustadoras, como: vírus, *worms,* spam*, bots, botnets, exploits, backdoors, brute force, trojan, spywares, malware, keyloggers, screenloggers, sniffers, spoofing, phishing, DoS, DDoS*. Na verdade, tudo isso tem a ver com ataques cibernéticos, desde simples furtos de senhas de usuários comuns até importantes investidas contra bancos de dados de informações críticas de grandes empresas.

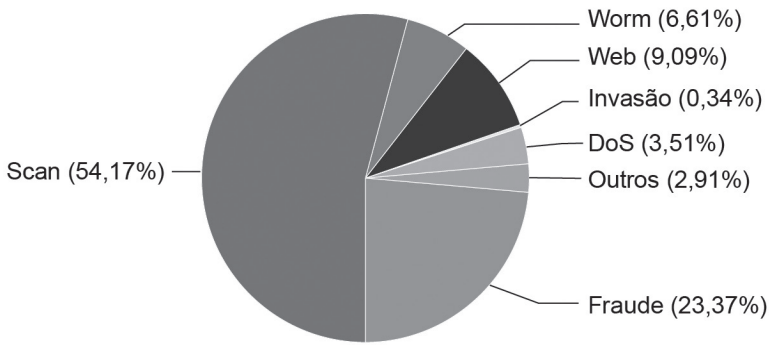
Reflita

E você, aluno, já pensou em como todas essas ameaças, e outras, podem agir sobre suas informações? Quais são suas informações mais valiosas? Elas estão seguras? Quais são as vulnerabilidades delas? Você toma alguma medida para protegê-las? Hoje em dia, nós temos que nos preocupar com essas questões. Você não acha?

No entanto, uma coisa é certa, esse tipo de violação da segurança da informação vem crescendo e se diversificando bastante com o passar dos anos e, sinceramente, já está difícil conseguir identificar todo tipo de ameaça que existe por aí. O que se faz atualmente e tem se mostrado uma boa prática é acompanhar quais são as ameaças que mais estão agindo no espaço

cibernético e planejar a SIC de acordo com essas tendências. É relativamente fácil identificar essas ameaças, podemos consultar estatísticas de incidentes de segurança da informação no portal do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Neste sítio, podemos identificar, por exemplo, que as ameaças mais comuns, em 2015, foram os ***worms***, tipo de verme cibernético muito pior que os vírus porque se propagam rapidamente pelas redes, infectando computadores e executando seus códigos maliciosos; os ***DoS***, ataques de negação de serviço (Denial of Service), impedindo a transmissão de informações; as **invasões**, acessos não autorizados a uma rede ou sistema computacional; os **web**, ações de desfigurar uma página ou comprometer um sítio na internet; os ***scan***, ações de caçar, por varredura, as vulnerabilidades existentes em redes de computadores para selecionar possíveis alvos; e as **fraudes**, tentativas de obter vantagem lesando pessoas e organizações (Gráfico 2.1) (CERT.BR, 2015).

Gráfico 2.1 | Incidentes reportados ao CERT.br por tipos de ataque



Fonte: <https://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque.html>. Acesso em: 26 abr. 2017.

Realmente não está fácil manter uma informação segura neste ambiente tão hostil e impiedoso no qual vivemos atualmente. Mas sempre existe uma forma de conseguir vencer esses adversários invisíveis e astuciosos. É o que passaremos a estudar a partir de agora, isto é, as defesas e os mecanismos de segurança da Segurança Pública e Privada. O setor público combate as ameaças, normalmente, criando leis que criminalizam as práticas de ataque

a informação; já o setor privado se encarrega de desenvolver ferramentas para combater as ameaças. Os mecanismos de defesa mais utilizados são sempre os mesmos, tanto faz se no âmbito da coisa pública ou privada. Vejamos, portanto, alguns deles.

- **Política de segurança da informação**: é o documento mestre de toda estratégia de segurança, porque prevê que informação deve estar segura, como deve ser feita a segurança, que meios serão empregados e, principalmente, dispõe sobre a atitude das pessoas em relação à SIC, prevendo, muitas vezes, punições em caso de não cumprimento do previsto.

- **Atualização de softwares**: é muito importante para a SIC que a infraestrutura na qual a informação circula esteja sempre livre de bugs e vulnerabilidades. Dessa forma, deve-se atualizar periodicamente o sistema operacional e os aplicativos de computador.

- **Controle de acesso**: medida que visa evitar acesso não autorizado à informação, pode ser físico, determinando quem pode acessar quais dependências da organização; e lógico, implementado por meio de contas, senhas e privilégios de acesso.

- **Antivírus, AntiSpam e AntiSpyware**: são softwares que protegem o sistema computacional de ataques desses *malwares*, evitando problemas diversos com a SIC.

- **Cópias de segurança (backup)**: previnem contra a perda de dados e informações decorrentes tanto de ataques intencionais quanto de falhas de hardware, software e peopleware.

- **Firewall**: é o dispositivo que aplica as regras da POSIC na rede interna da organização, protegendo a transmissão de informações entre a rede privada da empresa e a pública (internet).

- **Criptografia**: além de ser uma técnica de ocultação da

informação, a criptografia vem se mostrando como uma das mais poderosas ferramentas para a SIC, sendo empregada para garantir de forma muito eficaz a integridade, confidencialidade e autenticidade das informações, através do uso de certificados e assinaturas digitais, protegendo praticamente todos os atributos de violação da informação.

• **Biometria**: é a técnica de usar características físicas únicas (impressão digital, íris, pressão arterial, voz, DNA) para identificar um indivíduo no controle de acesso, eliminando a possibilidade de uma pessoa utilizar a senha ou o cartão de acesso de outrem; também vem sendo bastante empregada na SIC, particularmente, contra a irretratabilidade.

• **Registro de eventos (Log)**: é a prática de registrar os fatos ocorridos em um sistema computacional e armazená-los em arquivos, chamados logs, mantendo-se um histórico de tudo que aconteceu com a informação durante sua circulação pela infraestrutura de TIC, possibilitando o monitoramento das atividades dos sistemas de informação e a averiguação dos eventos e incidentes de segurança.

A despeito de todos esses mecanismos de defesa, deve-se ter especial atenção com o principal responsável pelo comprometimento da segurança da informação em uma organização, qual seja, o **usuário**. Já foi comprovado por diversas pesquisas e estatísticas que o usuário é a maior falha de segurança que existe, por isso, atuar sistematicamente sobre ele é uma ótima prática no contexto da SIC. Devemos manter uma rotina constante de conscientização do usuário sobre a segurança da informação, promovendo campanhas e workshops que realmente tragam esse assunto para seu dia a dia, alertando-o sobre os riscos de deixar uma porta aberta, um documento em cima da mesa, largar o *smartphone* em qualquer lugar, divulgar dados pessoais na internet (e-mail, telefone, endereço, nome de familiares, rotina diária, viagens, etc.), acessar links de e-mails ou sites escusos na internet, compartilhar senhas de acesso com colegas de trabalho, tratar de assuntos de trabalho em ambiente inadequado (ônibus, taxi, bar, academia) e muitos outros.

Exemplificando

A título de ilustração da importância do usuário na segurança da informação, podemos citar o caso do vazamento das informações da Agência de Segurança Nacional Norte-Americana (NSA) pelo site WeakLeaks, que ganhou repercussão mundial, inclusive, com reflexos no Brasil, por causa do acesso às mensagens eletrônicas da Presidente Dilma. O responsável pela publicação das informações secretas foi o ex-técnico da CIA, Edward Snowden, que burlou todos os mecanismos de defesa da NSA, contando apenas com a contribuição de um funcionário da agência que acessou fisicamente as informações em seu local de trabalho.

Assim, após termos passado por todo esse conteúdo, encerramos mais uma seção da nossa unidade de ensino e podemos partir para a próxima atividade.

Sem medo de errar

Com os conhecimentos adquiridos nesta seção, podemos agora ajudar Fernando e o Flávio a manter seus sistemas e informações em segurança, não é mesmo? Vamos a solução da nossa SP, lembrando que, ao responder os questionamentos, você estará realizando uma análise dos de alguns problemas vivenciados na Segurança Pública e Privada sobre a ótica da Segurança da Informação. Assim como ocorreu a invasão no sistema de controle de acesso do Condomínio de Escritórios Gallery, violando, com certeza, a confidencialidade das informações, também poderia ocorrer uma invasão aos sistemas da SSPMG. Você se lembra que, segundo as estatísticas do CERT.br, a invasão é uma das ameaças mais comuns no Brasil? Esse tipo de ataque acontece simplesmente porque não existe sistema totalmente seguro ou segurança 100% eficaz, isto é, não existe sistema sem informações de valor, ou sem vulnerabilidades, ou sem estar exposto a nenhuma ameaça. Mas as invasões acontecem, principalmente, porque existem sistemas sem uma Segurança da Informação e Comunicações - SIC adequada, ou com uma SIC mal dimensionada, deixando de lado as recomendações

e a padronização que vimos nas normas ABNT e legislações correlatas. E, é claro, que algumas ações desse tipo acabam refletindo no aumento da criminalidade, tanto na criminalidade cibernética quanto na criminalidade comum, materializada na forma de sequestros de executivos e assaltos às empresas que tiveram suas informações vazadas ou expostas. Mediante essa situação e na intenção de prevenir suas organizações contra esse tipo de infortúnio, Fernando e Flávio devem adotar um Sistema de Gestão da Segurança da Informação, conforme descrito na ABNT NBR ISO/IEC 27001:2013, para garantir o planejamento, a implementação, a manutenção e a melhoria constante da SIC sob sua responsabilidade. Para tanto, devem analisar criteriosamente quais são as informações sensíveis das suas organizações, levantando as vulnerabilidades na manipulação dessas informações e que tipos de ameaça podem explorar essas vulnerabilidades. Dessa forma, devem planejar a segurança física, lógica, da rede e de armazenamento, empregando mecanismos de defesa, como: firewall, controle de acesso, backup, logs e outros, tudo para manter essas informações seguras. Por fim, devem descrever isso tudo em uma Política de Segurança da Informação a ser adotada na organização e seguida por todos seus integrantes e colaboradores, assim como prevê a ABNT NBR ISSO/IEC 27002:2013. Não esqueçamos que para Flávio tudo isso não passa de diretrizes, recomendações e melhores práticas que a empresa dele pode optar por seguir; mas para Fernando é diferente, porque a SSPMG é um órgão de Segurança Pública e, apesar de ser do Estado de Minas Gerais e não Federal, também tem de seguir suas legislações próprias, sendo bom que ele se informe sobre elas para não deixar de cumprir alguma imposição legal no desempenho de suas atividades.

Feito isso, formate as respostas anteriormente dadas aos questionamentos apresentados no Diálogo Aberto, e fique consciente de que podemos, sim, proteger nossos sistemas, mantendo a disponibilidade, integridade, confidencialidade e autenticidade das nossas informações. Com o mínimo de vulnerabilidades e resguardadas das ameaças, podemos avançar na nossa prática, resolvendo mais uma situação-problema.

Avançando na prática

Recuperando-se de um ataque

Descrição da situação-problema

Caro aluno, continuaremos, agora, com a nossa prática resolvendo mais uma situação-problema. Acompanharemos a rotina de Roberto Rodrigues, um analista de TI que trabalha há cinco anos no SERPRO, que por ser uma empresa Pública Federal da área de TI, segue à risca todas as normas e leis sobre SIC e tem um complexo sistema de segurança da informação para garantir a incolumidade das informações sob sua gestão. Roberto trabalha na manutenção da página do SERPRO na internet, em que tranquilamente desempenha sua missão, acrescentando novidades, melhorando a navegabilidade, aperfeiçoando o design e desenvolvendo outras tarefas dessa natureza. Certo dia, notou que a página do SERPRO estava alterada, com notícias sobre times de futebol e com suas funcionalidades modificadas. E agora? O que aconteceu? Será possível corrigir os problemas da página? Como fazer isso? Por que isso aconteceu? Que mecanismos de defesa falharam? Como investigar esse ataque? Como evitar um novo ataque igual a esse? Parece que a tranquilidade do Roberto se desfigurou muito rapidamente, igual a página do SERPRO na internet. No entanto, nem tudo está perdido! Vamos buscar as soluções e ajudar o nosso Analista de TI a sair dessa?

Resolução da situação-problema

Para ajudar Roberto, começaremos com a identificação do que aconteceu com a página do SERPRO. Isto é fácil, porque foi um ataque característico de modificação e fabricação, violando a integridade e a autenticidade das informações. Este ataque é chamado de "pichação" ou "*defacement*" e faz parte do grupo de ataques **web** que, segundo o CERT.br, responde por quase 10% dos ataques via internet no Brasil. Para resolver este problema e retirar a pichação da página, Roberto deve retirar a página do ar, carregar as cópias de segurança (backup) da página no servidor web e colocar tudo no ar novamente. Pronto, o problema está parcialmente resolvido, isto é, Roberto pode continuar com o

serviço, mas agora é necessário apurar o que aconteceu. Como já vimos, embora o SERPRO tenha uma SIC bem estruturada e eficiente, não está livre de ataques como este, uma vez que as ameaças são imprevisíveis e sempre nos pegam de surpresa. Mas Roberto pode se valer da excelente estrutura de SIC do SERPRO para investigar como tudo aconteceu e que mecanismos falharam, basta analisar os registros de eventos do sistema, ou *logs*. Considerando o tipo de ataque, provavelmente, falham o *firewall*, que não protegeu adequadamente a rede privada do SERPRO das ameaças existentes na internet; o controle de acesso, que não evitou um acesso não autorizado no servidor web; e talvez até a atualização de software, que deixou uma aplicação ficar desatualizada com a exposição de vulnerabilidades já bem conhecidas pelos atacantes. Daqui em diante é só readequar os mecanismos de defesa para evitar um novo ataque com a mesma forma de atuação. A solução ficou muito boa! Agora podemos partir para o nosso questionário.

Faça valer a pena

1. Para entender como funciona um sistema de Segurança da Informação e Comunicações, é preciso ter em mente e bem consolidado o conhecimento sobre o conceito ou a definição de Segurança da Informação e Comunicações, sintetizando as ideias de acordo com as definições apresentadas pelas normas e padronizações que abordam esse tema, assim como a Norma ABNT NBR ISSO/IEC 27001:2013 e a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018: versão 1.0.

Escolha a única alternativa a seguir que contém o conceito correto de Segurança da Informação e Comunicações.

a) É uma maneira de preservar a informação ao longo do tempo e com solidez.

b) Uma forma de defesa que os especialistas em Gestão da Informação utilizam durante o ciclo de vida da informação para garantir os atributos da informação segura.

c) É um conjunto de medidas que visa proteger a informação das ações de atacantes cibernéticos.

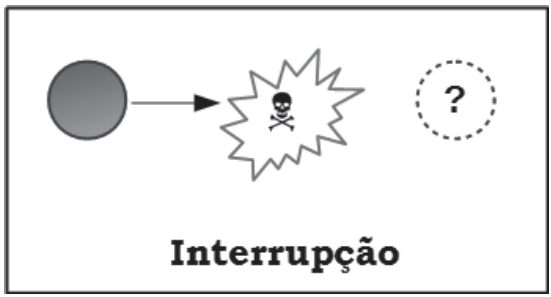
d) Um mecanismo de defesa eficiente e capaz de evitar que a informação sofra qualquer tipo de ataque que viole sua disponibilidade, integridade, confidencialidade, autenticidade e irretratabilidade.

e) É a forma de proteger a informação, preservando seu valor e garantindo os princípios da disponibilidade, integridade, confidencialidade, autenticidade e irretratabilidade.

2. A segurança da informação geralmente é obtida por meio da implantação de um conjunto de medidas que envolve pessoas, processos e tecnologias, visando garantir a disponibilidade, integridade, confidencialidade, autenticidade e irretratabilidade, sendo estes conhecidos como princípios de segurança da informação.

A figura a seguir ilustra um ataque de interrupção contra uma informação. Assinale a única alternativa que contém o princípio de segurança violado pela ameaça neste tipo de ataque.

Figura 2.6 | Ataque de Interrupção



Fonte: elaborada pelo autor.

a) Disponibilidade.

b) Irretratabilidade.

c) Autenticidade.

d) Integridade.

e) Confidencialidade.

3. Rodolfo é um Analista Júnior de Segurança da Informação, que recentemente começou a trabalhar em uma nova organização e, mesmo com sua pouca experiência, logo que assumiu suas funções vigentes verificou que precisaria implementar alguns mecanismos de defesa para melhorar a estratégia de SIC da empresa, uma vez que identificou

deficiências como: a ausência de cópia de segurança dos arquivos; a falta de prevenção contra recebimento de e-mails em massa; e a não codificação da informação.

Marque a alternativa que contém, respectivamente, quais mecanismos de defesa Rodolfo precisará empregar em sua nova empresa para suprir as deficiências identificadas.

a) Backup – AntiSpyware – Criptografia.

b) Registro de eventos – Controle de acesso – Antivírus.

c) Backup – AntiSpam – Criptografia.

d) Registro de eventos – Firewall – Criptografia.

e) Controle de acesso – AntiSpam - Biometria.

Seção 2.3

A segurança na era da internet

Diálogo aberto

Caro aluno, o ciberespaço realmente se tornou um ambiente repleto de riscos e você sabe muito bem disso porque conhece e navega por este universo de sistemas e aplicativos, daí a necessidade de conhecermos profundamente as particularidades desta dimensão, a legislação que regula a atividade cibernética e, principalmente, os sistemas que nos cercam e dos quais dependemos diuturnamente em nossos afazeres. Com base nisso, passaremos a nossa próxima situação-problema, na qual desta vez nosso personagem, o Analista de Riscos da Secretaria de Segurança do Governo do Estado de Minas Gerais - SSPMG, Fernando Bezerra continuava sua nobre e importante tarefa de analisar todos os sistemas da SSPMG, levantar os acessos indevidos e as tentativas de invadir a privacidade dos agentes públicos de sua Secretaria, quando recebeu a chamada do Delegado da Polícia Federal Joaquim Devoto. Este e sua equipe especializada em investigações de crimes eletrônicos investigavam uma rede internacional de pedofilia e, por ocasião do monitoramento das atividades que um determinado cidadão realizava no seu notebook quando navegava pela internet, registrou que o investigado também havia tentado alguns acessos indevidos em outros sistemas de órgãos públicos. Joaquim fez questão de frisar para Fernando que sua equipe, por meio do rastreamento do IP do suspeito, havia verificado que este havia realizado várias tentativas de acesso à Rede INFOSEG e, como o suspeito residia na cidade de Belo Horizonte, o mesmo local em que se encontra a SSPMG, o Delegado Joaquim resolveu contatar seu conhecido na Secretaria para que este redobrasse o monitoramento de sua rede, estabelecendo as medidas necessárias de proteção. Fernando Bezerra ficou refletindo: "a questão da Cibersegurança está cada vez mais séria"; "como posso garantir que nossos sistemas não sofram ataques"? "Se os hackers estão invadindo os sistemas de segurança públicos, talvez eles possam ter acesso aos dados dos cidadãos e dos agentes de segurança,

como os policiais, o que pode trazer vários transtornos para as rotinas de investigação"; "ainda, acho que preciso relembrar os aspectos legais da segurança da informação na internet, mas quais são os principais aspectos necessário para orientar para minha equipe de segurança?" Esses são mais alguns dilemas que você tentará solucionar, caso estivesse na função de Fernando Bezerra. Aluno, tenha sempre em mente que respondendo as reflexões apresentadas você contribuirá para que sejam estabelecidas medidas para compor a política de segurança da informação da SSPMG.

Não pode faltar

Na seção anterior, estudamos a Segurança da Informação de uma forma genérica, no entanto, nesta seção estudaremos especificamente como é a Segurança da Informação na era da internet e os aspectos particulares que envolvem essa vertente muito significativa. Começaremos relembrando que a era da informação nos trouxe uma nova dimensão, o espaço cibernético ou ciberespaço, ou seja, o espaço virtual no qual os sistemas de informação integram-se em uma enorme rede de comunicação. É justamente neste ciberespaço, caracterizado eminentemente pelo ambiente da internet, que a segurança da informação manifesta sua principal vertente, denominada segurança cibernética, ou, simplesmente, cibersegurança (SegCiber), que, segundo Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (BRASIL, 2015), é a forma de garantir a existência e a perpetuidade da Sociedade da Informação, assegurando e protegendo os ativos de informação e sua infraestrutura de TI. Devemos enxergar a cibersegurança como uma tarefa de Estado, assim como os órgãos de segurança pública e as forças armadas garantem a lei, a ordem e a soberania de um país, o Estado também tem de prover a segurança no ciberespaço, salvaguardando as atividades da sociedade neste ambiente. A cibersegurança também pode ser vista como uma dimensão de segurança além da Segurança da Informação e Comunicações ou ainda como uma barreira que antecede a SIC.

Assimile

Cibersegurança é o conjunto de medidas para proteger as informações, os sistemas de informação e os componentes da infraestrutura de TI (hardware, software, rede, bancos de dados e serviços), preservando os princípios da segurança da informação (disponibilidade, integridade, confidencialidade) e visando a garantia das atividades econômicas, políticas e sociais no ciberespaço.

A cibersegurança envolve, na verdade, uma preocupação tanto do Poder Público quanto do Setor Privado, uma vez que é encarado como um fenômeno global e que afeta todos os ramos da sociedade e, até mesmo, indivíduos isolados. Dessa forma, cabe ao Poder Público, além de proteger as informações do Estado como forma de manter a Soberania Nacional, convergir setores de sua estrutura para combater o crime cibernético, praticando a cibersegurança e garantindo um ambiente protegido para os indivíduos, para as organizações e para a sociedade. Do mesmo modo, cabe ao Setor Privado realizar parcerias e investimentos para combater as ameaças cibernéticas e contribuir com o Poder Público na construção da cibersegurança e na consequente prevenção dos ataques cibernéticos. Atualmente, a sociedade, de forma geral, depende do ciberespaço para sua sobrevivência, mesmo porque, nos últimos anos, cresceu exponencialmente o número de transações pela internet, ou como você acha que seria a vida moderna sem o Netflix, Booking, Google, WhatsApp, Uber, Facebook, OLX, Waze, Twitter, Youtube, Yahoo, 5º andar, e-mail ou os sites de comércio eletrônico do Ponto Frio, Casas Bahia, Lojas Americanas, Extra, Wal-Mart, Carrefour, Magazine Luíza. Isto sem falar nas facilidades do governo eletrônico, como: entregar a declaração de imposto de renda, emitir uma guia de INSS/FGTS, registrar um BO, consultar um processo da justiça, agendar um serviço e outras mil e uma atividades que a comodidade da vida moderna nos permite fazer sem sair de casa e, principalmente, sem perder tempo. Por isso, o ciberespaço é tão importante atualmente e deve ser preservado como um ambiente protegido e confiável, tanto quanto às fronteiras internacionais ou às vias públicas, para que a sociedade e o Estado possam desempenhar suas atribuições e afazeres de forma impassível e segura.

Pesquise mais

Já apresentamos a você na Seção 2.2 desta unidade, mas não deixe de conhecer com mais profundidade as estratégias de Cibersegurança do Brasil, acessando a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018: versão 1.0, disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf>. Acesso em: 26 abr. 2017.

Com os adventos do ciberespaço, da cibersegurança, da segurança da informação e do vasto emprego de meios eletrônicos no combate ao crime, cresceram muito os recursos e as possibilidades de monitoramento velado das ações ilícitas, visando a manutenção da segurança em sua expressão mais ampla. A proliferação do emprego desses meios de monitoramento, tanto por parte dos órgãos de segurança pública quanto pelas empresas de segurança privada, trouxe à tona o impasse entre a privacidade e a segurança, principalmente, por causa de vigilância eletrônica.

Exemplificando

A Polícia Militar de São Paulo implantou, desde 2008, um sistema de vigilância por câmeras, que, só na capital, conta com mais de 270 (duzentas e setenta) câmeras, totalizando mais de 350 (trezentas e cinquenta) em todo o Estado; e empregando um verdadeiro batalhão de policiais no monitoramento das imagens. Todo esse esforço foi capaz de reduzir em cerca de 15% os crimes nos locais sob ação das câmeras.

É evidente que a questão da segurança pública é um dever de todos os cidadãos e ninguém deve se esquivar de tomar as providências cabíveis diante de um ato criminoso. No caso do poder público, a segurança é tratada como uma obrigação, uma vez que é dever do Estado prover segurança para a sociedade. No caso da iniciativa privada, a segurança é tratada como um mercado consumidor, ou como uma necessidade diante da fragilidade da segurança provida pelo Estado. Em ambos os casos existe um esforço comum para produzir segurança e o que deve existir, na verdade, é uma cooperação entre todos esses meios no sentido de multiplicar a capacidade de se combater o crime, além

da consciência de praticar a segurança atendendo aos princípios éticos e legais. Dessa forma, a questão da vigilância por câmeras deve ser encarada como mais uma ferramenta a ser empregada em benefício da segurança, cumprindo o mesmo papel da vigilância tradicional executada por agentes de segurança, sendo diferenciada apenas por possibilitar uma abrangência de monitoramento que extrapola a capacidade humana, ou seja, ninguém vê um policial ou vigilante dentro de um banheiro, ou num quarto de hotel, ou em um vestiário, ou até mesmo no interior de uma residência bisbilhotando a vida privada das pessoas; mas vê policiais nas ruas, nas praças, circulando pelo comércio; e também vê vigilantes nas entradas das empresas, nos edifícios empresariais, nas portarias dos condomínios e fazendo rondas. Esta é a questão-chave da vigilância eletrônica, ser empregada visando a coletividade e a vida pública das pessoas, do contrário, talvez se corra o risco de invadir a privacidade do cidadão e este vem sendo o maior problema, porque as pessoas estão se sentindo vigiadas e cerceadas pelo excesso de câmeras existentes. E, realmente, hoje em dia pouca coisa escapa da lente de uma câmera de vigilância, por isso mesmo que este ramo de atividade deve ser muito bem regulamentado, visando o estabelecimento de regras efetivas e capazes de evitar que essa ferramenta legítima seja utilizada para fins torpes ou danosos.

No Brasil, ainda não existe uma lei específica sobre o assunto, a única iniciativa neste sentido é o Projeto de Lei nº 1759/2007, que legisla sobre as empresas de Sistemas Eletrônicos de Segurança, mas que ainda está tramitando no Congresso Nacional. Na ausência da legislação e de uma consciência ética por parte dos agentes da segurança, tanto públicos quanto privados, corre-se o risco de se transformar o cotidiano num imenso BBB, em que a privacidade não passará de um vago conceito. Por essas razões, respeitar a privacidade do indivíduo deve ser um ponto de honra na promoção da segurança, primordialmente, da segurança eletrônica.

A questão de privacidade na Era Digital vai muito além do aspecto da segurança pública e privada, envolvendo também os principais aspectos legais relacionados à Segurança da Informação na internet, os quais giram fundamentalmente em torno das questões de privacidade e criminalização dos delitos

cibernéticos. O direito à privacidade acaba sendo um empecilho ao emprego das medidas de segurança da informação, porque, às vezes, é utilizado como subterfúgio dos mal-intencionados para preservarem o anonimato. Existe também o conflito histórico entre o direito do empregador e a privacidade do empregado, que se manteve, e porventura se agravou, em relação à utilização de recursos cibernéticos de propriedade das empresas, onde existe um precedente para limitar a privacidade, uma vez que a utilização desses sistemas corporativos não se trata da intimidade ou da vida privada, mas sim da vida profissional e do exterior do indivíduo. Já o óbice da caracterização de crimes no ciberespaço é justamente a dificuldade de tipificação desses delitos, isto é, enquadrar os ilícitos cibernéticos na lei e classificá-los como delitos criminosos e passíveis de punição na forma da lei. Este embaraço, muitas vezes, impede a ação da justiça, livrando os criminosos de receberem uma punição pelos males, danos e prejuízos por eles causados. Embora a segurança da informação seja uma atividade totalmente lícita e necessária, às vezes, enfrenta alguns percalços para atingir seus objetivos, mas tudo isso deve ser encarado como fatores a serem considerados na hora de se estruturar a segurança da informação, de modo que ela seja eficaz e rigorosamente dentro dos limites estabelecidos pela lei.

O direito à privacidade está descrito no artigo 5º da CF88 que enuncia que todos são iguais perante a lei e garante aos brasileiros e aos estrangeiros que moram no Brasil a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade. E ainda determina nos seus incisos X, que a intimidade, a vida privada e a imagem das pessoas são invioláveis, garantindo direito, inclusive, à indenização pecuniária decorrente de sua violação; e XII, que o sigilo da correspondência, das comunicações e dos dados dos cidadãos também não pode ser infringido, exceto por ordem judicial. Somente lendo o texto da constituição já é perceptível que fazer SIC envolve lidar com a preservação desses direitos e que eles vão interferir significativamente na maneira de implementá-la. Particularmente, o inciso XII do artigo 5º é regulado pela Lei nº 9.296/1996 que dispõe sobre a interceptação de comunicações telefônicas, em sistemas de informática e redes de computadores, regulando claramente as situações em que se pode quebrar o sigilo das comunicações de uma pessoa ou organização. É importante

frisar que tal deliberação só pode ser determinada pela justiça. A questão da privacidade eletrônica também é regulamentada pela Lei nº 12.965/2014, considerada o Marco Civil da internet no Brasil, e que estabelece os princípios, as garantias e os deveres para a utilização da internet no País, e logo em seu artigo 3º é determinado que o uso da internet deve seguir o preceito da preservação da privacidade. Além disso, embora não exista lei específica sobre a privacidade dos dados, corre no Congresso Nacional o Projeto de Lei nº 5.276 de 2016 que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Essa questão é pertinente porque estabelece que não podemos sair por aí devassando a vida das pessoas eletronicamente, vasculhando seus hábitos e atitudes e aplicando regras corporativas à revelia da legislação vigente no país, ou seja, a privacidade das pessoas no meio eletrônico ou ciberespaço é uma questão fundamental para a legislação brasileira e, por causa disso, deve ser também uma preocupação muito séria e ponderada dos encarregados pela SIC nas organizações, sob o risco de passarem de defensores da informação para o banco dos réus.

Reflita

Suponha que um empregado foi chamado pelo seu chefe no trabalho e este apresentou a demissão daquele por justa causa, sob a alegação de que o empregado tinha revelado informações sensíveis da empresa para um concorrente através do e-mail corporativo. E que, além disso, ele seria processado por essa conduta. O que você acha disso? O empregador pode fiscalizar as mensagens de e-mail corporativo dos empregados? O empregado não tem direito à privacidade? A correspondência não é inviolável? Como ficam os direitos constitucionais do empregado? Será que ele pode ser demitido e processado?

Outro aspecto a ser considerado no contexto da SIC e a tipificação de crimes cometidos no ambiente cibernético, que até bem pouco tempo atrás sequer tinham uma legislação específica, que somente irrompeu após o caso do vazamento das fotos íntimas da atriz Carolina Dieckmann, com a aprovação da Lei nº 12.737/2012, apelidada com o nome da atriz, dispondo sobre a tipificação criminal de delitos cibernéticos, quando, então, passaram a ser considerados crimes as ações delituosas

de invasão de sistemas de informação, interrupção de serviço de comunicação de dados de utilidade pública, falsificação de documentos eletrônicos e a falsificação de cartões de crédito ou débito para uso na internet.

Para que um sistema de segurança da informação possa conviver harmoniosamente com todos os desígnios da legislação, sem que a organização enfrente qualquer tipo de problema com a justiça, as empresas devem se esmerar em elaborar uma Política de Segurança da Informação e Comunicações (POSIC) que estabeleça diretrizes claras em relação ao uso da internet e, principalmente, do correio eletrônico e das redes sociais pelos seus empregados. A POSIC, conforme já foi verificada na Seção 2.2, deve deixar incontestavelmente explícito que os usuários dos sistemas de informação e da internet da empresa, no momento em que se submetem voluntariamente à POSIC, renunciam ao direito de privacidade no tocante às informações manipuladas em seu ambiente de trabalho e utilizando os recursos de TI de propriedade da organização e disponibilizados aos empregados estritamente para fins profissionais, sem, portanto, nenhum cunho pessoal. A POSIC também deverá deixar expresso de forma transparente que a organização poderá realizar fiscalizações e auditorias em todo o tipo de informação registrada em seus sistemas, visando averiguar se a utilização destes está de acordo com os objetivos do negócio. Ainda dentro deste princípio de acordar previamente com o empregado os termos da utilização dos recursos de TI corporativos, a POSIC também deve prever as punições a que os usuários estarão sujeitos nos casos da não observância das diretrizes da organização, sendo que essas punições podem chegar até ao desligamento do funcionário, dependendo da gravidade da transgressão cometida por ele (BASSO, 2005).

A despeito de todos esses dilemas que envolvem a cibersegurança, a privacidade, os crimes cibernéticos, a segurança pública e privada, a segurança da informação e o código de leis, a preocupação com a ordem pública, o patrimônio e o bem comum devem sempre ser o foco principal dos agentes de segurança. Dessa forma, tanto o poder público quanto a iniciativa privada se valem das facilidades do mundo moderno utilizando sistemas de informação, através da internet, para viabilizar ações e fazer o gerenciamento de seus sistemas de segurança.

Depois que vimos os aspectos legais da segurança da informação na internet, vejamos, agora, alguns exemplos de SI da Segurança Pública e Privada na internet. Vamos começar pelo Portal Sinesp ou Sistema Nacional de Informações de Segurança Pública, uma iniciativa da Secretaria Nacional de Segurança Pública do Ministério da Justiça, que funciona totalmente pela internet, disponível em: <www.sinesp.gov.br>. Acesso em: 3 jul. 2017. (Figura 2.7), com o objetivo de disponibilizar serviços e integrar bancos de dados de segurança pública de todos os Estados da Federação, concentrando-se na disponibilização de dados estatísticos e na emissão de relatórios acerca da criminalidade no país, além de ter uma área restrita aos agentes da segurança pública, integrando as informações das polícias. O sistema conta também com o Sinesp Cidadão, um aplicativo que permite consultar a situação de veículos no banco de dados do Departamento Nacional de Trânsito – Denatran; e com o Sinesp Seguro, um sistema totalmente protegido e criptografado para a comunicação e o compartilhamento de documentos entre os integrantes da rede do Ministério da Justiça, criando um ambiente cibernético que interliga todas os setores que atuam na segurança pública.

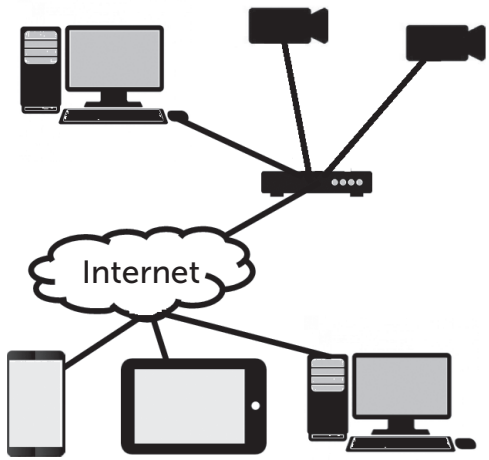
Figura 2.7 | Portal Sinesp na Internet

Fonte: <https://www.sinesp.gov.br/inicio>. Acesso em: 4 mai. 2017.

Como exemplo de sistema de informação de segurança privada pela internet, podemos apresentar os sistemas de vigilância por câmeras com acesso remoto, em que o vigilante, ou o cliente,

ou o dono da propriedade que está sendo vigiada, pode acessar, pela internet, as imagens geradas pelas câmeras. O sistema fundamentalmente é estruturado ligando-se uma câmera IP a um switch, hub ou roteador, por cabos ou wireless. Esses hardwares permitem o aceso de vários equipamentos à rede local e à internet, assim sendo, a câmera receberá um endereço IP, passará a estar on-line e poderá ser acessada pela internet (Figura 2.8).

Figura 2.8 | Sistema de vigilância com câmera IP



Fonte: elaborada pelo autor.

Existe uma variedade enorme de câmeras IP no mercado, alguns modelos permitem acessar as imagens pelo navegador de internet, outros necessitam de um aplicativo próprio para acesso às imagens, que geralmente são gratuitos e disponíveis para download. No contexto do sistema de vigilância é possível ainda definir quem terá permissão para acessar as imagens da câmera e outros privilégios de usuário. Esse tipo de sistema vem sendo largamente utilizado e de uma forma muito variada, como: em escolas infantis, permitindo aos pais monitorarem a criança ou o bebê; em construções, permitindo ao proprietário acompanhar o andamento da obra; no comércio, possibilitando ao dono verificar a segurança no período em que a loja está fechada; em oficinas, franqueando ao dono do veículo fiscalizar os serviços que estão sendo executados pelos mecânicos; e muitas outras formas de emprego. Neste exemplo, cabe destacar a importância de se

contar com um espaço cibernético seguro e confiável, para que as imagens das câmeras possam navegar pela Grande Rede sem contratempos, a despeito de toda a adversidade do ambiente.

Chegamos ao final de mais uma unidade didática. Já podemos quase nos considerar especialistas em Sistemas de Informação em Segurança, mas é melhor estudarmos mais um pouco, pois vencemos somente a primeira metade do desafio. Vamos prosseguir resolvendo a nossa situação-problema?

Sem medo de errar

Vamos resolver a nossa situação-problema envolvendo, mais uma vez, o nosso personagem Fernando Bezerra. A missão de assegurar que um sistema conectado à internet esteja resguardado de ataques de hackers não é fácil. Já vimos isso na seção anterior, mas algumas providências são sempre necessárias para que nossos sistemas possam cumprir o papel deles no ciberespaço com um nível de segurança adequado. Essa garantia vem de um gerenciamento criterioso do sistema de SIC, sempre mantendo um monitoramento das ameaças com maior possibilidade de atacar nossos sistemas. No caso da SSPMG, essa ameaça está configurada pelas atividades de um elemento que vem tentando invadir sistemas da Segurança Pública, conforme relato do Delegado Joaquim. Frente a este cenário e para continuar garantindo que os sistemas da SSPMG não sofram ataques, Fernando Bezerra deve estudar criteriosamente como o elemento tentou invadir o sistema da Rede INFOSEG e qual é a vulnerabilidade que ele tentou explorar. Tão logo consiga desvendar essas questões, Fernando deverá verificar se seus sistemas também apresentam essas vulnerabilidades, tomando as devidas providências para reduzi-las ou eliminá-las, tais como ampliar as regras de segurança do firewall, atualizar softwares aplicativos e antivírus e auditar os arquivos de log, por exemplo; tudo isso em conjunto com o monitoramento cerrado dos acessos aos sistemas da SSPMG. Tomadas as devidas medidas de defesa contra essa ameaça iminente, dificilmente, os atacantes lograrão êxito em tentativas de acesso aos dados dos cidadãos e dos agentes de segurança, e as rotinas de investigação poderão seguir normalmente. Fernando deve também relembrar para sua

que embora a segurança esteja sendo reforçada, aumentando principalmente o nível de monitoramento na rede, a privacidade dos usuários deve ser sempre preservada como prevê a CF88, a Lei nº 9.296, de 24 de julho de 1996, e a Lei nº 12.965, de 23 de abril de 2014, Marco Civil da Internet no Brasil; e que, caso ocorra algum tipo de acesso indevido aos sistemas da SSPMG, o responsável pela invasão responderá criminalmente, conforme estipulado na Lei nº 12.737, de 30 de novembro de 2012, Lei Carolina Dieckmann. Dessa forma, os sistemas sob os cuidados do Fernando Bezerra continuarão funcionando de forma segura e eficiente, além de você ter contribuído para a elaboração da Política de Segurança da Informação da SSPMG. O que você achou desta solução? Ela é mais um conteúdo que você deve analisar e considerar no seu aprendizado. E para consolidar ainda mais nossos conhecimentos, vamos tentar responder mais uma situação-problema.

Avançando na prática

Vigilância: serviço ou desserviço?

Descrição da situação-problema

Agora, analisaremos um fato ocorrido no Residencial Paraíso da Águas, um condomínio com oito prédios e mais de 600 apartamentos, onde convivem em torno de 2000 moradores. Atualmente, o residencial vem enfrentando um grande problema, porque um funcionário da portaria, com a intenção de burlar a segurança do sistema com um software de quebra de senha do administrador, se aproveitava das câmeras de vigilância para xeretar as pessoas em trajes de banho na piscina e ainda compartilhava as imagens capturadas em sites escusos na Internet. Até que em um certo dia bateu na porta do condomínio um agente da Polícia Federal com um mandado de busca e apreensão, objetivando recolher o computador da portaria para investigação do crime de pedofilia na internet. Pronto, estava feito o estrago. Será mesmo crime o que foi praticado pelo porteiro? Como a Polícia Federal descobriu isso? E como a PF provará isso através do computador apreendido? Como fica a questão da privacidade das pessoas que tiveram suas imagens veiculadas na internet? O que deve

ser mudado na segurança do residencial para que isso não aconteça de novo? Que responsabilidade terá o condomínio? E você, caro aluno? O que pode fazer para esclarecer esses questionamentos? Comece empregando os conhecimentos adquiridos nesta seção e siga em frente!

Resolução da situação-problema

A situação não está nada boa no residencial Paraíso da Águas, mas vamos esclarecer alguns pontos importantes. O porteiro realmente cometeu crime; primeiro porque violou indevidamente o mecanismo de segurança do sistema de vigilância para obter as imagens das câmeras, conforme prevê a Lei nº 12.737, ou a Lei Carolina Dieckmann, sobre a qualificação de crimes cibernéticos; além do crime de pedofilia, quando acessou e compartilhou na internet conteúdo erótico envolvendo menores de idade. A Polícia Federal descobriu o delito porque monitora esse tipo de atividade no ciberespaço, cumprindo o dever do Estado de manter segura a sociedade, e chegou ao residencial através do endereço do computador na internet (IP). A partir daí o computador apreendido é investigado, uma vez que nele estão registrados todos os fatos e as atividades executados por cada usuário (*logs*), permitindo identificar quem especificamente cometeu as infrações. Houve claramente violação da privacidade das pessoas que tiveram suas imagens veiculadas na internet, conforme previsto no inciso X do artigo 5º da CF88. O fato ocorrido deve gerar mudanças na segurança do condomínio, principalmente, no que se refere à senha do administrador do sistema de vigilância, que deverá ter um formato e uma rotina menos vulnerável aos softwares de quebra de senha. Por último, o Residencial poderá ser responsabilizado pelo ocorrido e, provavelmente, pelas indenizações pecuniárias devida aos moradores envolvidos no fato, também conforme o inciso X do artigo 5º da CF88. O grande trunfo que o condomínio pode ter nas mãos, e que talvez resguarde ou minimize a responsabilidade do residencial, é a POSIC, que, dependendo do que nela foi estabelecido, pode carrear a responsabilidade para o porteiro.

Faça valer a pena

1. A Era da Informação nos trouxe uma nova dimensão: o ciberespaço. Com esta dimensão veio novos desafios para a segurança da informação, promovendo uma nova vertente deste esforço, doravante denominada cibersegurança, qual seja, a segurança dessa nova dimensão da vida moderna. Diga-se de passagem, a mais difícil missão no ramo da segurança atualmente.

Analise as sentenças a seguir em relação à cibersegurança.

I. A cibersegurança é importante porque, atualmente, a sociedade depende do ciberespaço para sua sobrevivência.

II. Um conjunto de medidas que visa proteger a informação é a cibersegurança.

III. A cibersegurança envolve tanto o Poder Público quanto o Setor Privado, uma vez que é encarada como um fenômeno global e que afeta toda a sociedade.

IV. A cibersegurança ainda não é uma realidade no Brasil, tendo em vista que não existe nenhum órgão do Poder Público com essa incumbência.

Assinale a alternativa que contém somente as sentenças corretas:

a) I, II e III.

b) I e III.

c) I, III e IV.

d) II e III.

e) III e IV.

2. Existe uma certa dificuldade na caracterização de crimes no ciberespaço, isto é, enquadrar os ilícitos cibernéticos na lei e classificá-los como delitos criminosos e passíveis de punições legítimas. Este embaraço, muitas vezes, impede a ação da justiça, livrando os criminosos de receberem a devida sanção pelos males, danos e prejuízos por eles causados.

De certa forma, essa dificuldade foi amenizada quando passaram a ser considerados crimes a invasão de sistemas de informação e a interrupção de serviço de comunicação de dados de utilidade pública.

Qual foi a legislação que criminalizou as ações descritas no texto anterior?

a) Lei nº 9.296/96.

b) Projeto de Lei nº 1759/2007.

c) Lei nº 12.965/2014, considerada o Marco Civil da internet no Brasil.

d) Constituição da República Federativa do Brasil, 1988.

e) Lei nº 12.737/2012, Lei Carolina Dieckmann.

3. Para que um sistema de SIC possa conviver com as imposições das leis sem enfrentar problemas com a justiça, as organizações devem elaborar um(a) _____ que estabeleça diretrizes claras em relação ao uso da internet e, principalmente, do correio eletrônico e das redes sociais pelos seus empregados. Deixando claro que os usuários renunciam ao direito de _____ em relação às informações manipuladas no ambiente de trabalho e utilizando os recursos de TI da empresa, disponibilizados estritamente para fins _____.

A partir do texto anterior, assinale a alternativa que contém as palavras adequadas às lacunas.

a) Política de Segurança da Informação – propriedade – particulares.

b) Contrato de Trabalho – propriedade – pessoais.

c) Política de Segurança da Informação – privacidade – profissionais.

d) Contrato de Trabalho – propriedade – profissionais.

e) Política de Segurança da Informação – propriedade – pessoais.

Referências

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação** - Técnicas de segurança - Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2013. 2. ed. Rio de Janeiro, 2013.

CHIAVENATO, Idalberto. **Introdução à teoria geral da administração**. 7. ed. Rio de Janeiro: Elsevier, 2004.

BASSO, M. **E-mail e o direito de privacidade no trabalho**: pode a empresa bisbilhotar o empregado?. 2005. Disponível em: <http://www.buscalegis.ufsc.br/revistas/files/anexos/5453-5445-1-PB.htm>. Acesso em: 2 maio 2017.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 3 jul. 2017.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 3 jul. 2017.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 3 jul. 2017.

_____. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018: versão 1.0** / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações – Brasília: Presidência da República, 2015. 82 p.: il. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf>. Acesso em: 26 abr. 2017.

BROGNOLI, Alvaro. **Implementação de um sistema de inteligência de negócio** – Business Intelligence (BI). 2010. Disponível em: <http://alvarobrg.blogspot.com.br/2010/04/implementacao-de-um-sistema-de.html>. Acesso em: 20 abr. 2017.

FRANCO, Décio Henrique; RODRIGUES, Edna de Almeida; CASELA, Moisés Miguel. **Tecnologias e Ferramentas de Gestão**. Campinas: Alínea, 2013. 361 p.

LAUDON, Kenneth C.; LAUDON, Jane P.. **Sistemas de de informação gerencial**. 7. ed. São Paulo: Pearson Prentice Hall, 2007. 452 p. Tradução Thelma Guimarães; revisão técnica Belmiro N. João.

STAIR, Ralph M.; REYNOLDS, George W.. **Princípios de sistemas de informação**. 11. ed. São Paulo: Cengage Learning, 2015. 719 p. Tradução Noveritis do Brasil; revisão técnica Tânia Fátima Calvi Tait..

Sistemas e informações na segurança pública e privada

Convite ao estudo

Prezado aluno, após termos aprendido sobre a Gestão e a Segurança da Informação, daremos continuidade na nossa disciplina explanando sobre os Sistemas e as Informações na Segurança Pública e Privada, tema este de extrema importância, visto que praticamente todas as ações de segurança, atualmente, são apoiadas por algum sistema ou por alguma tecnologia da informação, recursos que permitiram uma considerável melhoria da qualidade e eficiência dos produtos e serviços de segurança. No decorrer desta unidade de ensino, veremos a lei de acesso a informação e os sistemas e informações na segurança pública e privada.

Para contextualizar nossa aprendizagem, consideraremos o seguinte cenário: Luke da Silva era um garoto que adorava ver filmes de guerra. Os épicos que falavam da Guerra do Vietnã eram seus preferidos. Na sua cabeça, só havia imagens suas voando de helicóptero, utilizando tanque de guerra, atirando com armas automáticas, fuzis e pistolas, enfrentando as adversidades da guerra, tudo isso como se fosse um herói. Quando fez 18 anos e teve de se alistar, para ele, aquilo parecia um presente. Enquanto muitos queriam fugir do alistamento, ele foi vibrando para servir em um Batalhão de Infantaria Leve, na cidade de Caçapava, no interior do estado de São Paulo. Aquilo foi uma glória para um rapaz de cidade do interior. Ele curtiu tudo que lhe foi permitido no ano de seu serviço militar obrigatório, mas não conseguiu prosseguir na carreira no Exército, por falta de vaga para engajamento. Nesse contexto, pensou: "eu não vou entregar os pontos". Ele sabia que sua vida seria sempre a de andar fardado, mexer com armas e esse era seu destino.

Assim, Luke decidiu que procuraria uma Escola de Formação de Vigilantes, para que pudesse continuar na atividade, ganhar um dinheiro lícito e viver um pouco de emoção. Mas, Luke não ficaria só no ramo da Segurança Privada, mas sim integraria a Polícia Militar, seu maior objetivo. Para tanto, ele teria de começar pela carreira de vigilante. Assim, será que Luke conseguirá atingir sua meta?

Com certeza, a jornada de Luke não será fácil e ele enfrentará vários desafios, considerando que a atividade de um vigilante ou policial nem sempre é repleta de emoções e aventuras. Os profissionais desta área devem ter conhecimentos que os permitam desempenhar várias atividades dentro das inúmeras oportunidades que o ramo da segurança oferece, ainda mais nos dias atuais, que a tecnologia vem tomando conta de praticamente todas as áreas de atuação profissional, ou você acha que a segurança está fora dessa? Será que a tecnologia é importante nesta área? A informatização está tão presente assim na segurança? Quais são os sistemas e as tecnologias mais utilizados?

Para entendermos como a tecnologia e, particularmente, os sistemas de informação são empregados no ramo da segurança, nesta unidade, discorreremos sobre a lei de acesso à informação, com foco nos seus pontos mais importantes, e traremos, além do conhecimento, uma reflexão sobre alguns aspectos que devemos observar na nossa relação com a informação pública. Feito isso, passaremos a conhecer um pouco mais dos Sistemas e das Informações na Segurança Pública e Privada, com o propósito de detalhar mais objetivamente este assunto.

Bons estudos!

Seção 3.1

Lei de acesso à informação (Lei nº 12.527, de 2011)

Diálogo aberto

Daremos início a mais uma das nossas situações-problema, desta vez, envolvendo o personagem Luke da Silva, que, após dar baixa no Exército Brasileiro em Caçapava, São Paulo, decidiu buscar seu objetivo de trabalhar na área de segurança, matriculando-se no curso de Reciclagem e Formação de Vigilantes em uma escola de formação, em São José dos Campos. Logo que terminou o curso, ele foi trabalhar na Defender vigilância, Escolta e Guarda. Sua primeira função foi a de Vigilante, responsável pela segurança patrimonial de uma empresa produtora de grãos. Luke ficou contente, porque a empresa estava localizada em um bairro de pouco histórico de criminalidade. Ele sabia que poderia estudar, nas horas vagas, para o concurso para Soldado da Polícia Militar (PM) do Estado de São Paulo, e concretizar seu sonho de ser militar.

Prosseguindo com seu objetivo, matriculou-se no curso preparatório para o concurso da PM. Logo nas primeiras aulas, foi lhe apresentado o conteúdo que seria solicitado nas provas do concurso. Um dos assuntos era a Lei de acesso à informação. O rapaz não entendia o motivo de ter que estudar sobre isso, mas, mesmo assim, continuou seus estudos. Para ajudá-lo, a apostila que recebeu abordava questões de concurso anteriores:

- Quais são os principais aspectos da Lei de acesso à informação?
- Como é realizada a classificação das informações públicas e privadas?
- Existe um controle da informação?
- Existem prazos para que os órgãos públicos respondam aos pedidos de informação realizados pelos cidadãos comuns?
- Quem pode solicitar e qual informação deve ser preservada? Ou será que tudo pode ser acessado por qualquer pessoa?

Como a proposição é que seja apresentada uma **análise escrita sobre a comparação entre os sistemas de informação da segurança**

pública e privada, procure sistematizar esta comparação com o Quadro 3.1, apresentado a seguir.

Quadro 3.1 | Comparação entre os sistemas de informação da segurança pública e privada

CLASSIFICAÇÃO DAS INFORMAÇÕES	
PÚBLICA	PRIVADA
PRAZOS DE SIGILO	
PÚBLICA	PRIVADA
CONTROLE DAS INFORMAÇÕES	
PÚBLICA	PRIVADA
PRAZOS PARA RESPOSTA A PEDIDOS DE INFORMAÇÃO	
PÚBLICA	PRIVADA
ACESSO ÀS INFORMAÇÕES	
PÚBLICA	PRIVADA

Fonte: elaborado pelo autor.

Nesse cenário, vamos nos colocar na posição de Luke e ajudá-lo para que ele possa esclarecer todas essas dúvidas e melhor se preparar para acertar todas as perguntas da prova? Lembre-se de que as respostas aos questionamentos do rapaz deverão compor o produto: a análise escrita sobre a comparação entre os sistemas de informação da segurança pública e privada. Além das respostas de Luke, deverá ficar claro no produto qual é o papel da Lei de acesso à informação em um sistema de segurança pública e em um de segurança privada. Dessa maneira, prepare-se e siga em frente! Boa Sorte!

Não pode faltar

Prezado aluno, finalizamos nossos estudos na unidade de ensino anterior conhecendo como é feita a gestão da informação e os aspectos fundamentais relacionados à segurança da informação.

Agora, prosseguiremos na nossa missão, estudando como o Governo Federal regulamenta o acesso às informações sob custódia de um órgão público. Na prática, este acesso é regulamentado pela Lei nº 12.527, de 18 de novembro de 2011, chamada de Lei de acesso à informação ou simplesmente LAI. Esta dispõe sobre os direitos garantidos aos cidadãos brasileiros de receberem de qualquer um dos órgãos públicos acesso às informações particulares, coletivas ou de interesse geral, conforme estabelecido no inciso XXXIII, do artigo 5º da Constituição Federal de 1988 – CF88, além de informações administrativas sobre os atos dos governos municipal, estadual e federal, segundo o previsto no inciso II, do parágrafo 3º do artigo 37 da CF88. A LAI também dispõe sobre a responsabilidade da administração pública em permitir o acesso à informação para quem dela precisar, obedecendo o disposto no parágrafo 2º, do artigo 216 da Constituição Federal de 1988.

A LAI, além de estipular que todo órgão ou toda entidade pública tenha um serviço de atendimento para prestar informações aos cidadãos, assegura que todos terão acesso às informações sobre:

- As atividades dos órgãos e das entidades públicas, bem como à sua organização e aos serviços prestados.
- A gestão e utilização dos recursos públicos.
- Os processos licitatórios, incluindo editais e contratos.
- As propostas e ações dos órgãos públicos e seus resultados.
- Os resultados de fiscalizações e controles executados pelos órgãos governamentais, responsáveis pelo controle dos gastos públicos.

O ponto principal desta lei é tornar transparente as ações de todos os órgãos públicos, entidades vinculadas à administração pública e às organizações privadas sem fins lucrativos que receberam verbas públicas para projetos de interesse coletivo, uma vez que o acesso às informações relativas aos atos destes órgãos, entidades e organizações podem ser franqueadas a qualquer cidadão ou organização que assim o desejarem.

Reflita

A proposta da Lei de acesso à informação é realmente muito louvável e interessante do ponto de vista da transparência dos atos dos poderes públicos. Mas será que esta abertura total das informações é mesmo válida? Alguém pensou que isso talvez possa trazer problemas para os órgãos públicos? Será que a exposição total dos gastos dos órgãos públicos acarretará em algum tipo de vulnerabilidade? Se você fosse funcionário do município e seu contracheque fosse exposto ao público, você se sentiria ameaçado ou constrangido? Qual é seu pensamento sobre a LAI?

Para que possamos começar a entender e conhecer a lei de acesso à informação, verificaremos, primeiramente, qual é o procedimento para que se possa ter acesso às informações dos órgãos públicos, tal procedimento está previsto e descrito no Capítulo III, da LAI, intitulado *Do Procedimento de Acesso à Informação*. Neste capítulo, está estabelecido que para ter acesso à informação deve ser realizado um pedido de acesso, que pode ser feito por qualquer um que tenha interesse na informação, tendo de fornecer apenas sua identificação e especificar qual informação deseja acessar. Tal pedido deve ser encaminhado pelos meios indicados pelo órgão custodiante da informação requerida, podendo, inclusive, ser através de páginas na internet. Se as informações solicitadas forem de interesse público, não poderão ser exigidos motivos para a liberação do acesso às informações. O órgão ou a entidade pública também deve conceder o acesso imediato às informações solicitadas e, caso o acesso imediato não seja possível, o órgão terá um prazo de 20 (vinte) dias, podendo ainda ser prorrogado por mais 10 (dez) para marcar uma data para liberação do acesso à informação ou apresentar integralmente as devidas justificativas para a não liberação do acesso. Caso esta seja devido à classificação sigilosa da informação, o interessado no acesso também deverá ser informado sobre como proceder nesse expediente. Nos casos em que o acesso à informação for negado, o interessado poderá recorrer desta negativa junto ao próprio órgão, manifestando-se em um prazo de 10 (dez) dias, ou ainda apelando para a Controladoria-Geral da União (CGU). Em ambos as situações, o órgão ou a CGU terá o prazo de 5 (cinco) dias para responder ao recurso do interessado. Os procedimentos para acesso à informação também incluem as informações disponibilizadas ao público, principalmente por meio digital, no qual, independentemente de qualquer pedido de acesso, o

interessado pode pesquisar e acessar as informações através de seus próprios meios, sem nenhum tipo de solicitação a órgãos públicos ou entidade pública. A LAI garante ainda que a busca e o fornecimento de qualquer informação do poder público sejam feitos de forma gratuita, excetuando-se as despesas com cópias (xerox) ou impressões. Portanto, podemos ter acesso à informação pública através de um pedido de acesso ou de um mecanismo de busca disponibilizado na página da web do órgão público.

Exemplificando

Para ilustrar o que foi dito até agora, vejamos o exemplo do Portal de Acesso à Informação do Governo Federal (vide Figura 3.1), no qual é possível realizar uma busca através da ferramenta "Buscar no portal" e fazer um pedido de acesso clicando no banner "Faça seu pedido", além de outros recursos.

Figura 3.1 | Portal de acesso à informação do Governo Federal

Fonte: <http://www.acessoainformacao.gov.br/>. Acesso em: 3 ago. 2017.

Reflita

No caso das informações pessoais dos agentes públicos, pela LAI é possível obter informações, por exemplo, de um Policial Federal, que atua contra o crime organizado? Em algum momento, o criminoso pode se valer de algum dado do agente público para inibir sua ação e continuar praticando crimes?

Agora que sabemos como obter acesso à informação pública, entenderemos como e porquê algumas informações apresentam restrições de acesso. A LAI prevê, em seu Capítulo IV, algumas restrições de acesso à informação devido a dois principais motivos: primeiro, informações de cunho pessoal, em relação à vida íntima, privada, honra e imagem dos cidadãos, sendo que, neste caso, o período de restrição é de até 100 (cem) anos; e segundo, devido ao teor sigiloso das informações, em decorrência da sua importância para a segurança da sociedade brasileira. Segundo a LAI, poderão ser classificadas como sigilosas as informações que:

- Comprometam a defesa e a soberania do Brasil ou a integridade do território nacional.
- Possam prejudicar os relacionamentos do Brasil com a comunidade internacional.
- Coloquem em risco à população.
- Prejudiquem financeira ou economicamente o país.
- Afetem às forças armadas.
- Comprometam as pesquisas, o desenvolvimento e as inovações na área científica e tecnológica, com reflexos nas estratégias nacionais.
- Exponham a segurança de autoridades nacionais e internacionais, inclusive, seus entes familiares.
- Abalem os serviços de inteligência ou investigações em curso no país.

As informações que integram o grupo descrito anteriormente podem ser classificadas como: ultrassecretas, secretas e reservadas, de acordo com o interesse público da informação, o grau de risco que ela oferece e o prazo para a restrição do acesso. A LAI estabelece os seguintes prazos para restrição de acesso à informação, em conformidade com seu grau de sigilo: ultrassecreta, 25 (vinte e cinco) anos; secreta, 15 (quinze) anos; e reservada, 5 (cinco) anos.

A restrição de acesso à informação também pode terminar em decorrência de algum evento que exclua a necessidade de se manter o sigilo sobre a informação. Em ambos os casos, transcorrido o prazo estabelecido ou ocorrido o evento que determine o fim do sigilo

da informação, a informação passará a ser franqueada ao acesso público. A Lei estabelece ainda que as informações que possam afetar a segurança do Presidente ou Vice-presidente, suas esposas ou seus maridos e filhos, devem ser classificadas como reservadas até o final dos respectivos mandatos.

Exemplificando

Algumas informações e documentos podem ser classificados em determinados graus de sigilo, com a finalidade de que apenas um grupo seleto e autorizado tenha conhecimento destas. Entretanto, com o passar dos anos, este grau de sigilo pode ser alterado e *desclassificado*. Veja os exemplos de desclassificação das informações do Ministério da Defesa, disponível em: <http://www.defesa.gov.br/informacoes-classificadas>. Acesso em: 3 ago. 2017.

A LAI também afirma que o estabelecimento do grau de sigilo de uma informação no âmbito da Administração Pública Federal será de competência das seguintes autoridades:

- **Grau ultrassecreto**: Presidente da República; Vice-presidente da República; Ministros de Estado e autoridades com as mesmas prerrogativas; Comandantes da Marinha, do Exército e da Aeronáutica; e Chefes de Missões Diplomáticas e Consulares permanentes no exterior.

- **Grau secreto**: as autoridades mencionadas no grau ultrassecreto, mais os titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista.

- **Grau reservado**: todas das autoridades citadas nos graus ultrassecreto e secreto, mais as autoridades que ocupem cargos de direção, comando ou chefia, de nível igual ou superior ao 101.5 do Grupo-Direção e Assessoramento Superiores (DAS), obedecendo ainda a regulamentação específica de cada órgão ou entidade.

Assimile

Confiar apenas a determinadas autoridades o acesso a um tipo de informação permite reduzir o número de pessoas que venha a ter seu conhecimento, bem como um controle maior da informação. Informações de operações de guerra ou de operações policiais, em princípio, não devem ser de conhecimento de todos. O êxito destas operações, muitas vezes, depende de que apenas os mandantes e executantes tenham conhecimento. Daí a necessidade de lhe atribuir um grau de sigilo.

Toda informação que recebe uma classificação sigilosa deve, portanto, receber também um tratamento diferenciado das demais, objetivando a segurança e o controle da informação sigilosa. A Seção III, do Capítulo IV da LAI, trata exatamente desta questão, estipulando que é dever do Estado proteger este tipo de informação, tomando as medidas necessárias para executar o controle do acesso e da divulgação das informações sigilosas sob custódia dos órgãos públicos e das entidades relacionadas aos governos. Além disso, essas medidas incluem:

- Permitir o acesso à informação sigilosa por pessoas devidamente credenciadas para isso.
- Garantir que a pessoa que obteve acesso à informação sigilosa preserve o sigilo da informação.
- Providenciar que as autoridades públicas adotem ações para garantir que seus funcionários subordinados conheçam as normas e cumpram os procedimentos para proteção da informação sigilosa.

A lei ainda prevê que a pessoa física ou entidade privada que, por motivo de vínculo com o poder público, tenha acesso à informação sigilosa, deverá zelar pela manutenção do grau de sigilo da informação, atitude esta extensiva aos seus empregados, aos colaboradores e ao pessoal relacionado.

Reflita

Você saberia dizer se um agente público, um Governador, um Presidente de um Câmara de Vereadores, com base na LAI, pode classificar um

ato administrativo como, por exemplo, o aumento dos salários de funcionários públicos, com a finalidade de que a população não possa tomar conhecimento, evitando-se, assim, algum desgaste na imagem do órgão público ou do político?

Finalizando o nosso estudo sobre a lei de acesso à informação, procuraremos identificar as responsabilidades a que estarão sujeitas as pessoas que tiverem algum envolvimento com o trato das informações públicas, regidas pela LAI. Neste particular, teremos caracterizados dois papéis distintos: o papel do agente ou órgão público e o da pessoa física ou entidade privada.

No tocante aos agentes e órgãos públicos, a LAI prevê que serão consideradas condutas ilegais as seguintes atitudes:

- Recusar, retardar ou fornecer incompletamente informação solicitada nos termos da LAI.
- Fazer uso indevido, modificar, anular ou esconder, mesmo que parcialmente, informação que esteja sob sua custódia.
- Agir fora do estabelecido na LAI, de forma intencional, em relação aos pedidos de acesso à informação.
- Violar de qualquer forma o grau de sigilo de uma informação.
- Valer-se da prerrogativa de estabelecer classificação sigilosa para a informação, a fim de obter vantagem pessoal ou ocultar condutas ilegais de si próprio ou terceiros.
- Destruir ou ocultar documentos relativos a violações de direitos humanos praticados por agentes públicos.

Os agentes públicos, civis e militares, que, por ventura, incorram em alguma das condutas ilícitas listadas anteriormente, após terem direito à sua defesa, atendendo ao princípio do contraditório e da ampla defesa, estarão sujeitos às sanções disciplinares cabíveis. No caso dos militares, poderão sofrer punições disciplinares regulamentadas pelas Forças Armadas; e, no caso dos civis, poderão sofrer penas de, no mínimo, suspensão, segundo os critérios estabelecidos na Lei nº 8.112/1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

Em relação às pessoas físicas e entidades privadas que, de alguma forma, tiverem envolvimento com as informações públicas, a LAI estabelece que também deverão observar os dispositivos da legislação, estando de maneira igual sujeitos às punições listadas a seguir, dentre outras igualmente previstas na lei:

- Advertência.
- Multa.
- Cancelamento do vínculo com o poder público.
- Interrupção na participação em licitações públicas.
- Suspensão de firmar contratos com a administração pública.

Pesquise mais

Como acontece o acesso à informação nas entidades privadas? Conheça mais sobre a lei de acesso à informação e seu efeito nos órgãos e nas entidades públicas, acessando a LAI, disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 3 ago. 2017; e a cartilha *Acesso à Informação Pública*, disponível em: <http://www.acessoainformacao.gov.br/central-de-conteudo/publicacoes/arquivos/cartilhaacessoainformacao.pdf>. Acesso em: 3 ago. 2017.

Tendo concluído esta seção, verificamos que a Lei de acesso à informação realmente estabelece regras muito claras para garantir a transparência do poder público por meio do acesso à informação sobre as atividades desenvolvidas por cada setor do Estado Brasileiro. Identificamos também que, para ter acesso a essas informações, basta um procedimento simples de formalização de um pedido de acesso ou até mesmo buscá-las na internet, na qual são disponibilizadas ao público pelos órgãos e pelas entidades da administração pública federal. Além disso, compreendemos que algumas informações recebem uma classificação sigilosa, em virtude da sua importância para a segurança e soberania do país e, por isso, têm o acesso restrito, segundo o grau e o prazo do sigilo. Vimos ainda que os agentes públicos, tanto civis quanto militares, estão sujeitos a diversas sansões, caso descumpram a LAI, e que isso vale para as pessoas físicas e entidades privadas, que compartilham informações públicas em virtude de algum vínculo com o poder público.

Dessa forma, concluímos mais uma etapa da nossa jornada. Agora, já podemos avançar para a próxima atividade, que será a solução da nossa situação-problema.

Sem medo de errar

Aluno, chegou a hora de resolvermos a nossa primeira situação-problema desta unidade. O nosso caro amigo Luke da Silva realmente se deparou com um dos primeiros desafios na caminhada para realização de seu sonho. O conhecimento sobre a Lei de acesso à informação (LAI) é fundamental para quem atuará na área de segurança, seja privada, ou, principalmente, pública, já que os órgãos de segurança pública são custodiantes de várias informações sujeitas à ação da LAI e, além disso, também estão passíveis, órgãos e agentes, às responsabilidades atribuídas pela LAI a quem toma conhecimento de informações públicas, especialmente se forem sigilosas. Dessa forma, para que Luke consiga aprender sobre a LAI e se sair bem na prova para Soldado da PM, vamos ajudá-lo respondendo aos questionamentos levantados durante seus estudos. Como se trata de uma análise escrita, preencheremos o Quadro 3.2 a seguir, com a finalidade de iniciarmos a comparação entre os sistemas de informação da segurança pública e privada.

Quadro 3.2 | Comparação entre os sistemas de informação da segurança pública e privada

CLASSIFICAÇÃO DAS INFORMAÇÕES	
PÚBLICA	**PRIVADA**
Ultrassecreta: Presidente da República, Vice-presidente da República, Ministros de Estado, Comandantes da Forças Armadas (Marinha, Exército e Aeronáutica) e Chefes de Missões Diplomáticas e Consulares. Secreta: pelas autoridades já citadas, titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista.	As informações pessoais sob custódia do Estado e referentes à intimidade, à honra e à imagem das pessoas não recebem uma classificação especial, no entanto, têm seu acesso igualmente restrito devido à garantia do direito de privacidade.

Reservada: por todas as autoridades anteriores mais as autoridades que ocupem cargos de direção, comando ou chefia, de nível igual ou superior ao DAS 101.5.	
PRAZOS DE SIGILO	
PÚBLICA	**PRIVADA**
Ultrassecreta: 25 (vinte e cinco) anos. Secreta: 15 (quinze) anos. Reservada: 5 (cinco) anos.	Independente de classificação sigilosa: 100 (cem) anos. As informações relativas à intimidade, à vida privada, à honra e à imagem das pessoas devem ter seu acesso restrito por 100 anos (BRASIL, 2011, art. 31, §1º).
CONTROLE DAS INFORMAÇÕES	
PÚBLICA	**PRIVADA**
É dever do Estado que somente deverá permitir o acesso à informação sigilosa por pessoas devidamente credenciadas para isso; garantir que a pessoa que obteve acesso à informação sigilosa preserve o sigilo da informação; e providenciar que as autoridades públicas adotem ações para garantir que seus funcionários subordinados conheçam as normas e cumpram os procedimentos para proteção da informação sigilosa. A LAI também prevê que a pessoa física ou entidade privada que, por motivo de vínculo com o poder público, tenha acesso à informação sigilosa, deverá também zelar pela manutenção do grau de sigilo da informação, atitude esta extensiva aos seus empregados, aos colaboradores e ao pessoal relacionado.	As informações pessoais, sob custódia do Estado, também têm restrição de acesso e seu controle seguirá a mesma conduta adotada para as informações sigilosas. A LAI não estabelece nenhum controle para informações privadas custodiadas por pessoas físicas ou jurídicas da iniciativa privada.
PRAZOS PARA RESPOSTA A PEDIDOS DE INFORMAÇÃO	
PÚBLICA	**PRIVADA**

O órgão ou a entidade pública deve conceder o acesso imediato às informações solicitadas e, caso não seja possível, terá um prazo de 20 (vinte) dias, podendo ser prorrogado por mais 10 (dez) para marcar uma data para liberação do acesso à informação ou apresentar as justificativas para a negativa de acesso. Nos casos em que o acesso à informação for negado, o interessado poderá recorrer desta decisão junto ao próprio órgão, em um prazo de 10 (dez) dias, ou apelando para a Controladoria-Geral da União (CGU), tanto um quanto o outro terão o prazo de 5 (cinco) dias para responder ao recurso do interessado.	Os prazos serão os mesmos das informações públicas, porém somente para informações pessoais, sob custódia do Estado. A LAI não estabelece nenhum prazo para resposta a pedidos de informação para informações privadas sob custódia de pessoas físicas ou jurídicas da iniciativa privada.
ACESSO ÀS INFORMAÇÕES	
PÚBLICA	**PRIVADA**
Qualquer pessoa ou organização poderá solicitar acesso, este só não será concedido se a informação requerida for sigilosa ou de caráter pessoal e privada. Só tem acesso a estes casos as pessoas devidamente credenciadas.	A critério das pessoas físicas ou jurídicas a que as informações se referirem ou por imposição legal, de acordo com os critérios previsto na LAI.

Fonte: elaborado pelo autor.

Para finalizar nossos estudos, complementaremos o que apresentamos até agora, ressaltando que qualquer pessoa ou organização com interesse em obter informações públicas poderá solicitá-las e, somente não receberá permissão de acesso, se a informação requerida for sigilosa ou de caráter pessoal e privada.

Assim, finalizamos a solução de mais uma situação-problema. Dessa forma, aproveitaremos o embalo e partiremos para o próximo desafio. Não se esqueça de que você finalizou, nesta seção, a primeira etapa do nosso produto. Nas Seções 2 e 3, você continuará a completar sua análise.

Avançando na prática

Capacidade de manter sigilo: uma virtude profissional

Descrição da situação-problema

Creio que você está disposto a aperfeiçoar seus conhecimentos mergulhando em mais uma situação-problema. Analisaremos, agora, uma situação fictícia, mas que poderia ocorrer com qualquer um de nós. Em certa oportunidade, a vigilante Carolina Correia, colaboradora da empresa TJM Segurança Ltda., especializada na segurança de aeroportos, foi convidada para participar de uma investigação conduzida pela Polícia Federal sobre o segmento, no Brasil, de uma quadrilha internacional de tráfico de drogas. Nossa vigilante, conhecida no âmbito da PF, por conta de seus conhecimentos, aceitou prontamente o desafio e iniciou sua participação na investigação da PF e, para tanto, tomou conhecimento de informações reservadas, necessárias à compreensão da sua missão junto ao trabalho daqueles agentes públicos.

Entretanto, o resultado da investigação foi frustrante, porque a agente Carolina Correia, na empolgação de participar de uma investigação sigilosa, não conseguiu manter o sigilo sobre sua missão e acabou contando detalhes da investigação para alguns amigos em um bar próximo ao aeroporto que trabalhava. Foi o suficiente para que ocorresse o vazamento das informações acerca da atividade da Polícia Federal, comprometendo o trabalho dos agentes federais e arruinando a investigação.

Dentro desse contexto, podemos refletir sobre os seguintes questionamentos: será que as informações da PF sobre a investigação poderiam ter grau de sigilo reservado? Caso positivo, até quando este sigilo deveria ser mantido? Os agentes da PF poderiam ter deixado Carolina ter acesso àquelas informações? Será que a agente Carolina também tinha que manter o sigilo daquelas informações, uma vez

que ela não é da PF? Por ter divulgado as informações para outras pessoas, Carolina pode sofrer algum tipo de punição? E aí, aluno? Você está preparado para responder esses questionamentos? Então, siga em frente!

Resolução da situação-problema

Realmente, Carolina Correia prejudicou totalmente a investigação da Polícia Federal. Para entender o que aconteceu, teremos como foco a Lei de acesso à informação, tentando responder aos questionamentos apresentados. Inicialmente, entenderemos que as informações da PF sobre a investigação poderiam ser sigilosas, porque, segundo a LAI, podem receber tal classificação as informações que abalam as investigações em curso no país. Considerando que as informações da PF eram reservadas, o grau de sigilo deveria ser mantido por, no máximo, cinco anos ou até que ocorresse algum evento que determinasse o fim do sigilo. Carolina poderia ter acesso à informação sigilosa, porque estava devidamente credenciada para isso, uma vez que participava oficialmente da investigação em curso. A LAI também determina que Carolina, mesmo sendo pessoa física e não fazendo parte da PF, deveria ter zelado pelo sigilo da informação reservada, uma vez que tomou conhecimento desta. Por ter violado o sigilo da informação, Carolina está sujeita à responsabilização prevista na LAI, podendo sofrer sanções, como advertência e multa, dentre outras.

Dessa maneira, conseguimos vencer mais uma etapa.

Faça valer a pena

1. O A Lei de acesso à informação obriga os órgãos públicos a tornarem transparentes seus atos através da divulgação de informações ao público em geral, por isso, alguns órgãos utilizam suas páginas na web para cumprir algumas determinações contidas na lei. Como podemos verificar no Portal de Acesso à Informação do Governo Federal, ilustrado na figura a seguir.

Fonte: <http://www.acessoainformacao.gov.br/>. Acesso em: 3 ago. 2017.

Assinale a alternativa correta que indica qual é a página da web que contém exemplos do cumprimento de determinações da Lei de acesso à informação.

a) Das restrições de acesso à informação.

b) Do acesso à informação e de sua divulgação.

c) Das disposições transitórias da lei.

d) Das responsabilidades dos agentes públicos em relação às informações.

e) Da classificação das informações.

2. Nos procedimentos de acesso à informação contidos no capítulo III, da Lei de acesso à informação, fica estabelecido que os órgãos públicos deverão franquear acesso imediato às informações solicitadas, entretanto, poderão também negar o acesso às informações restritas. Neste caso, cabe ainda ao interessado interpor recurso contra a negativa de acesso.

Nos casos em que o acesso à informação for negado, o interessado poderá recorrer desta negativa junto ao próprio órgão que negou o acesso ou, ainda, apelar para a:

a) Advocacia-Geral da União (AGU).

b) Procuradoria-Geral da União (PGU).

c) Tribunal de Contas da União (TCU).

d) Ouvidoria-Geral da União (OGU).

e) Controladoria-Geral da União (CGU).

3. A Lei de acesso à informação estabelece que, para ter acesso à informação, o interessado deve realizar um(a) _____, que pode ser feito(a) por qualquer pessoa que tenha interesse na informação, bastando fornecer seu(sua) _____ e especificar qual _____ se deseja acessar.

A partir da frase anterior, assinale a alternativa que contém as palavras que completam as lacunas.

a) Petição – nome – informação.

b) Pedido de acesso – informação – identificação.

c) Requerimento – função ou cargo público – documento.

d) Pedido de acesso – identificação – informação.

e) Protocolo – identificação – documento.

Seção 3.2

Sistemas e informações na segurança privada

Diálogo aberto

Prezado aluno, a vida do nosso personagem foi tomando seu rumo, o tempo foi passando e Luke da Silva, aquele dedicado rapaz, que tanto gosta da carreira militar, ainda não tinha passado no concurso da PM que tanto desejava. No primeiro concurso que se inscreveu, por conta da escala de serviço apertada na empresa Defender Vigilância, Escolta e Guarda, ele acabou não conseguindo estudar tanto quanto deveria. Mas, por outro lado, Luke vinha trabalhando com muito empenho em suas tarefas e acabou sendo promovido a Inspetor de Segurança, passando, assim, a trabalhar no ramo de escolta e guarda da empresa. A Defender tinha uma forte participação nos serviços de escoltas de cargas de altos valores, muito cobiçadas pela criminalidade.

Luke chegou para trabalhar em uma segunda-feira e acabou tomando conhecimento que um caminhão que transportava aparelhos eletrônicos, escoltado por sua empresa, havia sofrido uma ação de meliantes fortemente armados na semana anterior, fora do turno dele. Naquela segunda, Luke havia sido chamado pelo seu gerente de segurança da área para ser informado de que o sistema de monitoramento por satélite da viatura da Defender e do caminhão que transportava a carga roubada não havia funcionado, justo no momento da ação dos marginais. No entanto, os motoristas não haviam percebido a falha em seus GPS e o sistema da central de segurança, embora tivesse funcionado normalmente, apenas não tinha mostrado o posicionamento dos carros envolvidos na ação criminosa. Como isso poderia ter ocorrido? Será que foi alguma pane nos GPS? Quais outros aspectos devem ser considerados para garantir a segurança deste sistema? O desafio de Luke, agora, será identificar a possível causa da falha, descobrir as vulnerabilidades do sistema de monitoramento adquirido pela Defender, que permitiram a ação da quadrilha, e propor uma outra solução em sistemas de rastreamento, existentes no mercado, que a empresa Defender poderia comprar e implementar. Ajudando Luke a resolver seus desafios, você, aluno, estará contribuindo para a segunda parte do produto, a análise escrita

sobre a comparação entre os sistemas de informação da segurança pública e privada. Para tanto, deixe claro as principais características dos sistemas de informação empregados na segurança privada.

Vale lembrar que nossa proposição para o produto a ser entregue na Unidade 3 é que seja apresentada uma análise escrita sobre a comparação entre os sistemas de informação da segurança pública e privada. Dessa forma, retomaremos o Quadro 3.3, apresentado a seguir, que deve ser completado na resolução da situação-problema.

Quadro 3.3 | Continuação da comparação entre os sistemas de informação da segurança pública e privada

SISTEMAS E INFORMAÇÕES EMPREGADOS NA SEGURANÇA	
PRIVADA	
SISTEMA DE INFORMAÇÃO UTILIZADO	OBJETIVO
PÚBLICA	
SISTEMA DE INFORMAÇÃO UTILIZADO	OBJETIVO

Fonte: elaborado pelo autor.

Não pode faltar

Prosseguiremos, agora, em nossa aprendizagem destrinchando os Sistemas e as Informações na Segurança Privada. Já estudamos a importância e o emprego dos SI na Segurança Privada e, neste momento, aprofundaremos ainda mais neste tema. Para entendermos os tipos de SI empregados na Segurança Privada, compreenderemos que esses sistemas de informação devem ter suas características voltadas para atender às funções e atividades básicas da Segurança Privada, ou seja, vigilância patrimonial, transporte de valores, escolta armada e segurança pessoal, e dentro dos princípios comuns a todas essas atividades, isto é, o monitoramento, a detecção, o alarme ou a comunicação e a ação. Além disso, atuaremos nos níveis operacional,

tático e estratégico dentro das medidas de segurança patrimonial e pessoal. A seguir, descreveremos vários tipos de sistemas de informação que reúnem todas essas características, podendo ser empregados isoladamente em qualquer uma das atividades da Segurança Privada ou, ainda, combinando duas ou mais ações e dois ou mais sistemas, dependendo do planejamento e da estrutura da segurança.

Começaremos pelos **Sistemas de Monitoramento por Câmeras**. Você sabe o que é um CFTV? Um circuito fechado de televisão (CFTV) é um sistema que permite o monitoramento através de imagens capturadas por um conjunto de câmeras e enviadas, através de um canal de comunicação, para um computador central. A partir daí as imagens poderão ser exibidas em monitores de vídeo e acompanhadas por vigilantes, ou acessadas por meio de tablets, notebooks e smartphones, além de poderem ser gravadas, arquivadas e recuperadas, quando necessário.

O monitoramento por câmeras pode ser empregado em várias situações e com finalidades distintas, tais como: vigilância de áreas com grande circulação de pessoas e veículos; monitoramento de vias de acesso a prédios, lojas, condomínios, residências e outros; identificação de pessoal, veículo ou material; atividades produtivas, como linha de produção e funcionamento de máquinas; monitoramento de veículos e itinerários, no caso, das empresas de transporte; dentre várias outras possibilidades. As imagens das câmeras podem, ainda, ser utilizadas como evidência de crimes, servindo como provas para responsabilizar judicialmente criminosos e infratores (BRASILIANO; BLANCO, 2003).

Pesquise mais

Entenda um pouco mais sobre CFTV no seguinte link, disponível em: <http://www.onixsecurity.com.br/blog/entenda-o-que-e-um-sistema-cftv/>. Acesso em: 8 ago. 2017.

Vejamos agora os **Sistemas de Vigilância de Perímetro**, capazes de integrar equipamentos que permitem monitorar o estado do perímetro de um condomínio residencial ou empresarial, de uma indústria, de um comércio, de um shopping center, de um aeroporto, resumindo, de qualquer instalação. Esses equipamentos são normalmente:

sensores, de vários tipos, como de presença e infravermelho; barreiras de micro-ondas; cabeamento; sirenes; alarmes; luzes; câmeras, monitores de vídeo; computadores; e softwares de gerenciamento e comunicação. Comumente, a finalidade desses sistemas é detectar a violação do perímetro sob vigilância, determinando precisamente a localização do ponto de rompimento ou invasão e disparando os dispositivos de alarme necessários, possibilitando que sejam tomadas as devidas providências ou ações para a manutenção da segurança do patrimônio sob ameaça (SOARES, 2008).

Os **Sistemas de Controle de Acesso** são também muito utilizados, tendo como principal função identificar pessoas, materiais e veículos, permitindo ou negando acesso às instalações de uma organização. Este é um dos sistemas mais comumente empregados na segurança patrimonial e um dos mais sensíveis, uma vez que tem a missão de garantir o acesso físico ao interior da organização somente às pessoas e aos veículos autorizados, restringindo a entrada de possíveis ameaças ao interior da organização. Esses sistemas são compostos por: barreiras físicas, como: portas, portões, cancelas e catracas; detectores de presença, de metais, de explosivos, etc; placas controladoras; rede de comunicação; computadores; softwares de gerenciamento; web câmeras; e coletores de dados, equipamentos que farão a identificação e autorização de acesso, são eles: fechaduras eletrônicas e eletromecânicas, sensores de RFID (radiofrequência por aproximação), teclado de senhas, leitores de cartão (com tarjeta magnética, chip ou código de barras) e leitores biométricos (que capturam a impressão digital, a íris, a voz, etc.) (BRASILIANO; BLANCO, 2003).

Ainda existem os **Sistemas de Alarme**, talvez, um dos sistemas mais simples e mais empregados na segurança patrimonial, já que qualquer pessoa pode adquirir um kit de instalação e, com um mínimo de conhecimento, montá-lo, por exemplo, em sua casa. Este sistema é, na verdade, um conjunto de componentes eletrônicos que interagem entre si com a única finalidade de informar sobre a invasão do local que se deseja proteger. Sua constituição básica compreende os sensores (de presença, magnéticos, de vibração, de vidro); uma central de alarme, hardware específico para receber e processar os dados dos sensores; sirenes, para comunicar a invasão da instalação; teclados de senha, para ativação e desativação do sistema; controles remotos, para comandar funções específicas do sistema; e uma linha

de comunicação, para enviar mensagens de alerta preestabelecidas. São empregados, via de regra, em residências, em pequenos comércios e em instalações sensíveis dentro de uma empresa ou organização de médio e grande porte, tais como: almoxarifados, setor financeiro e instalações de TI. Algumas empresas, atualmente, comercializam sistemas de alarme monitorados remotamente por uma central de vigilância, que acompanha de longe a situação do sistema, sendo, inclusive, capaz de desencadear uma série de ações para garantir a segurança da instalação, no caso de uma eventual invasão.

Passaremos para os **Sistemas de Detecção e Combate a Incêndio**, voltados para a segurança patrimonial e pessoal, uma vez que um incêndio pode causar danos a ambos. De forma geral, é um sistema composto por sensores de fumaça, temperatura e chama, que devem estar posicionados inteligentemente pelas instalações e atuar de forma integrada para que ocorra a efetiva identificação do incêndio ou foco de incêndio; por uma central, que recebe e processa os dados dos sensores acionando os dispositivos necessários; por indicadores de incêndio, que podem ser sonoros e visuais; e por equipamentos de combate ao fogo, como pulverizadores de água (*sprinklers*), dispositivos de desligamento de elevadores, sistemas de condicionamento de ar e até corte parcial da energia elétrica. Esses sistemas também podem conter monitores de vídeo que exibem a posição precisa do foco de incêndio ou ainda painéis representativos da planta baixa das instalações com indicadores luminosos da posição do fogo (BRASILIANO; BLANCO, 2003).

Neste momento, veremos a descrição dos **Sistemas de Rastreamento**, empregados não só para rastreamento de veículos, mas também no de pessoas, através da localização do aparelho celular, e até de objetos, com o emprego de dispositivos localizadores específicos. Esses sistemas são compostos basicamente por três dispositivos: (1) **sistema de posicionamento**, responsável por informar a localização do veículo, pessoa ou objeto monitorado; (2) **rede de comunicação**, por meio da qual serão transmitidos os dados de localização; e (3) uma **central de rastreamento ou de segurança**, que tem um software que processa os dados de localização, exibindo a posição do alvo em um mapa, em um monitor, e gerando relatórios sobre o deslocamento. A comunicação da localização do alvo para a central de rastreamento pode ser feita empregando-se três tipos

de tecnologias de telecomunicações: **via satélite**, mais lenta, devido ao tempo de atraso da comunicação, porém com cobertura total; **via rede de telefonia celular**, mais rápida, mas depende da área de cobertura da operadora de telefonia, que usualmente apresenta grande abrangência; ou **via rádio**, também rápida, muito mais barata, porém com uma cobertura muito limitada, praticamente aos grandes centros urbanos e principais eixos de ligação entre eles (KLEIN, 2016).

Exemplificando

Você poderá encontrar uma alternativa de emprego do rastreamento na segurança privada, acessando *Empresas de Monitoramento: Quais serviços elas prestam e quais são as alternativas?*, disponível em: <http://www.snitch.com.br/empresas-de-monitoramento/>. Acesso em: 3 ago. 2017.

Outro bom exemplo sobre a fiscalização via satélite nas viaturas da PMRJ poderá ser verificado em *PM aumenta fiscalização via satélite das viaturas no Rio*, disponível em: <http://noticias.r7.com/rio-de-janeiro/noticias/pm-aumenta-fiscalizacao-via-satelite-das-viaturas-no-rio-20110702.html>. Acesso em: 3 ago. 2017.

Aproveitando sua citação no tópico anterior, abordaremos o conceito de **Central de Segurança**, instalação na qual são centralizados todos os controles dos diversos serviços de segurança, isto é, de onde é feito o gerenciamento e comando das ações de segurança. Por isso, a central de segurança deve ser conduzida pelo Gerente de Segurança. Segundo Soares (2008), a central de segurança pode reunir os seguintes recursos:

- Monitoramento de instalações e dependências, por meio de sensores e câmeras.
- Coordenação remota de sistemas de controle de acesso.
- Controle de sistemas de ar condicionado, energia elétrica e elevadores.
- Controle de sistemas de som ambiente.
- Controle de sistemas de alarmes.

- Central de comunicações, envolvendo radiocomunicação, telefonia e Internet, inclusive com canais exclusivos de comunicação.
- Monitoramento de sistemas de detecção e combate a incêndio.
- Monitoramento do deslocamento de veículos ou cargas.
- Coordenação do pessoal empregado na segurança.
- Tramitação de documentação relativa a segurança.

A Central de Segurança pode ser empregada tanto no gerenciamento da segurança interna de uma empresa quanto no gerenciamento remoto da segurança em diversas localidades distintas, atendendo a diferentes clientes, sendo que este último caso evidencia a atual tendência dos produtos de segurança, isto é, o gerenciamento remoto por uma central de segurança compartilhada.

Mais recentemente surgiram os **Sistemas de Portaria Virtual**, também conhecidos como ePortaria. Este é um sistema resultante da integração de outros, como o de monitoramento por câmeras, de vigilância de perímetro e de controle de acesso, sendo tudo controlado à distância, via internet, por uma central de segurança. O diferencial comercial desses sistemas está baseado na promessa de redução dos custos do condomínio com portaria 24h, através da implantação de um sistema remoto fundamentado no compartilhamento de uma central de segurança. O sistema é organizado estruturalmente por barreiras do tipo portões automáticos, tanto para pedestres quanto para veículos; por um sistema de câmeras; por sensores de perímetro; e, principalmente, por um canal de comunicação com a central de segurança. O acesso ao condomínio através da Portaria Virtual pode ser liberado por meio da identificação por senha pessoal, cartão de RFID, biometria e controle remoto (garagem) para as pessoas previamente cadastradas; ou por meio do atendimento pela central de segurança. Esta monitora ainda o perímetro do condomínio, através de sensores, e as principais instalações, por meio de câmeras, buscando impedir o acesso ao interior do patrimônio por pessoas não autorizadas ou mal-intencionadas.

Exemplificando

Veja como as portarias inteligentes funcionam nesta reportagem do G1, disponível em: <http://g1.globo.com/sao-paulo/sao-jose-do-rio-preto-aracatuba/mercado-imobiliario-do-interior/noticia/2016/08/portarias-inteligentes-fazem-gastos-com-seguranca-diminuirem-ate-70.html>. Acesso em: 3 ago. 2017.

Por último, mas não encerrando o assunto, descreveremos os **Sistemas de Gerenciamento da Segurança** voltados para o planejamento da segurança com base na análise de riscos. Normalmente, estes constituem-se em um software de computador que auxilia no planejamento de gerenciamento de riscos (PGR), apoiando as decisões dos gerentes de segurança. Esses sistemas ou softwares dão suporte para o levantamento de vulnerabilidades; a identificação de ameaças; a quantificação da probabilidade da ameaça explorar a vulnerabilidade, classificando-a por grau de risco; o processo decisório para tratamento dos riscos levantados; bem como o controle das ações que eventualmente serão desencadeadas em decorrência do planejamento da segurança.

Assimile

Os principais tipos de sistemas de informação na Segurança Privada são:

- Sistemas de monitoramento por câmeras.
- Sistemas de vigilância de perímetro.
- Sistemas de controle de acesso.
- Sistemas de alarme.
- Sistemas de detecção e combate a incêndio.
- Sistemas de rastreamento.
- Sistemas de portaria virtual.
- Sistemas de gerenciamento da segurança.

Uma vez que já conhecemos os tipos de Sistemas de Informação na segurança privada, entenderemos alguns aspectos envolvendo o acesso e o uso ilegal destes. Podemos definir como ilegal qualquer tentativa de acesso ou uso não autorizado do sistema, caracterizando acesso como sendo a possibilidade de entrar no sistema por meio de identificação (log in) e senha; e uso como a prerrogativa, daqueles que têm acesso ao sistema, de utilizar suas funções e seus recursos. Tanto o acesso quanto o uso ilegal de sistemas de informação devem ser uma preocupação constante no controle dos SI na segurança privada.

O acesso ilegal a um SI de segurança pode ser feito tanto por um funcionário de dentro da empresa, utilizando log in/senha de outra pessoa, quanto por um ***cracker***, tipo de **hacker** criminoso, caracterizando um ataque cibernético. O primeiro caso, apesar de não ser raro, geralmente não é utilizado para o cometimento de crime ou do serviço de segurança prestado, mas sim como uma forma de contornar situações para dar continuidade ao serviço. Já o segundo caso, constitui o principal problema do acesso ilegal e pode causar danos irreparáveis ao sistema e comprometer toda a segurança suportada por ele. Por isso, a prevenção contra esses ataques deve ser alvo de efetivas medidas de segurança da informação, como já estudamos anteriormente.

Já no tocante ao uso ilegal dos SI de segurança, a lógica é invertida, porque um cracker normalmente não utiliza funções do sistema na sua atividade criminosa, mas sim captura senhas de acesso, informações, imagens, ou simplesmente deixa o sistema inoperante para que outras ações possam ser desencadeadas. No entanto, tudo isso ficará bastante evidente e será tratado como um incidente de segurança. A principal preocupação aqui é justamente o uso ilegal dos sistemas pelo pessoal de segurança que tem acesso autorizado ao SI, porque, muitas vezes, essa prática passa desapercebida e, quando é identificada, o problema já está feito. O uso ilegal desses sistemas pelo próprio pessoal da segurança pode ser motivado por razões diversas, mas, em todos os casos, as consequências são desastrosas. Podemos citar situações desde

vigilantes que se utilizaram do sistema de monitoramento por câmeras para invadir a privacidade das pessoas, até aqueles que burlaram uma catraca para favorecer a entrada de pessoas de seu relacionamento pessoal no refeitório da empresa. Contudo, os casos mais sérios e preocupantes são os dos agentes de segurança que servem de informantes para quadrilhas ou qualquer outro tipo de organização criminosa. Estes normalmente utilizam o sistema para coletar informações e repassá-las aos criminosos, ou facilitar a ação de bandidos, ou até mesmo empregar o sistema em favor de seus comparsas (STAIR; REYNOLDS, 2015).

Fica fácil compreender que o problema de uso e acesso ilegal dos SI na segurança privada pode trazer consequências extremamente danosas, tanto para a empresa prestadora do serviço de segurança, impactando diretamente na qualidade do seu serviço e na sua reputação no mercado, quanto para o cliente, permitindo que este seja alvo da ação criminosa de marginais. Devemos entender também que as medidas preventivas contra o uso e o acesso ilegal aos SI da segurança envolvem ações de segurança da informação e comunicações nos sistemas; revisão e atualização constante dos processos de trabalho; e, principalmente, acompanhamento do comportamento do pessoal empregado na segurança, além da conscientização constante sobre a importância da legitimidade da conduta dos agentes nas ações de segurança.

Reflita

Como se pode identificar e combater o uso ilegal de SI na Segurança Privada pelo próprio pessoal envolvido na segurança? Quais medidas adotar, desde os casos mais simples e irrelevantes até o mais extremo, como a ação de informantes? Você tem a dimensão dos prejuízos sofridos pelas empresas nos casos de uso ilegal das informações por conta de seus próprios colaboradores? Pense muito bem nestas questões, pois a ameaça pode estar bem próxima a você.

Agora, partiremos para conhecer um pouco mais sobre as tecnologias empregadas nos sistemas de rastreamento, também chamados de sistemas de monitoramento e rastreamento. Estes

são empregados, normalmente, para monitorar ou rastrear veículos e objetos, podendo entender o **monitoramento** como sendo a atividade de fazer o acompanhamento remoto do deslocamento do veículo ou do objeto durante seu itinerário, permitindo, por exemplo, estimar quanto tempo falta para chegar ao destino ou se houve mudança da rota previamente estipulada; e o **rastreamento** como a prática de fazer uma investigação ou seguir pistas para se encontrar o veículo ou objeto desejado, normalmente, que tenha sido alvo de um roubo ou um furto. Nesse contexto, vejamos quais tecnologias são mais utilizadas em cada um dos casos. No monitoramento, as tecnologias mais usadas são o GPS e o GPRS, embora as abreviaturas sejam muito parecidas, as tecnologias são totalmente diferentes. *Global Positioning System* (GPS) ou Sistema de Posicionamento Global, é um sistema de determinação de posicionamento ou da localização através de informações fornecidas por satélites em órbita ao redor da Terra e recebidas por um dispositivo receptor instalado no veículo. Este receptor consegue, a partir das informações recebidas do satélite, calcular a distância dele até o satélite; e, como também faz esse cálculo para vários outros satélites, consegue calcular qual é sua posição na superfície terrestre, por meio da chamada triangulação (vide Figura 3.2).

Figura 3.2 | Triangulação no GPS

Fonte: <https://www.oficinadanet.com.br/post/12406-como-funciona-o-gps>. Acesso em: 25 mai. 2017.

Pesquise mais

Entenda melhor como funciona a tecnologia GPS, lendo o artigo da Oficina da Net. Disponível em: <https://www.oficinadanet.com.br/post/12406-como-funciona-o-gps>. Acesso em: 3 ago. 2017.

Sabemos, portanto, que o GPS serve para fornecer a localização do veículo. Dessa forma, agora precisamos enviar essa localização para a central de monitoramento. A partir disso, faz-se uso da tecnologia *General Packet Radio Service* (GPRS) para transmitir dados através de internet móvel, em altas taxas de transmissão, usando a rede de telefonia celular, ou seja, fazer a comunicação do veículo com a central de segurança, informando a localização deste a cada fração de segundo, permitindo, portanto, monitorar seu deslocamento. Não podemos nos esquecer de que essa comunicação também pode ser feita via satélite, como vimos anteriormente. Já no rastreamento, a tecnologia mais utilizada é a radiofrequência (RF), ou seja, o veículo, a carga ou o objeto, que recebe um dispositivo, normalmente pequeno e até equipado com uma bateria própria, que emite um sinal de RF constantemente, podendo este sinal ser captado por um equipamento receptor, determinando a localização do veículo ou objeto. Esses sistemas estão sendo cada vez mais utilizados, principalmente, para rastreamento de cargas roubadas. Como o alcance do sinal de RF é limitado, pode existir a necessidade de se fazer um patrulhamento da área, onde se suspeita que o objeto procurado possa estar, buscando localizar o sinal de rádio e, consequentemente, o objeto sinistrado. A RF também pode ser utilizada, assim como o GPRS, para fazer a comunicação da localização do veículo com a central de segurança. Usualmente, essas tecnologias são utilizadas em conjunto, de forma que se complementem entre si, visando uma maior qualidade nos serviços de monitoramento e rastreamento oferecidos pelas empresas de segurança privada.

Exemplificando

Para materializar o emprego dos rastreadores no mercado, podemos citar o produto da empresa CARSYSTEM, líder em rastreamento veicular no Brasil, que, utilizando a tecnologia de GPS, consegue atingir altíssimos índices de recuperação de veículos furtados e/ou roubados. Disponível em: <http://www.carsystem.com/>. Acesso em: 3 ago. 2017.

Encerrando esta seção, identificaremos quais são as vulnerabilidades a que estão sujeitos os sistemas de informação da segurança privada. Na verdade, estes estão sujeitos às vulnerabilidades comuns aos SI, de forma geral, enunciadas por Laudon e Laudon (2007) e agrupadas da seguinte forma:

- **Hardware**: quebra, erro, defeito ou falha. Por exemplo: a quebra de uma cancela de um sistema de controle de acesso.
- **Software**: desatualização, erro de configuração ou de programação.
- **Rede**: invasão ou interceptação (ação de hackers), falha ou falta de mecanismos de defesa, como firewall e antivírus, interrupção ou interferência (ocasional ou proposital), exposição à internet, ausência de redundância. Por exemplo: o emprego de um jammer que bloqueia o sinal de um GPS em um sistema de rastreamento.
- **Banco de Dados**: falha nos dispositivos de armazenamento, nas rotinas de cópias de segurança, erros de leitura e escrita de dados.
- **Ambiente**: falta de energia elétrica, incêndios, enchentes, descargas atmosféricas (raios), vandalismo ou quebra de equipamentos intencionalmente.
- **Usuários**: informantes, mal-intencionados ou mal preparados.

Assim, finalizamos mais uma seção de nossos estudos, confiantes em termos aprendido mais um conteúdo importante na nossa formação acadêmica. Agora, vamos à resolução da situação-problema.

Sem medo de errar

Resolveremos, agora, mais uma situação-problema, envolvendo Luke, que foi chamado pelo seu gerente de segurança para analisar o problema da falha do sistema de monitoramento da viatura da Defender e do caminhão da transportadora, no caso do roubo da carga. Dessa forma, aluno, como sabemos, um sistema de rastreamento é baseado em três componentes básicos, isto é, sistema de posicionamento, rede de comunicação e central de rastreamento; assim, basta analisar cada um deles separadamente. Primeiro, o sistema de posicionamento, que, caso tivesse falhado, não informaria mais a localização dos veículos e isso seria percebido no GPS da viatura e do caminhão, o que não ocorreu; em seguida, a rede de comunicação, que, em caso de falha, deixaria de informar a localização da viatura e do caminhão para a central de segurança, podendo isso ocorrer simultaneamente; e, finalmente, o software da central de segurança, que, caso tivesse uma pane, não mostraria mais a posição dos veículos rastreados, entretanto, isso ocorreria com todos os veículos e não só com aqueles dois.

Após essa análise inicial, podemos descartar a falha no sistema de posicionamento e no software da central de segurança, passando a investigar mais detalhadamente a rede de comunicação. Como a falha no sistema ocorreu justo no momento da ação dos marginais e nos dois veículos ao mesmo tempo, podemos levantar duas hipóteses: primeira, que ambos os veículos estavam em uma área sem cobertura para a comunicação e, de alguma forma, os bandidos sabiam disso, talvez contando com a colaboração de um informante, e se aproveitaram do momento para praticar o roubo da carga; ou, segunda, que os ladrões empregaram algum dispositivo que causou interferência na comunicação entre o equipamento instalado na viatura e no caminhão e a central de segurança da Defender, interrompendo a comunicação e indisponibilizando temporariamente o sistema.

Na primeira hipótese, as vulnerabilidades exploradas foram a interrupção ocasional da rede de comunicação associada à falta de redundância e o provável emprego de um informante; na segunda, foi a interferência proposital na rede de comunicação também associada à falta de redundância. O fato é que a vulnerabilidade do

sistema que proporcionou a ação dos bandidos foi a ausência de redundância, porque o sistema adquirido pela Defender não tinha um canal de comunicação alternativo entre os veículos e a central de segurança.

No mercado, existem soluções em sistemas de monitoramento e rastreamento implementadas das mais diversas formas, mas empregando as mesmas tecnologias de GPS, Telefonia Celular (GPRS), Link Satelital e Radiofrequência (RF), sendo que o GPRS é a mais utilizada na comunicação entre o veículo e a central de segurança e, por esse motivo, torna-se mais vulnerável à ação de marginais que utilizam equipamentos para bloquear essa comunicação.

Diante de todas essas conclusões, basta procurar no mercado outro produto em sistemas de monitoramento e rastreamento que tenha redundância de comunicação. Devemos considerar, nessa redundância, também a comunicação via satélite que, apesar de mais lenta, tem uma abrangência quase que total, servindo muito bem como canal alternativo. A indicação do produto existente no mercado e que tenha essas características fica sob sua responsabilidade, aluno. Não se esqueça de considerar que esse novo produto deve atender às necessidades da atividade de Segurança Privada, no tocante à escolta e ao rastreamento de cargas de alto valor, permitindo o adequado monitoramento, detecção e comunicação de ocorrências que violem a segurança da carga em questão.

Agora que você solucionou a situação-problema, baseado neste e nos conteúdos que você teve nesta seção, procure preencher o quadro a seguir, completando a segunda parte do seu produto.

Quadro 3.4 | Continuação da comparação entre os sistemas de informação da segurança pública e privada

SISTEMAS E INFORMAÇÕES EMPREGADOS NA SEGURANÇA PRIVADA	
SISTEMA DE INFORMAÇÃO UTILIZADO	**OBJETIVO**
Sistemas de Monitoramento por Câmeras	Vigilância de áreas com grande circulação de pessoas e veículos e monitoramento de acesso a prédios, lojas, condomínios, residências.

Sistemas de Vigilância de Perímetro	Detectar a violação do perímetro sob vigilância, um condomínio, uma fábrica, uma loja, um estacionamento, determinando a localização do ponto de rompimento ou invasão.
Sistemas de Controle de Acesso	Identificar pessoas, materiais e veículos, permitindo ou negando acesso às instalações de um prédio, loja, condomínio.
Sistemas de Alarme	Para dar o alerta sobre a violação de instalações em residências, pequenos comércios e em pontos sensíveis dentro de uma empresa de médio e grande porte, tais como: almoxarifados, setor financeiro e instalações de TI.
Sistemas de Detecção e Combate a Incêndio	Identificar um foco de incêndio em uma instalação patrimonial, acionando dispositivos de alarme e pulverização de água.
Sistemas de Rastreamento e Monitoramento	Monitorar o deslocamento de veículos, pessoas, valores, produtos, encomendas, para inibir furtos, roubos e sequestros.
Sistemas de Portaria Virtual	Utilizar um sistema remoto capaz de monitorar toda a segurança de prédios e instalações com base no compartilhamento da central de segurança.
Sistemas de Gerenciamento da Segurança	Planejamento da segurança com base na análise de riscos.
Central de Segurança	Centralizar todos os controles dos diversos serviços de segurança, fazendo o gerenciamento e comando das ações de segurança
PÚBLICA (a ser preenchido na Seção 3.3)	
SISTEMA DE INFORMAÇÃO UTILIZADO	**OBJETIVO**

Fonte: elaborado pelo autor.

Sem dúvidas, a solução está adequada à nossa situação-problema, mas é claro que você pode ir muito mais a fundo nesta questão e buscar novos conhecimentos. Por enquanto, vamos partir para a próxima missão.

Avançando na prática

A questão da qualidade na segurança eletrônica

Descrição da situação-problema

Vamos nos concentrar em uma nova situação-problema? Sr. Khalil, libanês naturalizado brasileiro e pequeno comerciante de tecidos na capital paulista, resolveu instalar um sistema de vigilância por câmeras na sua residência, frente ao aumento da criminalidade em seu bairro. Contudo, não querendo gastar muito dinheiro com o sistema, ele comprou um produto de segunda linha, mas, segundo o vendedor, com a mesma qualidade dos outros e pela metade do preço, que alegou que ele mesmo havia desenvolvido o aplicativo para ver as imagens e, por isso, era um software simples. Após tudo instalado e funcionando, o sr. Khalil estava satisfeitíssimo, pois, com o aplicativo em seu celular, ele conseguia ver as imagens das câmeras pela internet, de qualquer lugar que estivesse. Certo dia, sr. Khalil e a família saíram para uma viagem de fim de semana e por lá ele percebeu que o aplicativo do seu celular já não mostrava mais as imagens de sua casa, o que simplesmente o deixou insatisfeito com o produto e o fez pensar em resolver o problema quando retornasse. Mas qual não foi a surpresa da família do sr. Khalil quando retornaram para casa e constataram que haviam sido vítimas de um assalto e que grande parte dos seus pertences haviam sido roubados. Diante do ocorrido, sr. Khalil, além de prestar queixa na polícia, foi procurar o vendedor do sistema de câmeras, quando se surpreendeu novamente, pois o responsável havia sumido da região e várias outras pessoas relataram que também enfrentavam problemas com o CFTV vendido por ele, que, na verdade, era de péssima qualidade e cheio de defeitos, porém ninguém havia sido vítima de assalto. Mas o que teria acontecido com o sr. Khalil? Como aquele sistema de vigilância por câmeras poderia ter favorecido os ladrões? Será que houve uso ou acesso ilegal ao

sistema? Quais vulnerabilidades o sistema poderia ter? Você é capaz de retirar essas dúvidas do sr. Khalil e das outras pessoas lesadas pelo vendedor?

Resolução da situação-problema

Infelizmente, caro aluno, o sr. Khalil foi mais uma vítima dos profissionais sem escrúpulos, que vendem produtos de má qualidade, e sem reputação no mercado. E, como não poderia deixar de ser, produto de segurança com má qualidade, nos deixam mais inseguros ainda. Para dirimir todas as dúvidas sobre o sistema, começaremos pelas vulnerabilidades mais prováveis, em virtude do assalto à residência do sr. Khalil, que seriam: erro de configuração ou programação do aplicativo, uma vez que foi desenvolvido de forma amadora por uma pessoa que talvez não dominasse o conhecimento necessário para essa atividade; e invasão por crackers, explorando o erro de programação, já que o sistema estava exposto à internet. Diante do levantamento dessas vulnerabilidades, podemos supor que alguém invadiu o aplicativo do celular do sr. Khalil e obteve acesso ilegal às imagens das câmeras, passando a monitorar a atividade da casa e, talvez, até a localização do sr. Khalil, através do GPS do celular. Percebendo que a casa estava já há algum tempo sem movimentação, ou até que o sr. Khalil estava longe, resolveu executar o roubo, porém, desligando antes a transmissão das imagens para o celular. Enfim, resta o ensinamento de que se tratando de produtos e serviços de segurança, deve-se sempre optar pelos profissionais e pelas empresas sérios, éticos e responsáveis, que ofereçam soluções com comprovada qualidade e que realmente sejam capazes de cumprir sua tarefa dentro da atividade de segurança.

Faça valer a pena

1. A atividade de monitoramento e rastreamento de veículos desenvolvida pelas empresas de segurança privada atingiu um nível excepcional de desempenho e eficiência; e grande parte deste sucesso pode ser atribuído a alta tecnologia empregada, tanto na localização do veículo quanto na comunicação entre o veículo e a central de segurança.

Em relação às tecnologias citadas no texto anterior, analise as afirmativas a seguir:

I. A tecnologia de radiofrequência (RF) é utilizada tanto para a localização do veículo quanto para a comunicação deste com a Central de Segurança.

II. O GPS ou sistema de posicionamento global é utilizado para saber a localização do veículo.

III. A tecnologia GPRS é utilizada para a comunicação do veículo com a Central de Segurança, através de internet móvel.

Assinale a alternativa que contém somente as afirmativas corretas.

a) I e II.
b) II e III.
c) I, II e III.
d) I e III.
e) Somente II.

2. Assim como os sistemas de informação, os SI utilizados na Segurança Privada têm vulnerabilidades, ou seja, pontos fracos que possibilitam a ação de ameaças através de ataques, comprometendo a segurança do sistema e, às vezes, até impossibilitando seu funcionamento.

Assinale a alternativa a seguir que apresenta corretamente uma vulnerabilidade dos SI de segurança, relacionada com o respectivo elemento da infraestrutura de TI.

a) Rede: falha nos dispositivos de armazenamento.
b) Software: erro de configuração.
c) Hardware: falha nas rotinas de cópias de segurança.
d) Ambiente: falha no firewall.
e) Banco de dados: quebra.

3. Sistema caracterizado por ser um conjunto de componentes eletrônicos que interagem entre si com a única finalidade de informar sobre a invasão ou violação do local que se deseja proteger, podendo ser empregado tanto em residências quanto em empresas.

A descrição anterior trata de um Sistema de Informação muito utilizado na segurança privada:

a) Sistema de Detecção e Combate a Incêndio.
b) Sistema de Gerenciamento da Segurança.
c) Sistema de Portaria Virtual.
d) Sistema de Alarme.
e) Sistema de Rastreamento.

Seção 3.3

Sistemas e informações na segurança pública

Diálogo aberto

Agora vamos empregar os conhecimentos adquiridos até o momento na resolução de mais uma situação-problema, ainda envolvendo o personagem Luke, que continua na sua carreira de vigilante, sem desistir do seu sonho de integrar a Polícia Militar, tendo em mente sempre que a dedicação aos estudos pode garantir uma boa vitória na vida. Foi com esse pensamento que o rapaz fez, novamente, a inscrição para o concurso para Soldado da Polícia Militar do Estado de São Paulo e, depois de horas de dedicação, de empenho nos estudos, finalmente, foi aprovado. Parece que sua vocação para a carreira militar se comprovaria. Ele havia acumulado experiência nas fileiras do Exército, depois no ramo da segurança privada e agora tomaria conhecimento da segurança pública. E, dessa maneira, foi matriculado na Escola de Formação de Soldados. O curso se estruturava em uma boa carga horária de prática de policiamento, mas não deixava de lado os estudos teóricos da questão da segurança e das intervenções necessárias para mitigar a criminalidade e manter a ordem. Luke percebeu que a questão da informação para combater o crime era fundamental. Os conceitos de inteligência e contrainteligência, não tão novos para o novo aprendiz de soldado, seriam fundamentais para que o planejamento e emprego contra a marginalidade fossem efetivos. Luke teve a oportunidade de conhecer alguns sistemas de informação da segurança pública e no combate ao crime, estando muito ansioso para colocar tudo em prática. Entretanto, durante o curso, recebeu a tarefa de realizar uma comparação entre todos os sistemas de informações existentes na área da segurança. Nesse contexto, qual é a sua função desses sistemas? Qual é a utilidade deles para a segurança pública e para a segurança privada? Que objetivos, dentro de cada tipo de segurança, são atingidos pelo SI? Ele deveria apresentar uma análise escrita comparando os sistemas de informação da segurança pública e privada. Luke ficou tranquilo, porque já estava no ramo da segurança privada e, por isso, conhecia alguns aspectos. Agora, seus desafios

seriam estudar todos os sistemas existentes e apresentá-los em detalhes, com foco na segurança pública. Como será que Luke fará essa tarefa? Dessa maneira, caro aluno, junto com nosso soldado Luke, vamos apresentar essa análise comparativa entre os sistemas da segurança pública e privada?

Como você vem se dedicando a realizar comparações dos sistemas dos dois setores abordados, uma vez que seu produto previsto é a **análise escrita sobre a comparação entre os sistemas de informação da segurança pública e privada**, nesta seção, finalizaremos o trabalho. Para concluí-lo, observe o quadro a seguir.

Quadro 3.5 | Finalização da comparação entre os sistemas de informação da segurança pública e privada

PÚBLICA	
SISTEMA DE INFORMAÇÃO UTILIZADO	**OBJETIVO**

Fonte: elaborado pelo autor.

Não pode faltar

Agora, prosseguiremos com os estudos sobre os Sistemas e as Informações na segurança pública, uma vez que já aprendemos bastante sobre aqueles na segurança privada. Avançaremos compreendendo o papel das informações na segurança pública, lembrando que já sabemos que a informação vem transformando a sociedade nos dias de hoje e atingindo todos os ramos de atividade, principalmente, por causa do largo emprego dos sistemas de informação que automatizaram os processos informacionais.

Na segurança pública, esta realidade não poderia ser diferente, ou seja, ocorre também um extenso emprego da informação e dos sistemas de informação como base para a promoção da ordem pública, do cumprimento das leis e da manutenção da integridade física das pessoas. Daí, então, a grande importância da informação para a segurança pública, qual seja, servir de base ou de suporte para a formulação de políticas, estratégias e ações que objetivem combater a criminalidade e manter a sociedade em segurança.

Nesse contexto, as informações mais relevantes são aqueles referentes às ocorrências delituosas, que comumente são chamadas de informações criminais, isto é, dizem respeito a assaltos, assassinatos, furtos, estupros, tráfico de drogas, roubo de automóveis, estelionato, sequestro, processos judiciais, enfim, tudo aquilo que se relaciona à consecução de algum crime ou ato ilegal, englobando também informações sobre pessoas físicas, jurídicas, armas, veículos e entorpecentes.

Assimile

A principal serventia da informação para a segurança pública é permitir o conhecimento sobre a criminalidade e seus processos associados, servindo de sustentação e fundamentando a concepção de políticas, estratégias e ações, visando combater a criminalidade e manter a sociedade em segurança, por meio da garantia da lei e da ordem e da preservação da vida e do patrimônio. Isso quer dizer que todas as operações de forças de segurança e forças policiais são realizadas com base nas estatísticas criminais.

É evidente que, para se combater o crime, quanto mais informações sobre os criminosos, suas formas de atuação e seus principais alvos, maior será a probabilidade de se obter sucesso. Para tanto, faz-se necessário que as informações criminais sejam submetidas a um processo de análise integrada, apoiado por sistemas de informação e bancos de dados, de forma que se consiga reunir a maior quantidade possível de informações para que se possa planejar ações objetivas e eficientes, tanto preventivas quanto repressivas, contra os marginais e as organizações criminosas.

Incorporado a este esforço, é preciso que se tenha à disposição diversas fontes de dados e informações criminais, podendo ser consideradas as fontes das polícias (militar, civil, federal, rodoviária, florestal, bombeiros), das corretoras de seguro de automóveis e imóveis, das empresas de segurança privada, da justiça (processos e mandados de prisão), das agências de inteligência, das guardas municipais, dos conselhos comunitários de segurança, dos disque denúncias e de qualquer outra fonte capaz de fornecer informações ou dados correlatos.

Uma vez coletados todos esses dados e todas essas informações, é necessário fazer um cruzamento ou uma análise estruturados dessa massa de informações, buscando traçar um cenário de onde possam ser extraídos perfis da criminalidade, contendo informações detalhadas sobre a forma de atuação dos marginais, que tipo de ameaça eles representam e quais vulnerabilidades eles mais atacam. Pode parecer um esforço hercúleo processar todos esses dados e todas essas informações, mas não esqueçamos que estamos na Era da Informação e grande parte, senão a totalidade, deste esforço será levado a efeito pelos sistemas de informação, baseados nas tecnologias de informação e comunicação, cabendo aos agentes públicos de segurança aprender com todas essas informações e aplicar sua genialidade e inventividade na concepção de planos de ação, capazes de mitigar as ações criminosas, promovendo um ambiente social seguro e confiável para a convivência das pessoas e a atividade das organizações.

A partir do conhecimento sobre o delineamento das atividades criminosas, é possível, dessa forma, formular estratégias e táticas mais eficientes e adequadas para fazer frente à criminalidade, de acordo com a particularidade dos tipos de crime e seu georreferenciamento, possibilitando reprimir a atividade criminosa em todas as frentes e de forma sistêmica.

Você se lembra de que estudamos o conceito de conhecimento logo na primeira unidade? No contexto da segurança pública, o trabalho envolvendo a obtenção e o processamento de informações, resultando na construção de conhecimento para dar suporte ao processo decisório dos órgãos de segurança pública, normalmente, é relativo à atividade de inteligência, que estudaremos mais adiante, assim como o ramo da contrainteligência, atividade desenvolvida paralelamente com a da inteligência.

Uma vez compreendido o papel da informação na segurança pública, podemos passar a identificar alguns sistemas de informação criminal existentes no Brasil e a situação atual dessas ferramentas e das tecnologias da informação e comunicações empregadas neste mister. O objetivo principal de um sistema de informação criminal deve ser incorporar as tecnologias de informação e comunicações para proporcionar a integração entre as fontes de dados de informações criminais, possibilitando o rápido compartilhamento

dessas informações entre os diversos órgãos de segurança pública, interessados em utilizá-las nas suas ações contra à criminalidade, já que a maioria dos casos exige uma pronta resposta à ação dos criminosos, de forma que não se perca a oportunidade de debelar a criminalidade.

Exemplificando

Para demonstrar o emprego desse tipo de sistema, podemos citar o Portal da Secretaria de Estado de Defesa Social de Minas Gerais, no qual é possível obter informações sobre drogas, ações preventivas de combate ao crime, integração entre os órgãos de segurança pública e o sistema prisional, além de estatísticas de criminalidade, inclusive, com gráficos, sobre homicídios, roubos, furtos e até violência doméstica contra a mulher.

Disponível em: <http://www.seds.mg.gov.br/>. Acesso em: 4 ago. 2017.

Sistemas dessa natureza servem para suprir a imprescindível necessidade de obtenção da informação criminal, às vezes, em tempo real, e isso envolve, por exemplo, a necessidade de um policial consultar a situação de um veículo ou de um delegado fazer vista aos autos de um processo. Com certeza, há tempos atrás, situações como essas seriam resolvidas através de um complexo trâmite burocrático e demorariam dias, semanas ou até meses para que a informação chegasse ao interessado. Dessa forma, inviabilizaria uma série de ações imediatas contra o crime, favorecendo, logicamente, os marginais, que, muitas vezes, escapavam das garras da polícia e da justiça devido à lentidão das ações dos agentes e órgãos públicos de segurança, imobilizados pela ausência de informação para agir efetivamente na manutenção da segurança da sociedade.

Entretanto, atualmente, a realidade é outra. Mesmo que longe do ideal, desde que a Rede Infoseg, principal sistema de informação criminal do Brasil, foi lançada, em 2004, a integração dessas informações vem sendo cada vez operacionalizada, ajudando sobremaneira as ações de combate ao crime. Nesse cenário, nos aprofundaremos um pouco mais na Rede Infoseg.

Inicialmente, esta rede foi criada, em 2004, nos Estados do Rio Grande do Sul, Paraná e Santa Catarina, que reuniram esforços

com o objetivo de integrar as informações de segurança pública, abrangendo informações das polícias, da justiça, do Departamento Nacional de Trânsito, da Receita Federal e de outros, distribuindo o acesso, via internet, a todos aqueles integrantes da segurança pública que, por ventura, delas necessitassem, abrangendo desde os gabinetes das autoridades em segurança pública até as viaturas dos policiais que atuam nas ruas.

Nessa época, o sistema já contava com uma robusta e flexível infraestrutura de tecnologia da informação e comunicação que permitia a consulta on-line das informações de forma segura, descomplicada e confiável (PAULA, 2011). A partir dessa primeira iniciativa, o Ministério da Justiça, por intermédio da Secretaria Nacional de Segurança Pública (SENASP), passou a trabalhar no avanço da Rede Infoseg, idealizando um novo sistema que permitisse a integração de informações criminais entre todos os estados da federação, incluindo órgãos e entidades do Executivo, Legislativo e Judiciário e até entidades privadas, além de franquear acesso aos cidadãos, já que até então o sistema era voltado somente para os agentes públicos de segurança.

Dessa iniciativa nasceu o Sistema Nacional de Informações de Segurança Pública (Sinesp), com o lançamento do Portal Sinesp Infoseg, lembrando que já apresentamos a você, de forma sucinta, este portal, na Seção 3 da Unidade 2 deste livro didático. De fato, esta evolução não parou por aí e o Sinesp continuou evoluindo e recebendo novos incrementos e atualizações.

Atualmente, o Sinesp apresenta duas vertentes básicas: o Sinesp Segurança e o Sinesp Cidadão. O primeiro é dedicado aos agentes públicos de segurança e fiscalização, disponibilizando informações sobre pessoas físicas e empresas, veículos, motoristas, mandados de prisão, armas de fogo, processos, investigações, inquéritos e boletins de ocorrência, dentre várias outras. Já o segundo está voltado ao público, em geral, através, inclusive, de aplicativo de celular, e reúne informações sobre pessoas desaparecidas, situação de veículos e mandados de prisão, além de permitir a participação popular na melhoria das estratégias de segurança pública por meio de enquetes e participações em eventos de segurança pública, com o objetivo de aproximar a sociedade das questões de segurança pública no Brasil.

Recentemente, o Ministério da Justiça anunciou o lançamento de um novo Sinesp, que integrará, em âmbito nacional, as informações sobre justiça, fiscalização, segurança, defesa civil, identificação criminal, inteligência e registro civil (RG). Além disso, este novo sistema contará com uma potente ferramenta de pesquisa, possibilitando a obtenção de informações através da associação de múltiplos parâmetros de entrada e com o acesso totalmente via Internet, incluindo dispositivos móveis. A ideia é que o novo Sinesp possa contribuir ainda mais nas ações contra a criminalidade, facilitando a análise sobre os crimes, permitindo uma contenção dos riscos e potencializando as ações operacionais, bem como o trabalho de planejamento e estruturação dos meios empregados na segurança pública.

Ainda segundo informação disponibilizada pelo Conselho Nacional de Justiça, em página da internet (BRASIL, 2017), o sistema passará a contar com uma base nacional unificada e integrada de dados, dividida em três grandes blocos:

- **Informações sobre pessoas**: reunindo dados da Interpol, Receita Federal, do Sistema Único de Saúde (SUS), do Ministério do Trabalho e Emprego (MTE), do Sistema Integrado de Informações de Segurança do Mercosul (SISME), do Banco Nacional de Mandados de Prisão (BNMP) e outros.
- **Informações sobre veículos**: combinando informações do Sistema Integrado Nacional de Identificação de Veículos em Movimento (Sinevem), do Sisme, da Agência Nacional de Transportes Terrestres (ANTT), Departamento Nacional de Trânsito (Denatran), etc.
- **Informações sobre armas**: englobando registros do Sistema Nacional de Armas (Sinarm) da Polícia Federal, do Sistema de Gerenciamento Militar de Armas (Sigma) do Exército Brasileiro, do Cadastro Nacional de Apreensão de Drogas e Bens Relacionados (Sinad) e da Rede Desarma Brasil.

Como podemos verificar, o Brasil tem um sistema já muito bem estruturado de informações criminais, empregando tecnologias de ponta e disponibilizando informações de forma rápida, objetiva e confiável, multiplicando o potencial das estruturas de segurança públicas em combater com efetividade o avanço da criminalidade, através da promoção da integração das informações coletadas pelos diversos setores envolvidos na segurança pública no país.

Dessa forma, você percebe que, seguindo o viés do Sinesp, conseguimos apresentar inúmeros outros sistemas de informação criminal existentes no Brasil? Assim sendo, conseguimos atingir mais um dos nossos objetivos.

Avançando nesta seção, passaremos a estudar os conceitos de inteligência e contrainteligência, com os quais nossos objetivos serão compreender a definição e identificar as particularidades desse ramo de atividade. Inicialmente, é preciso deixar claro que abordaremos esse tema do ponto de vista da Segurança Pública, já que esse tipo de atividade apresenta muitas vertentes e nuances que a diversificam bastante.

Focaremos, portanto, na Inteligência de Segurança Pública. Entenderemos, antes de mais nada, onde se enquadra a Inteligência de Segurança Pública (ISP) dentro do contexto nacional. No Brasil foi instituído, pela Lei nº 9.883, de 7 de dezembro de 1999, o Sistema Brasileiro de Inteligência, com a criação da Agência Brasileira de Inteligência (ABIN), tendo como objetivo regulamentar toda a atividade de inteligência no país, estipulando também que a atividade de inteligência tem dois ramos de atuação, quais sejam, a inteligência e a contrainteligência.

A partir da Lei n° 9.883/1999 foram publicados o Decreto nº 3.695, de 21 de dezembro de 2000, que criou o Subsistema de Inteligência de Segurança Pública (SISP), com a finalidade de coordenar e integrar as atividades de Inteligência de Segurança Pública no Brasil, dando suporte ao processo decisório dos governos federal e estaduais no tocante às estratégias e ações de Segurança Pública; e o Decreto nº 4.376, de 13 de dezembro de 2002, que regulamentou a organização e o funcionamento do Sistema Brasileiro de Inteligência. Em seguida, vieram a Resolução nº 1, de 15 de julho de 2009, da Secretaria Nacional de Segurança Pública, regulamentando o Subsistema de Inteligência de Segurança Pública, e a Doutrina Nacional de Inteligência de Segurança Pública como fechamento da regulamentação desta atividade no âmbito da federação brasileira.

Visto isso, passaremos, com base no que está estipulado nessa legislação, a estudar essa atividade, começando pelo conceito de inteligência, atividade de obtenção e análise detalhada de um conjunto de dados, gerando informações importantes para o mapeamento da criminalidade, para o acompanhamento e entendimento das

atividades criminosas e para a identificação de marginais, permitindo a produção dos conhecimentos necessários para a promoção da Segurança Pública. Além disso, segundo o artigo 2º, do Decreto nº 4.376/2002, inteligência é a atividade de obtenção e análise de dados e informações e de produção e difusão de conhecimentos, apoiando o processo decisório e as ações de governo relacionadas à segurança da sociedade (BRASIL, 2002, art. 2º).

Ainda mais especificamente, a Resolução nº 1/2009 conceitua Inteligência de Segurança Pública como a atividade duradoura e sistêmica que tem por objetivo identificar, monitorar e classificar as ameaças existentes e iminentes sobre a Segurança Pública, produzindo os conhecimentos e as informações necessários ao planejamento e à execução de políticas dessa segurança, bem como operações de prevenção, neutralização e repressão de ações delituosas de qualquer tipo (BRASIL, 2009, art. 1º, § 4º, III).

Dessa maneira, podemos inferir resumidamente que Inteligência de Segurança Pública é a atividade de obter e analisar dados, produzindo informações e conhecimento que darão suporte ao processo decisório dos órgãos de segurança pública no combate à criminalidade.

Agora que já conhecemos o conceito de inteligência, podemos atentar a algumas particularidades desta atividade. Nesta, um ponto-chave é justamente a obtenção de dados, já que, normalmente, esta atividade envolve a busca por dados que não estão disponíveis ao público em geral, seja por causa de suas características particulares, ou por sua grande importância e valor, ou pela necessidade de sigilo. A partir disso, faz-se necessário que esta atividade seja desenvolvida somente por profissionais especializados e devidamente credenciados para esse ofício, desenvolvendo suas funções de forma discreta e, na maioria das vezes, em segredo, fato este previsto na legislação.

Reflita

Durante muitos anos, a atividade de inteligência foi vista com "maus olhos" no Brasil, tanto que o Serviço Nacional de Informações (SNI), criado pelo Presidente Castello Branco, em 1964, foi extinto pelo Presidente Fernando Collor de Mello, em 1990. Este serviço só foi retomado institucionalmente em 1999, pelo Presidente Fernando Henrique Cardoso, com a Lei nº 9.883 e a criação da ABIN. Mas qual seria o problema desta atividade?

E por que ainda, atualmente, muitas pessoas ficam incomodadas só em ouvir falar na atividade de inteligência? Você já pensou nisso? Talvez esta seja uma boa oportunidade para você formular sua opinião sobre esse assunto, com pleno conhecimento da causa.

Segundo a Doutrina Nacional de Inteligência de Segurança Pública, esta atividade se desenvolve basicamente pela obtenção dos dados, produção do conhecimento e comunicação do conhecimento. Dessa forma, vejamos cada um deles.

Você se lembra do conceito de dado, o qual dados são fatos brutos? A **obtenção dos dados** considera basicamente os tipos de fonte e os meios utilizados. As fontes de dados podem ser: abertas, aquelas cujo acesso aos dados é livre e ilimitado; e protegidas, isto é, aquelas nas quais os dados são resguardados e o acesso é negado. Os meios de obtenção de dados são os humanos e os eletrônicos, sendo que, na Inteligência Humana, o objetivo da obtenção da informação é o homem e, na Inteligência Eletrônica, os objetivos são centrados nos equipamentos, podendo-se ter a Inteligência de Sinais, relativa à interceptação de sinais de comunicação; a Inteligência de Imagens, relacionada à obtenção de imagens de câmeras, radares, sensores e satélites; e a Inteligência de Dados, envolvendo a captura de dados eletrônicos em computadores ou redes de telecomunicação.

A obtenção de dados pode ser feita por meio de Ações de Inteligência (coleta ou busca) e Operações de Inteligência (exploratórias ou sistemáticas), a diferença entre elas é que aquelas se ocupam da obtenção de dados de fontes abertas ou protegidas que não requeiram grandes esforços para acessá-las, e estas são ações que visam a obtenção de dados de fontes protegidas de difícil acesso e de alto risco, que exigem o emprego de pessoas, técnicas e equipamentos específicos.

A **produção do conhecimento** compreende o tratamento dos dados e das informações coletadas por um profissional especialista, Analista de Inteligência, sendo, inclusive, o responsável pela produção do conhecimento. O conhecimento produzido pelo Analista de Inteligência pode ser qualificado em quatro tipos diferentes:

• **Informe**: é resultante do julgamento feito pelo Analista de Inteligência, expressando suas certezas, opiniões ou dúvidas em relação à verdade sobre um fato ou uma situação passada ou presente.

• **Informação**: é fruto do raciocínio realizado pelo Analista de Inteligência, manifestando sua certeza sobre a verdade de um fato ou uma situação passada ou presente.

• **Apreciação**: também é resultado do raciocínio realizado pelo Analista de Inteligência, mas que apresenta sua opinião sobre a verdade de um fato ou uma situação passada ou presente.

• **Estimativa**: é fruto do raciocínio elaborado pelo Analista de Inteligência e que revela sua opinião sobre a tendência futura de um fato ou uma situação.

Após a obtenção dos dados e a produção do conhecimento, resta que as pessoas e entidades interessadas façam uso desse conhecimento. Para isso, é necessário que seja feita a comunicação ou **transmissão do conhecimento** produzido, que, normalmente, é realizada por meio de um documento de Inteligência conhecido como **Relatório de Inteligência**, ou seja, um documento, via de regra sigiloso e que tem um padrão de formatação, no qual o Analista de Inteligência transmite os conhecimentos produzidos para as entidades e pessoas interessadas ou outras agências de inteligência.

Na certeza de que alinhamos os principais aspectos da atividade da Inteligência de Segurança Pública, passaremos agora a estudar o ramo da contrainteligência de segurança pública. Esta é o ramo da atividade de Inteligência de Segurança Pública que tem por finalidade realizar ações e produzir conhecimento para proteger a atividade de Inteligência, através de medidas para salvaguardar os dados, as informações e os conhecimentos sigilosos, por meio da neutralização de ameaças que podem se manifestar na forma de espionagem, vazamentos, sabotagens, terrorismo, etc. A contrainteligência de Segurança Pública, segundo a Doutrina Nacional de Inteligência de Segurança Pública, deve atuar nos seguimentos da Segurança Orgânica, de Assuntos Internos e da Ativa, de acordo com o detalhamento a seguir.

• **Segurança Orgânica**: conjunto de medidas para proteger o pessoal, a documentação, as instalações, o material, as comunicações e a informática, todas descritas no Plano de Segurança Orgânica.

• **Segurança de Assuntos Internos**: tem como principal objetivo a produção de conhecimento para ajudar a corregedoria dos órgãos de Segurança Pública.

• **Segurança Ativa:** são medidas de caráter ativo para identificar e combater as ações adversas direcionadas contra a sociedade e podem ser operacionalizadas através da contrapropaganda, da contraespionagem, da contrassabotagem e do contraterrorismo.

Assimile

De forma geral, perceba que todas estas medidas com o prefixo "contra" denotam uma ação oposta. Por exemplo, contraespionagem são aquelas medidas destinadas a neutralizar as ações de espionagem.

Pesquise mais

Para aumentar seus conhecimentos em inteligência e contrainteligência de Segurança Pública, conheça e estude a Doutrina Nacional de Inteligência de Segurança Pública.

MINISTÉRIO DA JUSTIÇA. Secretaria Nacional de Segurança Pública. **Doutrina Nacional de Inteligência de Segurança Pública**. Revisão das Normas Metodológicas: Prof. Dr. José Luiz Gonçalves da Silveira. 2. ed. Brasília: Coordenadoria-Geral de Inteligência, 2009.

Mais uma etapa da nossa disciplina foi concluída e, mais uma vez, com a aquisição de conhecimentos muito valorosos para a construção das competências necessárias para o profissional da área de segurança, seja atuando no setor público, seja atuando no privado. Dessa forma, continuaremos resolvendo nossa situação-problema.

Sem medo de errar

Estamos de volta para a resolução de mais uma das nossas situações-problemas e, desta vez, resolveremos aquela tarefa, que o nosso amigo, agora Soldado PM Luke, precisa cumprir no seu curso de formação: elaborar uma análise escrita sobre a comparação entre os Sistemas de Informação (SI) da Segurança Pública e Privada, sendo este o produto final desta unidade. Portanto, para isso, é necessário que preenchamos o quadro a seguir.

Veja como ficará a nossa **comparação entre os sistemas de informação da segurança pública e privada**.

Quadro 3.6 | Finalização da comparação entre os sistemas de informação da segurança pública e privada

CLASSIFICAÇÃO DAS INFORMAÇÕES	
PÚBLICA	**PRIVADA**
Ultrassecreta: Presidente da República, Vice-presidente da República, Ministros de Estado, Comandantes da Forças Armadas (Marinha, Exército e Aeronáutica) e Chefes de Missões Diplomáticas e Consulares. Secreta: pelas autoridades já citadas, titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista. Reservada: por todas as autoridades anteriores mais as que ocupem cargos de direção, comando ou chefia, de nível igual ou superior ao DAS 101.5.	As informações pessoais sob custódia do Estado e referentes à intimidade, à honra e à imagem das pessoas, não recebem uma classificação especial, porém têm seu acesso igualmente restrito devido à garantia do direito de privacidade.
PRAZOS DE SIGILO	
PÚBLICA	**PRIVADA**
Ultrassecreta: 25 (vinte e cinco) anos. Secreta: 15 (quinze) anos. Reservada: 5 (cinco) anos.	Independente de classificação sigilosa: 100 (cem) anos. As informações relativas à intimidade, à vida privada, à honra e à imagem das pessoas devem ter seu acesso restrito por 100 anos (BRASIL, 2011, art. 31, §1°).

CONTROLE DAS INFORMAÇÕES	
PÚBLICA	**PRIVADA**
É dever do Estado somente permitir o acesso à informação sigilosa para pessoas devidamente credenciadas; garantir que a pessoa que obteve acesso à informação sigilosa preserve o sigilo da informação; e providenciar que as autoridades públicas adotem ações para garantir que seus funcionários subordinados conheçam as normas e cumpram os procedimentos para proteção da informação sigilosa. A LAI também prevê que a pessoa física ou entidade privada que, por motivo de vínculo com o poder público, tenha acesso à informação sigilosa, deverá também zelar pela manutenção do grau de sigilo da informação, atitude esta extensiva aos seus empregados, colaboradores e pessoal relacionado.	As informações pessoais, sob custódia do Estado, também têm restrição de acesso e seu controle seguirá a mesma conduta adotada para as informações sigilosas. A LAI não estabelece nenhum controle para informações privadas custodiadas por pessoas físicas ou jurídicas da iniciativa privada.
PRAZOS PARA RESPOSTA A PEDIDOS DE INFORMAÇÃO	
PÚBLICA	**PRIVADA**
O órgão ou a entidade pública deve conceder o acesso imediato às informações solicitadas e, caso não seja possível, terá um prazo de 20 (vinte) dias, podendo ser prorrogado por mais 10 (dez) para marcar uma data para liberação do acesso à informação ou apresentar as justificativas para a negativa de acesso. Nos casos em que o acesso à informação for negado, o interessado poderá recorrer desta decisão junto ao próprio órgão, em um prazo de 10 (dez) dias, ou apelando para a Controladoria-Geral da União (CGU), tanto um quanto o outro terão o prazo de 5 (cinco) dias para responder ao recurso do interessado.	Os prazos serão os mesmos das informações públicas, porém somente para informações pessoais, sob custódia do Estado. A LAI não estabelece nenhum prazo para resposta a pedidos de informação para informações privadas sob custódia de pessoas físicas ou jurídicas da iniciativa privada.

ACESSO ÀS INFORMAÇÕES	
PÚBLICA	**PRIVADA**
Qualquer pessoa ou organização poderá solicitar acesso e somente não receberá permissão para isso se a informação solicitada for sigilosa ou de caráter pessoal e privada.	A critério das pessoas físicas ou jurídicas a que as informações se referirem, ou por imposição legal, de acordo com os critérios previsto na LAI.

SISTEMAS E INFORMAÇÕES EMPREGADOS NA SEGURANÇA	
PRIVADA	
SISTEMA DE INFORMAÇÃO UTILIZADO	**OBJETIVO**
Sistemas de Monitoramento por Câmeras.	Vigilância de áreas com grande circulação de pessoas e veículos e monitoramento de acesso a prédios, lojas, condomínios e residências.
Sistemas de Vigilância de Perímetro.	Detectar a violação do perímetro sob vigilância, um condomínio, uma fábrica, uma loja, um estacionamento, determinando a localização do ponto de rompimento ou invasão.
Sistemas de Controle de Acesso.	Identificar pessoas, materiais e veículos, permitindo ou negando acesso às instalações de um prédio, loja e condomínio.
Sistemas de Alarme.	Para dar o alerta sobre a violação de instalações em residências, pequenos comércios e em pontos sensíveis dentro de uma empresa de médio e grande porte, tais como: almoxarifados, setor financeiro e instalações de TI.
Sistemas de Detecção e Combate a Incêndio.	Identificar um foco de incêndio em uma instalação patrimonial, acionando dispositivos de alarme e pulverização de água.
Sistemas de Rastreamento e Monitoramento.	Monitorar o deslocamento de veículos, pessoas, valores, produtos, encomendas para inibir furtos, roubos e sequestros.

Sistemas de Portaria Virtual.	Utilizar um sistema remoto capaz de monitorar toda a segurança de prédios e instalações com base no compartilhamento da central de segurança.
Sistemas de Gerenciamento da Segurança.	Planejamento da segurança com base na análise de riscos.
Central de Segurança.	Centralizar todos os controles dos diversos serviços de segurança, fazendo o gerenciamento e comando das ações de segurança.
PÚBLICA	
SISTEMA E INFORMAÇÃO UTILIZADA	**OBJETIVO**
Informação Criminal.	Servir de base para a formulação de políticas, estratégias e ações que objetivem combater a criminalidade e manter a sociedade em segurança.
Portal Sinesp Infoseg.	Incorporar as tecnologias de informação e comunicações para proporcionar a integração entre as fontes de dados de informações criminais, possibilitando o rápido compartilhamento dessas informações entre os diversos órgãos de Segurança Pública.
Sinesp Segurança.	Disponibilizar, para os agentes públicos de segurança e fiscalização, uma ferramenta de consulta às informações sobre pessoas físicas, empresas, veículos, motoristas, mandados de prisão, armas de fogo, processos, investigações, inquéritos e boletins de ocorrência.
Sinesp Cidadão.	Disponibilizar, para o público em geral, informações sobre pessoas desaparecidas, situação de veículos e mandados de prisão, além de permitir a participação popular na melhoria das estratégias de segurança pública por meio de enquetes e participações em eventos de segurança pública.

Fonte: elaborado pelo autor.

Excelente, aluno, concluímos a nossa tarefa desta Seção 3.3 e, com ela, nosso produto da Unidade 3. Parabéns e sucesso na próxima missão!

Avançando na prática

Inteligência no cotidiano

Descrição da situação-problema

Dessa vez, você acompanhará a tarefa de Álvaro Araponga, um Analista de Inteligência da Polícia Federal (PF), que trabalha em uma Agência de Inteligência (AI). Certa vez, Álvaro foi selecionado para compor um grupo de trabalho (GT) que deveria apresentar um estudo solicitado pela Secretaria de Segurança Pública do Rio de Janeiro (SSP/RJ). A missão de Álvaro, nesta tarefa, era produzir conhecimentos sobre o prognóstico da evolução da criminalidade na Baixada Fluminense, com base nos índices de tráfico de drogas, homicídios e apreensão de armas. Dessa forma, Álvaro realizou seu trabalho de forma eficiente e discreta, documentando tudo e colaborando com o estudo do GT. No entanto, no dia de entregar o pronto da sua missão, verificou que o documento produzido por ele e salvo no servidor de arquivos da AI não estava mais na sua pasta, sendo encontrado mais tarde em uma outra pasta de arquivos. Nesse contexto, aluno, sua tarefa será responder aos seguintes questionamentos: Para que a SSP/RJ solicitou um estudo a Inteligência da PF? Que tipo de conhecimento Álvaro deveria produzir para cumprir sua missão? Justifique sua resposta. Que tipo de fonte e que meios Álvaro poderia empregar para obter os dados necessários ao seu trabalho? Será que ele pode utilizar um Sistema de Informação Criminal do Brasil? Caso positivo, quais são eles? Qual documento de Inteligência que o GT deveria elaborar para enviar a SSP/RJ e por quê? Que segmento da AI deveria ter providenciado a proteção do servidor de arquivo? E que documento deve ser revisado depois desse problema? Com base nos conhecimentos adquiridos nesta seção, o que você supõe que poderia ter ocorrido com o arquivo do Álvaro? Todas essas respostas produzidas por você devem ser apresentadas em um resumo.

Resolução da situação-problema

Resumidamente, apresentaremos algumas possíveis respostas para os questionamentos apresentados. A SSP/RJ poderia ter solicitado tal estudo a Inteligência da PF a fim de conhecer melhor a atuação da criminalidade, utilizando esse conhecimento como fundamento na concepção de políticas, estratégias e ações de segurança pública. Para tanto, Álvaro deveria produzir uma Estimativa, um conhecimento que revelaria a opinião dele sobre a tendência futura da criminalidade na Baixada Fluminense. Na busca de dados, Álvaro poderia usar fontes abertas, empregando meios eletrônicos, principalmente através da Inteligência de Dados, minerando dados nos Sistemas de Informação de Segurança Pública do Rio de Janeiro ou através do Portal Sinesp, consultando o Banco Nacional de Mandados de Prisão (BNMP), o Sistema Nacional de Armas (SINARM) ou o Cadastro Nacional de Apreensão de Drogas e Bens Relacionados (Sinad). Em resposta à solicitação da SSP/RJ, deveria ser enviado um Relatório de Inteligência, documento padronizado para a transmissão dos conhecimentos produzidos por uma AI para as entidades e pessoas interessadas. Já a proteção do servidor de arquivo deveria ter sido providenciada pelo pessoal da contrainteligência, que deve fazer a proteção da Inteligência, e, após o ocorrido, deve ser feita uma revisão no Plano de Segurança Orgânica que prevê as medidas de segurança para esse tipo de situação. Em relação ao ocorrido com o arquivo do Álvaro, pode-se supor que tenha acontecido uma ação de espionagem e até o vazamento das informações.

Conseguimos mais uma vez e, para finalizar, só falta o questionário.

Faça valer a pena

1. O Sistema Brasileiro de Inteligência e Agência Brasileira de Inteligência (ABIN) foram instituídos no Brasil com o objetivo de regulamentar toda a atividade de inteligência no país, estipulando também que esta atividade tem os ramos da inteligência e a da contrainteligência.

Assinale a única alternativa a seguir que contém o dispositivo legal que criou o Sistema Brasileiro de Inteligência e Agência Brasileira de Inteligência (ABIN).

a) Decreto nº 3.695, de 21 de dezembro de 2000.

b) Resolução nº 1, de 15 de julho de 2009.

c) Decreto nº 4.376, de 13 de dezembro de 2002.

d) Constituição Federal, de 5 de outubro de 1988.

e) Lei nº 9.883, de 7 de dezembro de 1999.

2. A Doutrina Nacional de Inteligência de Segurança Pública estabelece que uma das atividades da Inteligência de Segurança Pública é a produção de conhecimento, através da análise e do tratamento dos dados e das informações por um profissional especialista, o Analista de Inteligência, que, no desempenho de suas tarefas, pode produzir quatro tipos diferentes de conhecimento, de acordo com o estado da sua mente e o trabalho intelectual por ele desenvolvido.

Considerando o exposto no texto anterior, associe os conhecimentos produzidos pelo Analista de Inteligência, da coluna da esquerda, com suas respectivas definições, apresentadas na coluna da direita. Em seguida, marque a alternativa que contém a sequência correta de associações.

I. Informe.	1. Produto do raciocínio elaborado pelo Analista de Inteligência e que revela sua opinião sobre a tendência futura de um fato ou de uma situação.
II. Informação.	2. Fruto do raciocínio realizado pelo Analista de Inteligência, manifestando sua certeza sobre a verdade de um fato ou de uma situação passada ou presente.
III. Apreciação	3. Resultante do julgamento feito pelo Analista de Inteligência, expressando suas certezas, opiniões ou dúvidas em relação à verdade sobre um fato ou uma situação passada ou presente.
IV. Estimativa.	4. Resultado do raciocínio realizado pelo Analista de Inteligência, mas que apresenta sua opinião sobre a verdade de um fato ou de uma situação passada ou presente.

a) I-3; II-1; III-4; IV-2.

b) I-2; II-1; III-4; IV-3.

c) I-3; II-2; III-4; IV-1.

d) I-2; II-3; III-4; IV-1.

e) I-1; II-2; III-4; IV-3.

3. Atualmente, o Portal Sinesp é um dos mais importantes sistemas de informações criminais do Brasil e o Ministério da Justiça. Através da Secretaria Nacional de Segurança Pública, está constantemente buscando atualizar e renovar esta ferramenta, tanto que recentemente lançou o aplicativo Sinesp Cidadão, conforme mostra a figura a seguir.

Figura | Aplicativo Sinesp Cidadão

Fonte: Aplicativo Sinesp Cidadão (2017).

Com base no texto anterior, na figura apresentada e nos conhecimentos aprendidos nesta seção sobre o Portal Sinesp, assinale a única alternativa que contém uma afirmação válida sobre o aplicativo Sinesp Cidadão.

a) O aplicativo permite a participação popular na melhoria das estratégias de segurança pública, por meio de enquetes e participações em eventos de segurança pública, com o objetivo maior de aproximar a sociedade das questões de segurança pública no Brasil.

b) A consulta a um mandado de prisão, através do Banco Nacional de Mandados de Prisão (BNMP), disponível no Sinesp Cidadão, não é o mesmo disponibilizado no Sinesp Segurança.

c) Através do aplicativo não é possível obter informação sobre a situação de um automóvel.

d) O Sinesp Cidadão é uma poderosa ferramenta de participação da população na promoção da segurança pública, permitindo até a consulta a registros de armas e as formas de participar de campanhas de desarmamento.

e) Através do aplicativo Sinesp Cidadão não é possível obter informações sobre uma criança desaparecida, por exemplo.

Referências

BRASIL. Conselho Nacional de Justiça (CNJ). Ministério da Justiça (Org.). **Infoseg**. 2017. Disponível em: <http://www.cnj.jus.br/sistemas/infoseg>. Acesso em: 1 jun. 2017.

_____. **Lei nº 9.883**, **de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9883.htm>. Acesso em: 7 ago. 2017.

_____. **Decreto nº 3.695**, **de 21 de dezembro de 2000**. Cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência, e dá outras providências. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3695.htm>. Acesso em: 7 ago. 2017.

_____. **Decreto nº 4.376**, **de 13 de dezembro de 2002**. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei no 9.883, de 7 de dezembro de 1999, e dá outras providências. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4376compilado.htm>. Acesso em: 7 ago. 2017.

_____. Ministério da Justiça – Secretaria Nacional de Segurança Pública. **Resolução nº 1**, **de 15 de junho de 2009**. Regulamenta o Subsistema de Inteligência de Segurança Pública - SISP, e dá outras providências. Brasília, DF.

_____. Ministério da Justiça – Secretaria Nacional de Segurança Pública. **Doutrina Nacional de Inteligência de Segurança Pública**; Revisão das Normas Metodológicas: Profº Dr. José Luiz Gonçalves da Silveira. 2ª Edição – Brasília: Coordenadoria-Geral de Inteligência, 2009.

BRASILIANO, Antonio Celso Ribeiro; BLANCO, Lucas. **Manual de planejamento tático e técnico em segurança empresarial**. São Paulo: Sicurezza, 2003. 174 p.

PAULA, G. de. **Sistema de informações em segurança**. 2011. Portal de e-governo, inclusão digital e sociedade do conhecimento. Disponível em: <http://egov.ufsc.br/portal/conteudo/sistema-de-informações-em-segurança>. Acesso em: 1 jun. 2017.

KLEIN, Rodrigo Maciel. **Dicas para levar em consideração antes de contratar um sistema de rastreamento veicular**. 2016. Disponível em: <https://www.rotaexata.com.br/dicas-para-contratar-um-sistema-de-rastreamento-veicular/>. Acesso em: 29 maio 2017.

LAUDON, Kenneth C.; LAUDON, Jane P.. **Sistemas de informação gerencial**. 7. ed. São Paulo: Pearson Prentice Hall, 2007. 452 p.

SOARES, Plácido Ladercio. **Segurança patrimonial**. São Paulo: Sicurezza, 2008. 95 p. (Coleção Segurança Operacional).

STAIR, Ralph M.; REYNOLDS, George W.. **Princípios de sistemas de informação**. 11. ed. São Paulo: Cengage Learning, 2015. 719 p.

A gestão do conhecimento na segurança pública e privada

Convite ao estudo

Caro aluno, na Unidade 3, estudamos os sistemas e as informações na segurança pública e privada e verificamos a importância das informações e desses sistemas de informação para agilizar os processos relacionados à segurança, permitindo o acompanhamento da dinâmica do mundo moderno. Continuando nossos estudos, nos dedicaremos, nesta unidade, ao estudo da gestão do conhecimento, das técnicas e tecnologias para o suporte do conhecimento e à gestão do conhecimento nas organizações e na segurança pública e privada, principalmente, por causa da grande rapidez que as coisas acontecem na Era da Informação. O conhecimento passou a ser um grande diferencial na manutenção da qualidade dos produtos e serviços de uma organização, uma vez que permite a rápida adaptação às constantes mudanças que vivenciamos atualmente. Lembrando que a competência geral da nossa disciplina é interpretar a gestão do conhecimento dentro do contexto da segurança pública e da segurança privada, consideraremos o seguinte contexto para a nossa aprendizagem: "No mundo atual, somente terá sucesso aquele que tiver disponível as melhores informações e, na hora certa, aquele que souber gerir melhor o conhecimento". Foi uma frase que Marilinda Fernandes ficou pensando, após sair de uma das aulas do curso superior de Tecnologia - CST em Gestão da Segurança Privada, que cursava há mais de um ano. Mas por que será que informação e conhecimento são tão importantes? Para que serve o Capital Intelectual? Essas eram algumas das perguntas de Marilinda. Ela trabalhava na Guardian Segurança Patrimonial e havia acabado de ser aprovada no concurso de

escrivão da polícia civil do Estado de São Paulo. Marilinda já estava na Guardian há mais de dez anos, lugar no qual havia começado como auxiliar de monitoramento eletrônico e, com o tempo, tornou-se supervisora de segurança. A Guardian Segurança Patrimonial era uma das empresas de segurança especializada em segurança bancária, que garantia isso por meio de seu monitoramento remoto. Marilinda, inclusive, é uma expert em sistemas de monitoramento à distância. Entretanto, esta supervisora sabia que, a partir da aprovação no concurso, teria novos desafios pela frente. Grande era sua expectativa quanto à possibilidade de utilizar todo o conhecimento que tinha na segurança patrimonial, aplicado a uma função da segurança pública. E quanto aos conceitos aprendidos no CST que vinha cursando, será que estes seriam também aplicáveis à nova função? Nesse contexto, vamos ver como Marilinda se sairá em seu novo cargo?

Para que consigamos aprender tudo isso, deveremos entender o que é gestão do conhecimento, quais são as técnicas e tecnologias que dão suporte ao conhecimento nas organizações e como é realizada a gestão do conhecimento nas organizações e na segurança pública e privada.

Dessa forma, vamos iniciar nossos estudos?

Seção 4.1

A gestão do conhecimento

Diálogo aberto

Caro aluno, estamos de volta a mais uma das nossas situações-problema e, desta vez, aplicaremos nossos conhecimentos sobre a gestão do conhecimento, no caso da personagem Marilinda Fernandes, aprovada no concurso de escrivão de polícia civil e que, finalmente, tomou posse de seu cargo no 33º Distrito Policial – DP de Pirituba. A novata sabia que não seria uma tarefa tão simples, afinal, tratava-se de um DP da maior cidade do Brasil, complexa e com várias ocorrências policiais a serem registradas todos os dias. Chegando à delegacia, ela foi muito bem recepcionada por Franklin da Silveira, um escrivão, com mais de trinta e cinco anos de serviço e muita experiência na área. Franklin sabia muito bem todos os processos, todas as leis, os chamados "pulos do gato" e, com boa vontade, começou a tentar transmitir parte do que sabia. Entretanto, Marilinda, ao começar a entender as peculiaridades da função, ficou um tanto quanto apreensiva, porque Franklin havia anunciado que permaneceria apenas quatro meses na DP, o prazo final de seus trabalhos, uma vez que se aposentaria. Assim, como Marilinda se sairia, uma vez que passaria a ser a única escrivã da delegacia?

Ela, nas aulas da faculdade, tinha ouvido falar sobre o processo de transmissão do conhecimento, mas não se lembrava muito bem desse assunto. Nesse contexto, Marilinda passou a refletir sobre algumas questões: a aula de conhecimento tácito e explícito se aplica neste meu caso? A delegacia ou o Estado tem algum programa que prepara os novos escrivães? E agora? Conseguirei aprender toda as minhas tarefas em tão pouco tempo?

Estas são as dúvidas de Marilinda e você, caro aluno, terá a missão de, na posição de escrivão da polícia, responder a todos estes e outros questionamentos, com a finalidade de demonstrar as ações sobre a gestão do conhecimento deste cargo, com a finalidade de que as atividades deste sejam bem cumpridas depois que Marilinda substitua Franklin definitivamente. Baseando-se nos aspectos da gestão do conhecimento, um dos desafios será demonstrar como

transmitir o conhecimento e a aprendizagem organizacional, evitando a interrupção de atividades e processos na delegacia de polícia.

Com certeza, depois de ler o *Não pode faltar*, você terá condições de apontar todas as soluções.

Não pode faltar

Caro aluno, após estudarmos uma infinidade de conteúdos sobre o emprego dos sistemas de informação em segurança, ingressaremos na nossa última unidade didática, buscando aprender a perpetuar tudo aquilo que uma organização, que atua na área de segurança, aprende, desenvolve e transmite de experiência e conhecimento para promover a segurança. Para tanto, iniciaremos, na Seção 4.1, os estudos com a gestão do conhecimento, começando pelo próprio conceito de conhecimento, já estudado na Seção 1.1, na qual vimos que este indica um grau de compreensão que vai além das informações; pois além de um significado, pode ter uma aplicação, isto é, o conhecimento é a compreensão de um conjunto de informações, por meio do raciocínio e da experiência, e como estas podem ser úteis para a execução de uma determinada tarefa ou tomada de alguma decisão (STAIR; REYNOLDS, 2015). Para Takeuchi e Nonaka (2008), existem dois tipos de conhecimento: o explícito, ou seja, aquele que pode ser expresso por palavras, números ou sons e facilmente compartilhado na forma de dados, fórmulas, especificações, relatórios e manuais; e o tácito, isto é, aquele de foro pessoal e difícil de ser formalizado, como palpites subjetivos, intuições, emoções, valores e ideais.

Assimile

Tipos de conhecimento:

- **Explícito**: pode ser expresso por palavras, números ou sons e facilmente compartilhado na forma de dados, fórmulas, especificações, relatórios e manuais. É manipulado e comunicado de forma fácil.
- **Tácito**: altamente pessoal e difícil de ser formalizado, como palpites subjetivos, intuições, emoções, valores e ideais. Existe na cabeça das pessoas e é obtido por meio da experiência adquirida ao longo da vida.

Exemplificando

Como exemplo de **conhecimento explícito**, podemos citar um vigilante que realizará um exercício de tiro em um estande e que lê as regras de segurança com armas de fogo afixadas no mural, antes da seção de tiro.

Já no que se refere ao **conhecimento tácito**, este pode ser aplicado no seguinte contexto: um policial recém-ingresso na corporação observa a conduta de seus companheiros, na abordagem de suspeitos, e depois reflete e interioriza os procedimentos mais importantes, para poder ter uma atuação melhor em abordagens futuras.

Ainda segundo Takeuchi e Nonaka (2008), nos dias atuais e em plena Era da Informação, o conhecimento passou a ser a única fonte permanente de vantagem competitiva e, por esse motivo, as empresas vêm buscando, cada vez mais, soluções para fazer a gestão ou o gerenciamento do conhecimento. A gestão do conhecimento pode ser definida, dessa forma, como sendo o processo que tem por objetivo gerar, transmitir, armazenar e incorporar, nas atividades da organização, os conhecimentos produzidos por ela, por meio do processamento de dados e informações, envolvendo desde o emprego de sistemas de informação até a interpretação e compreensão através do raciocínio e da experiência dos colaboradores da empresa, sempre dentro de um processo de agregar significado aos dados e às informações (FRANCO; RODRIGUES; CASELA, 2013).

Assimile

Gestão do conhecimento: processo que tem como objetivo criar, transmitir, armazenar e incorporar, nas atividades da organização, os conhecimentos produzidos por ela, seja por meio do processamento dos dados e das informações pelos sistemas de informação, seja através da interpretação e compreensão desses dados e dessas informações pelos seus colaboradores, sempre em um processo de agregar significado a isso.

Já entendemos que a desenfreada evolução tecnológica associada à grande mudança global decorrente da explosão da informação nos conduziu para a Era da Informação e fez que as organizações passassem a viver em uma rotina constante de busca por uma vantagem competitiva, baseada, via de regra, na informação e na

inovação, como a única forma de sobrevivência no mercado em que atuam. Esta dinâmica vivenciada pelas organizações têm gerado uma grande quantidade de conhecimento, já que a informação é a mola propulsora dessa revolução e a matéria-prima do conhecimento.

Para gerar todo esse conhecimento e buscar a criação e a inovação tão almejadas pelas organizações, as pessoas têm sido muito exigidas, uma vez que constituem o único recurso capaz de gerar o conhecimento, através de sua habilidade de raciocínio, interpretação e integração. Sendo assim, ao contrário do que acontecia no passado, no qual os recursos físicos eram as mais importantes riquezas das empresas, porque eram responsáveis pela eficiência produtiva que representava o grande diferencial competitivo do mercado, atualmente, percebemos que as pessoas passaram a assumir o protagonismo na tarefa de aumentar a vantagem competitiva das organizações, justamente pela sua capacidade de produzir conhecimento, gerando inovação nos produtos e serviços e satisfazendo, de forma mais efetiva, os clientes. Dessa forma, o capital intelectual das organizações passou a ser formado.

Nesse cenário, como as pessoas não são propriedades das empresas, assim como as máquinas e os insumos de produção, ao deixarem a organização, elas levam consigo toda a experiência e todo o conhecimento adquiridos durante sua jornada de atividade na companhia. Diante desta situação, as organizações se vêm obrigadas a desenvolver métodos e estratégias para, além de disseminar os conhecimentos individuais de seus colaboradores e agregá-los em novos produtos e serviços, armazená-los, de forma permanente, para que não sejam perdidos ou simplesmente partam junto com as pessoas. Esta prática é chamada de gestão do conhecimento.

Em resumo, tudo que argumentamos até agora serve como base para o entendimento do que é a aprendizagem organizacional, ou seja, uma moderna e inovadora forma de gestão organizacional, fundamentada na formação de uma cultura organizacional que privilegia a participação de seu principal recurso, qual seja, o colaborador. No modelo de gestão alicerçado na aprendizagem organizacional, destaca-se a gestão do conhecimento e o capital intelectual.

Nesse contexto, a aprendizagem organizacional passou a ser de fundamental importância para as organizações porque promove a

expansão e a disseminação do conhecimento dentro da empresa, exteriorizando-se em uma dinâmica contínua que tem por objetivo transformar esses conhecimentos em vantagem competitiva, manifestada na criação e inovação de produtos e serviços (FRANCO; RODRIGUES; CASELA, 2013). Além disso, aprendizagem organizacional envolve o constante aperfeiçoamento dos recursos humanos, através de cursos e treinamentos que proporcionem o crescimento intelectual dos funcionários, motivando-os a participarem ativamente do processo de ampliação do conhecimento na organização, além da satisfação própria advinda do crescimento pessoal e da motivação pelo desenvolvimento profissional, fazendo que os colaboradores se sintam cada vez mais valorizados e reconhecidos como pessoas e profissionais.

Reflita

Imagine uma empresa pequena de segurança privada que comercializa soluções e serviços de controle de acesso, mas que praticamente todos os projetos de implantação de serviços são elaborados a partir do conhecimento de um único funcionário, o qual trabalha na empresa desde sua fundação. Mas, quando a empresa não puder mais contar com esse funcionário, como ela ficará? E se ele pedir demissão? E quando ele se aposentar? Você concorda que o conhecimento vital para o negócio da empresa não pode ficar na mão de somente uma pessoa? Você já pensou nisso? Você conhece algum caso assim?

A partir da abordagem da aprendizagem organizacional, teve início um novo ciclo da teoria organizacional que elevou o funcionário ao patamar de principal recurso da empresa, precisamente por sua capacidade de gerar conhecimento, consolidando a ideia de que as pessoas são o que fazem as empresas serem o que elas são, ao invés do que se pensava antes, ou seja, que as companhias existiam por conta de seus equipamentos e de suas máquinas que produziam cada vez mais. Daí surgiu o conceito de capital intelectual, que, segundo a definição de Franco, Rodrigues e Casela (2013), é o conjunto de componentes imateriais da organização que tem a capacidade de aumentar o valor organizacional, proporcionando vantagem competitiva para a empresa.

O capital intelectual, portanto, deve ser corretamente administrado pela empresa, principalmente aquele conhecimento pertencente a alguns poucos funcionários, mas que compõe a base fundamental de expertises indispensáveis para a existência da empresa. A gestão do capital intelectual deve valorizar tanto o conhecimento quanto a experiência das pessoas na atividade da organização, como forma de estimular o processo de criação de mais conhecimento e elevar, portanto, a vantagem competitiva da empresa.

Além disso, esse capital é considerado um ativo intangível da empresa, uma vez que faz parte dos recursos organizacionais, difíceis de serem percebidos e, muito mais, de serem medidos ou registrados, mas que compõem um patrimônio imaterial importantíssimo para o sucesso da organização e sua sobrevivência no mercado.

Reflita

Caro aluno, perceba que já abordamos, algumas vezes, o conceito de *vantagem competitiva*. Você entende o quanto ele é importante para as organizações modernas? Além disso, quanto é significativa a relação entre esse conceito e capital intelectual?

O capital intelectual está estruturado, segundo Franco, Rodrigues e Casela (2013), como o somatório dos ativos intangíveis, formados pela estrutura externa, pela estrutura interna e pela competência individual de cada colaborador.

A **estrutura externa** compreende a marca da empresa (Ex.: Coca-Cola, Ferrari, Apple), suas relações com os clientes, a imagem da organização e sua reputação no mercado. Já a **estrutura interna** é composta pelos seus processos de trabalho, sistemas de informação, manuais, pesquisas e outros. A **competência individual**, por sua vez, engloba a escolaridade, as competências, a experiência, os valores, as habilidades, as emoções e as atitudes das pessoas que trabalham para a organização.

Assimile

São ativos intangíveis de uma organização:

- **Estrutura externa**: marca, relacionamento com os clientes, imagem e reputação.
- **Estrutura interna**: processos de trabalho, sistemas de informação, manuais, pesquisas e outros.
- **Competência individual**: escolaridade, competência, experiência, valores, habilidades e emoções.

Atualmente, o valor de mercado de uma organização inclui a soma de seus ativos tangíveis (prédios, dinheiro, máquinas, estoques) e seus ativos intangíveis, que podem agregar um valor considerável ao patrimônio total da empresa.

Exemplificando

Para demostrar que os ativos intangíveis podem agregar muito mais valor ao patrimônio da empresa do que os tangíveis, vejamos o exemplo do Instagram, que foi comprado pelo Facebook, em 2012, por 1 bilhão de dólares e, atualmente, mesmo sem gerar nenhum faturamento, está estimado em um valor de mercado de mais de US$ 33 bilhões, tudo por causa dos seus mais de 300 milhões de usuários no mundo inteiro. Disponível em: <http://convergecom.com.br/tiinside/20/02/2015/instagram-tem-valor-de-mercado-de-us-33-bilhoes-segundo-consultoria/>. Acesso em: 4 set. 2017.

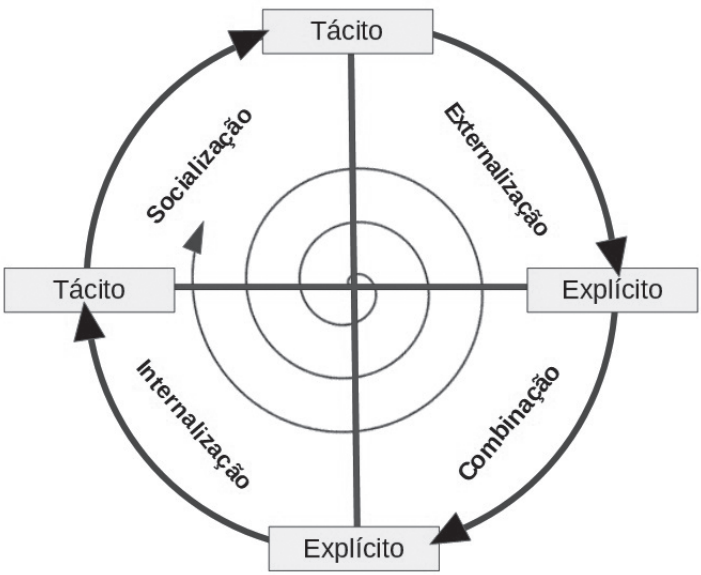
Depois de aprender sobre a questão da aprendizagem organizacional, da gestão do conhecimento e do capital intelectual, entenderemos, agora, o processo de criação do conhecimento.

Segundo Takeuchi e Nonaka (2008), a gestão do conhecimento ainda pode ser vista como um ciclo contínuo de criação de conhecimento, no qual as organizações devem gerar o conhecimento, transmiti-los rapidamente por toda sua estrutura organizacional e incorporá-los no lançamento de novos produtos e serviços. Esse processo de criação acaba envolvendo os vários níveis da organização (operacional, tático e estratégico) em um movimento de interação para transformar o conhecimento

tácito em explícito, em um processo conhecido como SECI (Socialização – Externalização – Combinação – Internalização), o qual exploraremos mais intensamente a partir de agora.

O processo de criação do conhecimento organizacional chamado de **SECI** é fruto de uma dinâmica interativa e constante envolvendo o conhecimento tácito (subjetivo) e o explícito (objetivo). Desta interação podemos identificar quatro processos diferentes de conversão do conhecimento, quais sejam: **socialização**, conversão do conhecimento tático para conhecimento tácito; **externalização**, conversão do conhecimento tácito para conhecimento explícito; **combinação**, conversão do conhecimento explícito para conhecimento explícito; e **internalização**, conversão do conhecimento explícito para conhecimento tácito (TAKEUCHI; NONAKA, 2008). Esses quatro processos são integrados através da **espiral do conhecimento**, que se inicia na socialização, já que todo novo conhecimento surge a partir de uma pessoa, passando por todos os modos de conversão do conhecimento e ampliando o conhecimento organizacional (vide Figura 4.1).

Figura 4.1 | Espiral do conhecimento



Fonte: adaptada de Takeuchi e Nonaka (2008).

Nesse contexto, vejamos como funciona cada um desses processos de criação do conhecimento, segundo Takeuchi e Nonaka (2008).

- **Socialização**: geralmente é um processo que envolve a interação entre dois indivíduos, que compartilham e criam conhecimento tácito por meio de uma troca mútua de experiências e saberes, como o estagiário que aprende com seu chefe e pares através da observação e imitação das práticas da empresa. No entanto, este tipo de conhecimento é muito difícil de ser formalizado e relatado, constituindo, dessa maneira, uma forma um tanto quanto limitada de criação de conhecimento organizacional.

- **Externalização**: configura um processo de interação entre o indivíduo e o grupo, articulando o conhecimento tácito, através da conversação e da reflexão, e criando o conhecimento explícito. Em outras palavras, é quando o indivíduo consegue sistematizar todo o conhecimento tácito, desenvolvido por meio de sua experiência trabalhando na organização, em um conhecimento explícito, através de ações, planos ou documentos, de forma que possa ser compartilhado e entendido pelo grupo, produzindo inovações nos processos da empresa.

- **Combinação**: é um processo que relaciona um grupo de colaboradores com a empresa como um todo, sistematizando e aplicando o conhecimento explícito, evidenciado na forma de informações, em um sistema de gestão do conhecimento, no qual o grupo troca conhecimento explícito com a empresa de forma estruturada e sistemática. Nesse processo, o conhecimento explícito é obtido de fontes internas e externas à organização para, dessa forma, ser combinado ou associado, a fim de formar um novo conhecimento explícito que permitirá à organização inovar em suas práticas e processos de trabalho.

- **Internalização**: neste processo ocorre uma relação entre o colaborador e a empresa, na qual aquele adquire novos

conhecimentos tácitos através do compartilhamento dos novos conhecimentos explícitos por esta. Em outras palavras, os colaboradores passam a internalizar o novo conhecimento explícito, utilizando-o na prática para criar ou aumentar seus próprios conhecimentos tácitos. A partir desse momento, o novo conhecimento passa a compor a cultura organizacional.

Com base no conteúdo apresentado, podemos, neste momento, imaginar que após um ciclo completo da espiral do conhecimento, ou seja, a cada internalização de novos conhecimentos explícitos, um novo conhecimento estará consolidado na cultura da organização e, portanto, pronto para ingressar em um novo ciclo, e mais um e outro, em uma constante e interminável interação que promove o aperfeiçoamento e a inovação na organização. Dessa forma, entendemos que a criação de conhecimento é um processo que engloba tanto os indivíduos quanto os grupos e a organização como um todo, sendo necessário que a empresa estimule e facilite, além da aprendizagem individual de cada colaborador, através de cursos e treinamentos, atividades em grupo, nas quais as pessoas possam compartilhar conhecimento dentro e fora de seus times, por meio de encontros, workshops e dinâmicas, os quais impulsionam a aprendizagem organizacional.

Pesquise mais

Para saber mais sobre o processo de criação do conhecimento e a espiral do conhecimento, leia o Capítulo 3 – Teoria da Criação do Conhecimento Organizacional, em: TAKEUCHI, H.; NONAKA, I. **Gestão do conhecimento**. Porto Alegre: Bookman, 2008. 320 p.

Assim, chegamos ao final de mais uma seção, na qual conseguimos aprender os conceitos de gestão do conhecimento e de capital intelectual, compreendendo que é através deles que a aprendizagem organizacional acontece, viabilizando a inovação e ampliando a vantagem competitiva da empresa. Além disso, identificamos como ocorre o processo de criação do conhecimento por meio da espiral do conhecimento, enfatizando

que o novo conhecimento é resultante da integração dos indivíduos, dos grupos e da própria organização. Dessa forma, temos condições de partir para a solução da nossa situação-problema. Vamos seguir em frente!?

Sem medo de errar

Caro aluno, Marilinda está, de fato, diante de um grande desafio e, para enfrentá-lo, os conhecimentos adquiridos nos bancos escolares sobre gestão do conhecimento podem auxiliá-la e muito a lograr êxito na adaptação à sua nova função de escrivã de polícia. O processo de passagem do conhecimento a que Marilinda se referiu em uma de suas indagações é o mesmo processo de criação do conhecimento que aprendemos como "espiral do conhecimento", naquele movimento de interação para transformar o conhecimento tácito em explícito, em um processo conhecido como SECI (Socialização – Externalização – Combinação – Internalização), no qual a **socialização** é o compartilhamento de conhecimento tácito através da troca direta de experiências, as quais Marilinda passará a viver junto com o seu colega Franklin; a **externalização** é a articulação do conhecimento tácito através da conversação e da reflexão para criar o conhecimento explícito; a **combinação** é a sistematização e aplicação do conhecimento explícito; e a **internalização** é a obtenção de novo conhecimento tácito a partir da prática do conhecimento explícito recém-adquirido. Nesse contexto, a aula de conhecimento tácito e explícito que Marilinda estudou faz relação e se aplica totalmente em sua atual situação. Com certeza, a polícia civil tem um programa de preparação de novos escrivães, porém, muito provavelmente também este programa de treinamento estará voltado para passar o conhecimento explícito relativo ao cargo e que deverá ser praticado pelos novos policiais, evidenciando um processo de internalização desses conhecimentos. Mas para que Marilinda desempenhe suas funções com eficiência e objetividade, é muito importante que ela consiga aprender, ao máximo, com Franklin da Silveira, que apresenta bastante experiência na função e poderá ajudá-la no processo de socialização. Além disso, este conhecimento tácito, apesar de

não estar escrito em lugar algum, será de grande valia para que Marilinda consiga resolver por si mesma depois da aposentadoria do Franklin. Raciocinando desta forma e conseguindo organizar sua rotina segundo o processo de transmissão do conhecimento, Marilinda conseguirá aprender todas suas tarefas nesses quatro meses que dispõe antes da partida de seu colega de trabalho.

Avançando na prática

Quem sabe, sabe!

Descrição da situação-problema

Caro aluno, observaremos, agora, a situação que envolve Geraldo Gonçalves, um experiente gerente de segurança que trabalhava há mais de dez anos na SafetyExpress, uma organização de escolta armada de cargas. A imagem atual da empresa é fruto da grande experiência pessoal de Geraldo no ramo, que desenvolveu uma técnica própria para planejar itinerários seguros, livrando-se das ameaças e empregando a escolta armada com eficácia na condução da carga até seu destino final. A técnica desenvolvida por Geraldo era tão complexa e considerava tantas variáveis que nem mesmo o fundador da empresa conseguia entender como ele fazia aquilo, mas o importante é que dava certo, tanto que a SafetyExpress se tornou uma das melhores empresas deste ramo. Entretanto, com a partida do antigo dono e a assunção da direção da empresa pelo seu filho e herdeiro, Geraldo passou a se sentir desiludido com a SafetyExpress porque não vinha sendo devidamente reconhecido pela nova direção da companhia e estava muito insatisfeito. Em virtude desse cenário, Geraldo resolveu aceitar uma proposta da GoSafely, uma concorrente da SafetyExpress, e partiu em busca de novas realizações. Na GoSafely, ele recebeu total liberdade para implantar sua técnica de trabalho, além de contar com todo apoio da diretoria nos seus projetos e ganhar mais. Após sua contratação, a GoSafely, em pouco tempo, começou a ganhar mercado e a crescer dia após dia, enquanto a SafetyExpress via seus clientes mais fiéis migrarem para a concorrente e seu negócio ir de mal a pior.

Considerando o contexto apresentado, aluno, faça um resumo destacando a importância do conhecimento de Geraldo para a SafetyExpress e os principais erros cometidos pela empresa, dentro do que foi aprendido nesta seção sobre a gestão do conhecimento.

Resolução da situação-problema

Com o caso apresentado, é possível perceber como a gestão do conhecimento assume um papel vital para a organização. Mas vamos ao que interessa, ou seja, as falhas que a SafetyExpress cometeu neste quesito. Como todo o diferencial competitivo da SafetyExpress estava baseado no conhecimento tácito de Geraldo Gonçalves em planejar itinerários seguros para a escolta armada, a companhia cometeu vários erros, que serão listados a seguir, em relação à gestão desse conhecimento como forma de sobrevivência no mercado:

- Não criou condições para que Geraldo transmitisse seu conhecimento para outros colaboradores da empresa, ao invés de trabalhar sozinho.
- Não buscou uma forma de transformar o conhecimento tácito de Geraldo em conhecimento explícito para a empresa.
- Não se preocupou em armazenar, de maneira formal, o conhecimento de Geraldo.
- Deixou de valorizar Geraldo como um dos principais recursos e seu cabedal de conhecimentos específicos e importantes que fazem parte do capital intelectual.
- Não promoveu a disseminação e expansão do conhecimento de Geraldo no âmbito interno da empresa.
- Não reconheceu o conhecimento de Geraldo como sua principal vantagem competitiva.
- Não identificou que o conhecimento de Geraldo incorporou inovação aos seus serviços.

Faça valer a pena

1. Sabemos que conhecimento indica um grau de compreensão que transcende a informação, porque, além do significado, pode ter uma aplicação na prática. Ainda, para produzir conhecimento, é necessário a intervenção humana, através do raciocínio e da experiência, agregando significado à informação.

Com base no conceito de conhecimento, analise as afirmações a seguir:

I. Atualmente, na Era da Informação, o conhecimento vem demonstrando ser uma importante fonte permanente de vantagem competitiva.

II. A produção do conhecimento envolve somente os sistemas de informação e o processamento de dados.

III. Para a produção do conhecimento, a matéria-prima é a informação.

IV. O processo que objetiva criar, transmitir, armazenar e incorporar conhecimento nas atividades da organização é chamado de gestão do conhecimento.

Estão corretas somente as afirmações:

a) I e IV.

b) I, III e IV.

c) II e III.

d) II, III e IV.

e) III e IV.

2. No modelo de gestão alicerçado no(a) _____, ganha ênfase o(a) _____ e o(a) _____, porque possibilitam a expansão e a disseminação do conhecimento no ambiente interno da organização.

A partir da frase anterior, assinale a alternativa que contém as palavras adequadas às lacunas.

a) gestão do conhecimento – aprendizagem organizacional – capital intelectual.

b) aprendizagem organizacional – conhecimento – informação.

c) gestão do conhecimento – informação – conhecimento.

d) aprendizagem organizacional – gestão do conhecimento – capital intelectual.

e) gestão do conhecimento – capital intelectual – informação.

3. O processo de criação do conhecimento acaba envolvendo os vários níveis de uma organização, desde o operacional, passando pelo tático ou gerencial, até o estratégico, em um movimento de interação que transforma o conhecimento organizacional, expandindo-o continuamente em um processo conhecido como SECI.

Considerando o processo SECI de criação de conhecimento organizacional, podemos afirmar que a conversão de conhecimento explícito para conhecimento tácito é chamada de:

a) Internalização.

b) Somatização.

c) Combinação.

d) Externalização.

e) Socialização.

Seção 4.2

Técnicas e tecnologias para o suporte ao conhecimento

Diálogo aberto

Caro aluno, vamos relembrar nosso contexto de aprendizagem? Conhecemos, na seção anterior, a história de Marilinda Fernandes, uma dedicada aluna do curso superior de Tecnologia - CST em Gestão da Segurança Privada, que já estava no último semestre e havia assumido o cargo de escrivão de polícia. Marilinda venceu os desafios e acabou dominando todos os conteúdos necessários para desempenhar suas tarefas com efetividade e contribuir muito em sua função, quando recebeu o telefonema de sua amiga, Mônica Aparecida, da faculdade. Mônica não hesitou em buscar ajuda, sabendo que Marilinda havia passado dificuldades em absorver todos os novos conhecimentos de sua função. Ela também havia se destacado em sua carreira e acabado de assumir o cargo de gestora de segurança em sua empresa de segurança patrimonial. Mônica Aparecida era chefe de alguns inspetores de segurança, sendo responsável por vários municípios, nos quais sua companhia executava serviços de segurança patrimonial e de escolta e guarda. Seu grande desafio era treinar, desenvolver e atualizar os conhecimentos e procedimentos dos vigilantes integrantes de sua equipe. Como o serviço de segurança patrimonial acontecia em vários locais e empresas diferentes, reunir todos os vigilantes em um mesmo local, em uma mesma data, para informar novas condutas, era realmente quase impossível. Quando Marilinda tomou conhecimento desses óbices, logo sugeriu à amiga: "Não daria para realizar um treinamento on-line, igual àquela aula que tivemos sobre e-learning?". Mônica achou a ideia interessante e pensou: como desenvolver um sistema que permita treinamento por meio de computadores e da internet? Nossa empresa tem estrutura para implementar tal sistema de informação? Qual será o conteúdo que terei de passar para os nossos funcionários? Eles realmente aprenderão à distância? Nesse contexto, você, na posição de Mônica, como garantiria que seus colaboradores

fossem treinados por meio de um sistema de informação, ou melhor, um sistema de gestão do conhecimento? Para resolver essa situações, seguiremos com os estudos.

Não pode faltar

Caro aluno, vencida a primeira parte desta unidade, na qual aprendemos bastante sobre a gestão do conhecimento, na Seção 4.1, partiremos, agora, para o estudo das técnicas e tecnologias para o suporte ao conhecimento, começando pelo entendimento da relação entre os sistemas de informação com a gestão do conhecimento. Para tanto, deveremos retornar ao conceito de sistemas de informação, aprendido na Seção 1.1, que, segundo Laudon e Laudon (2007), trata-se do conjunto de elementos inter-relacionados, que trabalham colaborativamente para coletar, processar, armazenar e transmitir informações em uma organização, apoiando seus processos decisórios; mas que, para Stair e Reynolds (2015), é o conjunto de componentes que se relacionam entre si para coletar, manipular e disseminar informações dentro das empresas; ou, resumindo, um sistema de informação é um todo coeso e organizado, que contém componentes (pessoas, processos e tecnologias) que se relacionam entre si para coletar dados, processá-los, armazená-los e difundir informações, provenientes desses dados, para a organização, a fim de maximizar sua produtividade. Além disso, relembrar o conceito de gestão do conhecimento, recém-aprendido na Seção 4.1, faz-se importante. Segundo Franco, Rodrigues e Casela (2013), este conceito é o processo que objetiva criar, transmitir, armazenar e incorporar, nas atividades da organização, os conhecimentos produzidos por ela, seja por meio do processamento dos dados e das informações pelos sistemas de informação, seja através da interpretação e compreensão destes e das informações pelos seus colaboradores, agregando sempre um significado a esses pontos.

Reflita

Considerando que o conhecimento somente pode ser criado pelo ser humano, por que empregar tecnologias para dar suporte ao

conhecimento? Qual seria o papel destas na criação do conhecimento? Até que ponto o emprego delas, na gestão do conhecimento, é válido? Será que elas complicarão mais do que facilitarão?

Depois de recordar esses conceitos relevantes para o estudo, podemos, a partir deste momento, descrever a ligação entre os sistemas de informação e a gestão do conhecimento. Antes, no entanto, devemos entender também que para uma organização desenvolver suas atividades e seus processos são empregados os conhecimentos de várias pessoas, as quais, geralmente, possuem treinamento, experiência, criatividade, motivação, opinião e inteligência para executarem suas tarefas, e é rigorosamente a integração dos conhecimentos desses indivíduos que resultará na conquista do objetivo final da organização.

Para promover a integração entre os conhecimentos das pessoas envolvidas nas atividades e nos processos da organização, os sistemas de informação e a gestão do conhecimento se vinculam um ao outro. Nesta vinculação, estes dois sistemas darão origem aos sistemas de informação de gestão do conhecimento ou sistemas integrados de gestão do conhecimento (SIGC).

Cabe lembrar, ainda, que os sistemas de gestão do conhecimento (SGC) darão suporte tecnológico à gestão do conhecimento, permitindo que cada um dos envolvidos nas tarefas organizacionais possam ter acesso ao conhecimento do outro, em qualquer lugar e a qualquer momento, viabilizando, desta forma, a integração de saberes dentro e fora da organização (STAIR; REYNOLDS, 2015).

Nesse contexto, podemos considerar os sistemas integrados de gestão do conhecimento basicamente uma grande coleção de dados e informações que suprem as necessidades de conhecimento das pessoas, possibilitando que estas incorporem saberes de outras áreas do conhecimento distintas das delas, mas que as permitirão complementar seus próprios saberes, potencializando sua produtividade e sua capacidade de atuar como fonte criadora de novos conhecimentos.

Segundo Stair e Reynolds (2015), um sistema integrado de gestão do conhecimento deve ter como finalidade ajudar as pessoas e as

organizações a alcançarem suas metas, ora dando total suporte para alguma ação decisiva, ora auxiliando na descoberta e correção de algum problema.

Um sistema de gestão do conhecimento, também conhecido como *Knowledge Management System* (KMS), pode envolver tanto o conhecimento explícito, aquele expresso em relatórios e manuais, quanto o conhecimento tácito, aquele subjetivo, altamente pessoal e difícil de ser formalizado, porém as organizações se esforçam para converter o conhecimento tácito em conhecimento explícito e, dessa forma, armazená-lo e disseminá-lo através dos sistemas de gestão do conhecimento. Para Laudon e Laudon (2007), esses sistemas melhoram a qualidade e a utilização do conhecimento usado tanto no processo decisório quanto no desenrolar das atividades da organização, aumentando a capacidade da empresa de criar novos conhecimentos organizacionais e incorporá-los aos seus processos, produtos e serviços, como forma de obter vantagem competitiva, já que os conhecimentos compartilhados dentro da empresa agregam valor à organização.

Encerrando a primeira parte desta seção, podemos, dessa maneira, apresentar uma definição para sistema de gestão do conhecimento, que, na visão de Stair e Reynolds (2015), é um conjunto organizado de pessoas, processos, softwares aplicativos, sistemas de banco de dados e qualquer outra tecnologia utilizada para criar, armazenar, compartilhar e utilizar o conhecimento e a experiência das pessoas e da própria organização.

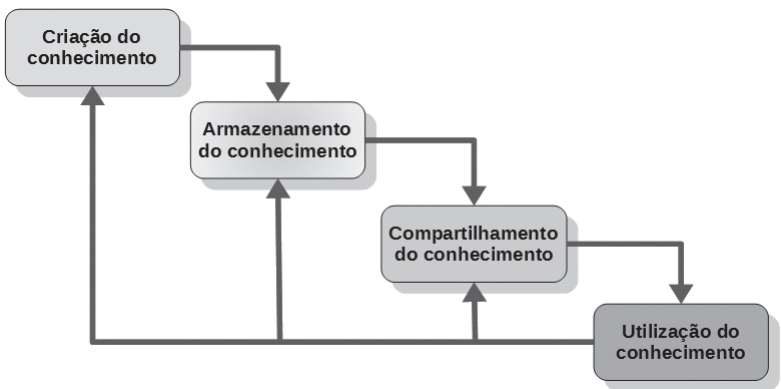
Assimile

Sistema de gestão do conhecimento é um conjunto organizado de pessoas, processos, softwares aplicativos, sistemas de banco de dados e qualquer outra tecnologia utilizada para criar, armazenar, compartilhar e utilizar o conhecimento e a experiência das pessoas e da própria organização.

Compreendida esta primeira etapa, passaremos a identificação de como é a gestão do conhecimento nas empresas. Para Stair e Reynolds (2015), esta envolve desde os funcionários que lidam com

os dados brutos até aqueles que manipulam o conhecimento. Isto significa que as secretárias, assistentes e auxiliares normalmente fazem a entrada de dados no sistema, no nível operacional da empresa, e, de modo geral, utilizam sistemas de processamento de transações (SPT). A partir desses dados, passam a fazer parte do processo os profissionais do conhecimento, que podem ser engenheiros, arquitetos, advogados, contadores e pesquisadores, dentre outros, que terão o encargo de criar, disseminar e utilizar o conhecimento na organização. Neste cenário também pode existir a figura do diretor de conhecimento que, via de regra, trata-se de um gestor de alto nível que ajuda a empresa a utilizar o sistema de gestão do conhecimento para criar, armazenar, compartilhar e utilizar o conhecimento para atingir os objetivos organizacionais (vide Figura 4.2). Atualmente, existe a praxe de compartilhar conhecimento por meio de comunidades na internet, nas quais profissionais de determinadas áreas do conhecimento ou com algum interesse em comum participam interagindo e compartilhando uma imensidão de conhecimentos e experiências de forma rápida e eficaz, originando uma abundante quantidade de conhecimento novo. Muitas vezes, eles acabam alcançando soluções primorosas para resolver desde os mais simples problemas até as questões da mais alta complexidade, concorrendo muito para a conquista de objetivos individuais, coletivos e organizacionais.

Figura 4.2 | Esquema de um sistema de gestão do conhecimento



Fonte: adaptada de Stair e Reynolds (2015).

Após sua criação, o novo conhecimento é armazenado em um conjunto de conhecimentos, composto por documentos, relatórios, arquivos de computador e grandes bancos de dados. Esse repertório, no qual o conhecimento está armazenado, é acessado pelas pessoas interessadas em compartilhar deste conhecimento e utilizá-lo para contribuir com a conquista dos objetivos organizacionais, além de gerar novos conhecimentos realimentando todo o ciclo novamente (Figura 4.2).

Segundo Laudon e Laudon (2007), os conhecimentos criados na própria empresa constituem um recurso organizacional importantíssimo para a construção de uma vantagem competitiva sólida e capaz de aumentar a lucratividade do negócio, sendo que as empresas somente conseguirão atuar com eficiência no mercado se seus conhecimentos estiverem disponíveis no momento certo para o desenvolvimento de suas atividades produtivas ou para serem aplicados em alguma decisão. Nesse contexto, Laudon e Laudon (2007) consideram dois principais tipos de sistemas de gestão do conhecimento para atender a esse tipo de demanda das organizações, são eles: os **sistemas integrados de gestão do conhecimento** (SIGC) e os **sistemas de trabalhadores do conhecimento** (STC).

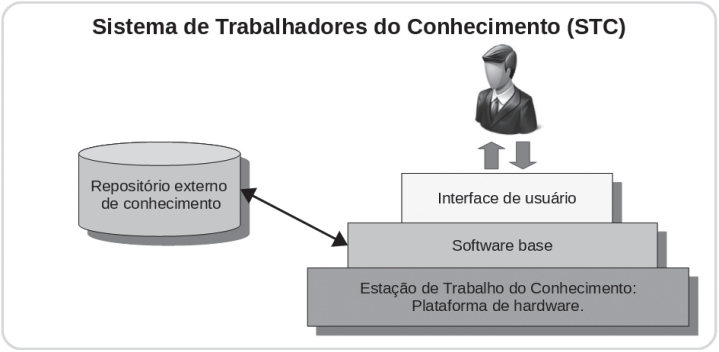
Os sistemas integrados de gestão do conhecimento (SIGC) são empregados para auxiliar as empresas na gestão dos conhecimentos explícitos e tácitos, sendo que os conhecimentos explícitos podem ser entendidos na forma de conhecimentos estruturados, como relatórios, documentos formais e manuais, e conhecimentos não estruturados, ou seja, e-mails, vídeos, fotos, folhetos, conversas e outros. O objetivo dos sistemas integrados de gestão do conhecimento é justamente integrar todos esses conhecimentos de forma a capturá-los, armazená-los e distribuí-los dentro de toda a empresa, permitindo a utilização deles por quem desejar e quando for necessário. Esses tipos de sistemas são compostos por ferramentas de busca de informações; por recursos de armazenamento de dados; por mecanismos de localização de funcionários com conhecimento técnico específico dentro da empresa (rede de conhecimento); por softwares aplicativos que promovem a colaboração entre as pessoas, tais como: serviços de correio eletrônico, programas de mensagens instantâneas, salas de bate-papo, fóruns e groupwares; e por subsistemas de gestão do aprendizado organizacional (vide Figura 4.3) (LAUDON; LAUDON, 2007).

Figura 4.3 | Sistema integrado de gestão do conhecimento

Fonte: elaborada pelo autor.

Os sistemas de trabalhadores do conhecimento (STC), por sua vez, são desenvolvidos para atender áreas do conhecimento específicas de cada trabalhador, auxiliando-os nas suas atividades, aumentando sua produtividade e facilitando a criação de novos conhecimentos organizacionais. A estrutura básica desses sistemas conta com uma estação de trabalho do conhecimento, entendida como uma plataforma de hardware com grande capacidade de computação; um software base que apresenta recursos gráficos, ferramentas de modelagem e simulação, canais de comunicação, gerenciamento de documentos e uma interface de usuário para o trabalhador; e, por fim, acesso a um repositório externo de conhecimento (vide Figura 4.4) (LAUDON; LAUDON, 2007).

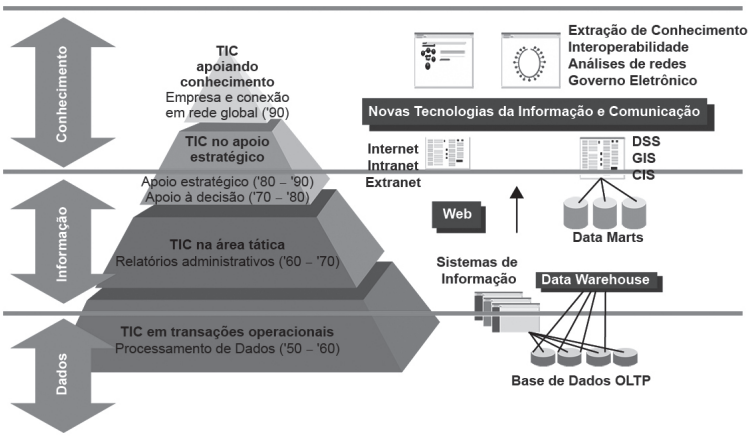
Figura 4.4 | Sistemas de trabalhadores do conhecimento



Fonte: adaptada de Laudon e Laudon (2007).

Considerando tudo que estudamos até aqui, percebemos que a função das tecnologias da informação e comunicações (TICs) é dar suporte à gestão do conhecimento (GC), identificando, desenvolvendo e implantando tecnologias que permitam o compartilhamento e a gestão dos conhecimentos através de ferramentas que propiciem a comunicação organizacional, possibilitando, dessa forma, que as empresas se mantenham competitivas no mercado onde atuam (ROSSETTI; MORALES, 2007). Como base e suporte para todos esses sistemas empregados na gestão do conhecimento nas empresas, são utilizadas várias tecnologias, conforme ilustra a Figura 4.5.

Figura 4.5 | TICs de suporte à GC



Fonte: <http://revista.ibict.br/ciinf/article/view/1191/1362>. Acesso em: 5 set. 2017.

A seguir, compreenda uma breve explanação sobre cada uma dessas tecnologias e mais algumas outras que não aparecem na figura, porém são igualmente importantes.

• **Groupware**: ou software colaborativo, é formado por um conjunto de aplicativos que podem interagir em tempo real, ou não, e que são integrados com a intenção de constituir um ambiente de trabalho cooperativo entre as pessoas envolvidas na atividade da organização e que podem estar dispersas geograficamente. Esse tipo de software permite agilizar a troca de informações entre os colaboradores da organização, possibilitando uma interação muito grande entre eles, gerando um esforço colaborativo mútuo e

alavancando a produtividade de todos os participantes. Aplicativos de correio eletrônico, videoconferências, mensagens instantâneas, wikis, blogs, fóruns e salas de bate-papo são alguns dos softwares que integram um groupware.

• **Internet, intranets e extranets (portais web)**: é o aproveitamento dos recursos de redes e telecomunicações existentes nas organizações que disponibilizam os serviços de páginas web, tanto internas quanto externas às empresas, baseadas nos princípios da restrição de acesso, da comunicação rápida entre os funcionários e a empresa e do compartilhamento de recursos, dados e informações. Esses portais servem, normalmente, como plataforma para os sistemas de informação das organizações, dando total suporte para execução dos processos empresariais, para a produção de conhecimento e para a tomada de decisão.

• **Sistemas especialistas**: são sistemas ou aplicações que tentam reproduzir o conhecimento de um especialista humano, através de inferências sobre a base de conhecimento, com o auxílio de ferramentas de inteligência artificial. Normalmente, são sistemas muito complexos e caros, que resolvem problemas específicos e muito restritos.

Exemplificando

Existem diversos sistemas especialistas no mercado, podemos citar alguns deles e suas áreas de atuação: FOLIO, Administração de Empresas; JUDITH, Advocacia; SOPHIE, Eletrônica; GAMMA, Física Nuclear; e Quick Medical Reference System (QMR), Medicina.

• **Agentes de pesquisa inteligentes (OLAP)**: do inglês *On-Line Analytical Processing*, ou Processo Analítico em Tempo Real, são poderosas ferramentas de busca e exploração de dados em um Data Warehouse, que permitem uma análise posterior dessa massa de dados sob diversos pontos de vista, possibilitando classificar e comparar séries históricas de dados e apoiar processos decisórios.

• **Bases de dados OLTP**: do inglês *On-Line Transaction Processing*, são as bases de dados necessárias para os sistemas de processamento de transações das organizações, mas que estão disponíveis on-line. Em resumo, essas bases dão suporte

à execução das funções operacionais dos negócios das empresas.

- **Data Warehouse**: ou depósito de dados, são grandes bancos de dados estruturados que armazenam os dados relativos às atividades das empresas, normalmente coletados nos sistemas de processamento de transações (SPT) através de ferramentas OLTP e que possibilitam uma futura análise desse grande volume de dados com o auxílio de agentes OLAP.
- **Data Marts**: são conjuntos menores de dados, geralmente extraídos de um Data Warehouse, que passam a constituir subdivisões deste, facilitando a busca e análise de dados específicos de um departamento ou tipo de negócio da empresa, agilizando muito a exploração desses dados e dessas informações.
- **Data Mining**: ou mineração de dados, são tecnologias usadas para mapear padrões, ou associações, ou mudanças, ou tendências, ou relacionamentos entre os dados em grandes bancos de dados, auxiliando nas estratégias das organizações.

Gerenciamento Eletrônico de Documentos (GED): pode ser considerado como o conjunto de tecnologias que auxiliam a organização a gerenciar todos os documentos, via de regra, em formato de arquivos digitais, independentemente de como o documento foi originalmente gerado, ou seja, impresso em papel, ou gravado em vídeo, ou um registro fotográfico ou desenho. O gerenciamento eletrônico de documentos permite que a organização localize, com precisão e rapidez, seus documentos, agilizando seus processos de tomada de decisão e de criação de conhecimento, além de outras várias vantagens operacionais, como o melhor aproveitamento do espaço físico da empresa.

Pesquise mais

Para obter mais informações sobre as tecnologias empregadas na gestão do conhecimento, leia o artigo a seguir:

ROSSETTI, A.; MORALES, A. B. O papel da tecnologia da informação na gestão do conhecimento. **Ciência da Informação**, Brasília, v. 36, n. 1, p. 124-135, jan./abr. 2007. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652007000100009&lng=pt&tlng=pt>. Acesso em: 5 set. 2017.

Para finalizar esta seção, veremos, agora, o papel do e-learning no desenvolvimento dos profissionais de segurança. Por uma questão de nivelamento de conhecimentos, devemos entender essa ferramenta como sendo a modalidade de ensino baseada na independência do aluno em relação ao professor no tempo e no espaço, totalmente fundamentada na internet e no emprego de meios eletrônicos e sistemas de informação para operacionalizar o processo de aprendizagem do estudante, que passa a ser on-line. Atualmente, existe uma tendência muito forte das empresas em adotar o e-learning como meio de ministrar cursos e treinamentos para seus colaboradores, já que esta modalidade de ensino permite rápida obtenção de conhecimento sobre os processos organizacionais, além de padronizar a maneira como os conhecimentos organizacionais são transferidos e disponibilizados para os funcionários. A partir desta linha de raciocínio, o ramo da segurança não poderia ficar de fora, uma vez que tanto as empresas de segurança privada quanto os órgãos de segurança pública estão sempre em busca do aperfeiçoamento de seu pessoal. Nesse cenário, os próprios profissionais da área de segurança acabam buscando seu desenvolvimento profissional, aproveitando-se desta modalidade de ensino, que também pode ser empregada em conjunto com atividades presenciais, as quais exigem uma prática específica, por exemplo, tiro, condução de veículo, manejo de armamento ou equipamento, técnicas de luta e defesa pessoal, dentre outras.

No tocante ao e-learning na segurança pública, a Secretaria Nacional de Segurança Pública do Ministério da Justiça (Senasp) promove, todos os anos, o Ciclo de Capacitação da Rede Nacional de Educação a Distância para Segurança Pública, no qual são oferecidos mais de sessenta cursos para profissionais de polícia civil, polícia militar, policia federal, polícia rodoviária federal, perícia criminal, guarda municipal e outras ocupações ligadas à segurança pública. As inscrições podem ser realizadas através do portal da Rede EaD Senasp, no endereço, disponível em: <http://portal.ead.senasp.gov.br> (acesso em: 5 set. 2017) e são privativas para quem tem vínculo funcional junto aos órgãos de segurança pública, uma vez que a disponibilização dos cursos é fruto de parcerias entre a Senasp, as Secretarias de Segurança Pública dos Estados e as prefeituras dos municípios. Dentre os vários cursos

oferecidos no portal, podemos citar, por exemplo, os cursos de Polícia Comunitária, Uso Diferenciado da Força, Análise Criminal, Atendimento às Mulheres em Situação de Violência, Aplicação do Estatuto da Criança e do Adolescente, além de Libras, Inglês e Espanhol. Os cursos normalmente têm duração aproximada de um mês e carga horária que pode variar de 40h a 60h, constituindo-se em uma excelente oportunidade de crescimento profissional para os agentes de segurança pública. Além dos disponibilizados no Portal Senasp e outros órgãos ligados à Segurança Pública, ainda existem diversos cursos nesta área, oferecidos por instituições de ensino privadas, que vão desde treinamentos e certificações até a especialização e pós-graduação.

Na área de segurança privada também existem várias oportunidades de aperfeiçoamento profissional através de e-learning, com as quais vigilantes, supervisores ou gerentes podem obter conhecimentos e se especializar em diversas áreas, como Gestão de Segurança Privada, Inteligência de Segurança Corporativa, Tecnologia da Informação em Segurança, Segurança em Eventos e outras.

Com isso, caro aluno, chegamos ao final de mais uma seção. Agora, podemos continuar, praticando o que foi estudado, com a situação-problema que será apresentada a seguir. Bons estudos e sucesso na atividade!

Sem medo de errar

Caro aluno, você já formulou sua resposta para a situação-problema desta seção? Aquela em que Mônica pediu ajuda para sua amiga Marilinda sobre a melhor maneira de atualizar os conhecimentos e procedimentos dos vigilantes da sua equipe. Nesse contexto, veremos uma possível solução!

A tarefa de Mônica realmente é desafiadora, pois sua equipe trabalha descentralizada em várias empresas, em diversos municípios, e reuni-la para desenvolver qualquer tipo de treinamento acaba sendo um esforço muito grande e dispendioso. Mas, atualmente, na Era da Informação, existe solução para tudo, sendo esta a sugestão de Marilinda para Mônica, ou seja, realizar um treinamento on-line empregando o conceito de e-learning

que elas haviam aprendido na faculdade. Mônica gostou da sugestão e passou a levantar alguns questionamentos sobre como operacionalizar essa ideia. Assim, vamos ajudá-la a tirar suas dúvidas e a esclarecer alguns pontos sobre essas tecnologias, com base, é claro, naquilo que aprendemos até agora.

Começando com o desenvolvimento de um sistema que permite treinamento por meio de computadores e da internet, isso, na verdade, é uma atividade para os especialistas no assunto, não sendo o caso de Mônica nem da empresa em que ela trabalha. Portanto, o melhor caminho seria utilizar uma ferramenta pronta e existente no mercado, como a plataforma Moodle, desenvolvida para o ensino via internet e completamente flexível, que permite a montagem de qualquer tipo de curso ou treinamento. Esta seria uma boa opção, porém acarretaria em uma certa demanda de trabalho adicional para estruturar a ferramenta e os treinamentos, a um custo baixo. Outra alternativa seria contratar uma empresa especializada em treinamentos on-line para fazer todo o trabalho, permitindo o desenvolvimento dos treinamentos via internet. No entanto, neste caso, os custos seriam elevados e deveriam ser colocados na balança para avaliar sua viabilidade. Visto isso, consideraremos se a empresa, na qual Mônica trabalha, terá estrutura para implementar um sistema dessa natureza. Para isso, é necessário basicamente um bom computador, do tipo servidor e com grande capacidade de processamento e armazenamento, e um link de internet com uma boa velocidade. Além disso, é preciso destacar uma pessoa com conhecimentos avançados em informática para instalar e configurar os softwares e outra para estruturar e montar os treinamentos. Dessa forma, não é necessária uma superestrutura para implementar soluções como esta, o ponto crítico destas iniciativas recai justamente na dedicação e no conhecimento das pessoas que construirão o ambiente de e-learning.

Agora, orientaremos Mônica em relação à sua expectativa sobre o que poderia passar para seus funcionários via e-learning. Como estudamos, nesta seção, a modalidade de ensino e-learning pode ser tranquilamente empregada nas empresas de segurança privada, não sendo somente indicada para as atividades que exijam uma prática específica, como tiro, condução de veículo, manejo de armamento ou equipamento, técnicas de luta e defesa pessoal.

Mas como a necessidade de Mônica é atualizar os conhecimentos e procedimentos dos vigilantes integrantes de sua equipe, muito provavelmente não terá dificuldade para fazê-lo totalmente à distância. Concluindo as dúvidas de Mônica, podemos afirmar que os vigilantes realmente aprenderão à distância, através da modalidade de ensino e-learning, pois essa tecnologia, além de permitir uma rápida obtenção de conhecimento sobre os processos organizacionais por parte dos colaboradores, proporciona ainda uma padronização da maneira como os conhecimentos organizacionais são transferidos e disponibilizados para os funcionários. Dessa forma, os resultados no processo de ensino-aprendizagem, através do e-learning, vêm sendo bastante positivos. Assim, podemos considerar que Mônica poderá desenvolver treinamentos para seus vigilantes empregando essa ferramenta, como forma de garantir que eles sejam treinados por meio de um sistema de informação, dentro do contexto de gestão do conhecimento na empresa em que ela trabalha.

Além desta solução, caro aluno, podem existir também outras formas de responder à essa situação-problema, mas o importante é expressar essas mesmas ideias em sintonia com os conhecimentos que foram adquiridos durante o desenvolvimento da disciplina e, particularmente, desta Seção 4.2.

Avançando na prática

Trabalhando para não faltar conhecimento

Descrição da situação-problema

Caro aluno, vamos aperfeiçoar nossa prática em mais uma situação-problema? Imaginemos a situação do nosso personagem José Jacinto, que trabalha em uma escola de formação de vigilantes que, além desse curso, também oferece treinamentos específicos em parceria com algumas empresas de segurança. A rotina diária de José é organizar as turmas e elaborar um cronograma para o curso, porém ele tem plena consciência que no curso formal os alunos obterão somente o conhecimento explícito sobre a matéria ou o assunto em questão. Considerando isso, como o curso poderia implementar uma forma de agregar algum conhecimento tácito a ser passado para os

alunos? Tendo em vista que no ramo da segurança a experiência e vivência na atividade conta muito e isso seria um grande diferencial para a escola.

O que você sugere? Como a escola de formação de vigilantes pode passar algum conhecimento tácito para seus discentes? Para tanto, faça uma proposta baseada no seu estudo dos assuntos desta seção e no seu próprio conhecimento sobre este ramo de atividade. Boa sorte e siga em frente!

Resolução da situação-problema

Caro aluno, você já aprendeu que o conhecimento tácito é aquele altamente pessoal e difícil de ser formalizado, geralmente adquirido pelas pessoas ao longo das suas vidas e de suas experiências profissionais, sendo este o tipo de conhecimento que almejamos aos cursos da escola. Na verdade, não existe uma maneira estabelecida de fazer isto, mas com certeza podemos idealizar algumas baseadas no nosso conhecimento.

Uma sugestão seria promover a interação dos alunos com profissionais experientes, os quais, em determinadas aulas, poderiam relatar suas experiências e sua visão de como agir em determinadas situações, trazendo um conhecimento além daqueles descritos nos livros e nas notas de aula.

Outra maneira de atingir esse objetivo poderia ser através da utilização de tecnologias de groupware, com as quais os alunos poderiam trocar experiências com profissionais selecionados via internet e, dentro de uma relação colaborativa, obter os conhecimentos informais daqueles que apresentam grande vivência no ramo.

Além disso, outra forma seria colocar, à disposição do aluno, via portal na internet, uma página de consulta com relatos de profissionais do ramo de segurança sobre situações críticas que se defrontaram durante suas carreiras e como fizeram para enfrentá-las obtendo sucesso em suas ações.

A partir disso, caro aluno, temos certeza de que ainda existem muitas outras formas de se atingir esse objetivo, mas deixamos a seu critério descobri-las.

Faça valer a pena

1. Atualmente, as empresas vêm apostando no conhecimento como base única e permanente de obter sucesso e vantagem competitiva no mercado, tanto que a informação e o conhecimento acabaram por se tornar os bens mais valiosos das organizações, chamados de ativos intangíveis. Para acompanhar essa nova era e se manter competitiva no mercado, as companhias estão empregando largamente os sistemas de informação e a gestão do conhecimento como formas de promover a rápida integração dos conhecimentos das pessoas com os processos organizacionais, a fim de possibilitar a melhoria da qualidade de seus produtos e serviços.

Considerando o exposto no texto anterior sobre a relação entre sistemas de informação e gestão do conhecimento, assinale a única alternativa que apresenta um sistema que teve origem nessa integração.

a) Sistema integrado de gestão do conhecimento.

b) Sistema de informações gerenciais.

c) Sistema de controle de acesso.

d) Sistema de inteligência artificial.

e) Sistema de informação de conhecimento.

2. Um sistema de gestão do conhecimento em uma empresa envolve desde os funcionários que lidam com os dados brutos até aqueles que manipulam o conhecimento. Isto significa que as secretárias, assistentes e auxiliares normalmente fazem a entrada de dados no sistema, no nível operacional da empresa, e, de modo geral, utilizam sistemas de processamento de transações (SPT). A partir desses dados, entram em cena os profissionais do conhecimento, que podem ser engenheiros, arquitetos, advogados, contadores e pesquisadores, dentre outros, que terão o encargo de processar novos conhecimentos dentro da organização.

O processo, descrito no texto anterior, evidencia que uma empresa utiliza um sistema de gestão do conhecimento para:

a) Produzir conhecimento tácito.

b) Produzir novos dados e informações para seus colaboradores e parceiros.

c) Criar, armazenar, compartilhar e utilizar o conhecimento.

d) Resguardar o conhecimento organizacional da espionagem empresarial.

e) Obter conhecimento experimental.

3. A função das tecnologias da informação e comunicações (TICs) é dar suporte à gestão do conhecimento (GC), identificando, desenvolvendo e implantando tecnologias que permitam o compartilhamento e a gestão dos conhecimentos através de ferramentas que propiciem a comunicação organizacional, possibilitando, dessa forma, que as empresas se mantenham competitivas no mercado onde atuam (ROSSETTI; MORALES, 2007).

Considerando as tecnologias que dão suporte à gestão do conhecimento, analise as afirmativas a seguir:

I. Um groupware é um sistema que tenta reproduzir o conhecimento de um especialista humano.

II. O Data Warehouse é um grande banco de dados estruturados que armazena os dados relativos às atividades de uma empresa, normalmente coletados nos sistemas de processamento de transações (SPT).

III. Um agente de pesquisa inteligente (OLAP) é uma poderosa ferramenta de busca e exploração de dados em um Data Warehouse.

IV. Um Data Mining é um subconjunto de dados extraídos de um Data Warehouse.

Assinale a alternativa que contém somente as afirmativas corretas.

a) I e II.

b) I, II e IV.

c) II e IV.

d) II e III.

e) II, III e IV.

Seção 4.3

Gestão do conhecimento nas organizações e na segurança pública e privada

Diálogo aberto

Caro aluno, chegamos à última situação-problema da disciplina. Para tanto, relembraremos o contexto de aprendizagem de nossa unidade, que se trata de Marilinda Fernandes, que trabalhava na Guardian Segurança Patrimonial e tinha sido aprovada no concurso de escrivão da polícia civil do Estado de São Paulo. Dando continuidade a esse contexto, Marilinda assumiu o cargo, enfrentando os desafios de assimilar todos os conhecimentos necessários ao desempenho de sua nova função. Como tem experiência na área de segurança privada, ela estava orientando Mônica Aparecida, sua amiga de faculdade, com dicas para desenvolver o pessoal da segurança privada por meio de cursos e treinamentos à distância.

Procurando aproveitar todo o cabedal de conhecimentos que Marilinda tinha na segurança privada, Mônica solicitou auxílio em outros problemas, uma vez que era inspetora de segurança e percebia algumas situações que poderiam ser aperfeiçoadas em sua equipe de vigilantes. Uma das grandes falhas encontradas por Mônica estava relacionada à passagem das funções, durante o término de turno de trabalho de cada posto em que os vigilantes prestavam seu serviço de vigilância patrimonial, e às ocorrências acontecidas naquele período, transmitidas sem muita formalidade, isto é, sem que houvesse uma padronização. De modo geral, cada vigilante fazia a passagem da maneira que desejava. Nesse cenário, outro empecilho ganhou destaque, isto é, a cada semestre, no mínimo, um dos subordinados de Mônica saía da empresa, tendo ela de contratar um novo profissional para sua equipe, fato este que demandava treinamentos e orientações constantes.

A partir do que foi exposto, Você, na posição de Marilinda, deve apresentar algumas oportunidades de melhoria para que Mônica possa solucionar seus problemas. Para tanto, oriente-se pelos

seguintes questionamentos: quais são os principais documentos de segurança que os vigilantes de uma equipe de segurança patrimonial devem conhecer e manipular? Existe algum relatório de segurança, produto de uma compilação de dados, que possa ser utilizado para aperfeiçoar os sistemas de segurança? Por que profissionais da segurança privada deixam seus empregos? Como minimizar, nesta área, essa questão do *turnover*?

Caro aluno, para resolver esta situação-problema, você deverá ter conhecimento sobre o emprego dos documentos de segurança privada e dos relatórios de segurança, além de ter compreendido a influência do *turnover* e do capital intelectual na segurança privada.

Nesse contexto, vamos solucionar mais um desafio?

Não pode faltar

Caro aluno, prosseguiremos com nossos estudos, partindo para a parte final desta disciplina, explorando a gestão do conhecimento nas organizações e na segurança pública e privada. Antes de abordarmos o assunto propriamente dito, devemos, primeiramente, entender a importância da documentação para a atividade de segurança, no sentido de permitir que tudo seja devidamente registrado e relatado e que estes registros possam ser arquivados e consultados, constituindo-se como fontes de consulta para estudos de melhoria das medidas de segurança ou provas documentais da ocorrência de fatos relativos à essa área.

Dessa forma, conheceremos os documentos de segurança privada, os quais, segundo Soares (2008), são basicamente:

- **Livro diário**: documento no qual deverão ser realizadas anotações relativas à rotina diária da segurança, tais como situação do material de segurança, pessoal empregado na segurança, horários da realização de atividades específicas, como rondas e fiscalizações, dentre outras informações e dados necessários para manter um registro formal sobre a atividade de segurança desenvolvida em um determinado dia.

- **Registro de ocorrência**: este documento tem a finalidade de registrar eventos e circunstâncias que, de alguma forma, comprometeram a atividade de segurança em determinado

momento, como uma tentativa de violação de um perímetro monitorado, ou até mesmo focos de incêndio. Este Registro de ocorrências é o documento ideal para o registro daqueles fatos que ocorrem fora da normalidade.

- **Arquivo de correspondências**: também denominado de livro registro de correspondências, é o documento no qual são registradas as entradas e saídas de todo o tipo de correspondências e encomendas recebidas pelo pessoal de segurança, procurando-se manter informações sobre datas e pessoas envolvidas nesta atividade, inclusive, com as respectivas assinaturas ou rubricas, tudo com a finalidade de se manter um histórico sobre o trâmite desses volumes, permitindo que se possa fazer um rastreamento futuro, se for o caso.

- **Planejamentos**: são documentos mais complexos, que estabelecem, segundo Brasiliano e Blanco (2003), um conjunto de ações e providências a serem adotadas pela segurança para evitar a ocorrência de situações que coloquem em risco as pessoas e o patrimônio que se deseja preservar. Os autores ainda apontam que, em linhas gerais, um planejamento de segurança, independentemente de ser operacional, tático, técnico ou estratégico, deve estabelecer objetivos e metas; relacionar os meios a serem empregados na segurança, tanto pessoal quanto material, e equipamentos; e prever mecanismos que possibilitem verificar o desempenho da segurança.

- **Relatórios**: são documentos destinados a apresentar descrições detalhadas sobre fatos, ocorrências ou um aspecto específico, geralmente, muito relevantes em relação à atividade de segurança. Estudaremos, mais adiante, os relatórios de segurança.

Pesquise mais

Para conhecer melhor os documentos de segurança, leia o seguinte texto:

SOARES, P. L. **Segurança Patrimonial**. São Paulo: Sicurezza, 2008. 65 p.

Além disso, leia o texto a seguir:

LIVRO de ocorrências: qual a sua importância? Para que serve? Disponível em: <http://segurancaprivadadobrasil.blogspot.com.br/2010/09/livro-de-ocorrencias-qual-sua.html>. Acesso em: 5 set. 2017.

Cada um dos documentos que descrevemos anteriormente deve seguir alguns princípios de elaboração e ter algumas características fundamentais que caracterizam um certo padrão técnico de produção de documentos de segurança (vide Figura 4.6). De acordo com Soares (2008), os documentos de segurança devem apresentar as seguintes particularidades:

• **Redação objetiva**: o documento de segurança deve ser redigido de forma clara, precisa e concisa, usando uma linguagem simples e direta para que possa ser facilmente entendido por qualquer pessoa. Portanto, deve-se evitar o emprego de palavras rebuscadas, expressões idiomáticas complexas ou vocábulos que sugiram duplo sentido ou permitam interpretações equivocadas sobre o conteúdo que se deseja expressar.

• **Classificação sigilosa**: normalmente, um documento de segurança requer um certo grau de controle em relação à sua divulgação, não sendo, portanto, franqueado a pessoas não credenciadas para acessar seu conteúdo. Por isso, sua classificação sigilosa deve estar bem clara e visível em todas as páginas.

• **Numeração de páginas**: todo documento, com um certo grau de relevância, deve ter medidas para evitar que sua integridade seja violada, sendo a numeração de páginas uma delas. Esta deve ser feita de forma que expresse a posição de uma página em relação ao documento todo, no formato *nº da página/ nº total de páginas*. Por exemplo, se estivermos lendo a página 3/27, significa que o documento tem 27 páginas e estamos na página 3. De forma simples, a numeração permite ao leitor identificar a falta de alguma página.

• **Numeração de documento**: assim como a numeração das páginas apresenta certa importância e finalidade, a numeração dos documentos também. Por isso, eles devem ser numerados ordenadamente, pois se um documento estiver faltando será facilmente percebido através da descontinuidade na numeração. Da mesma forma que a numeração total de páginas, os documentos com números permitem: rastreabilidade, controle da produção e de seu arquivamento.

• **Rubrica, assinatura e carimbo**: um documento de segurança deve ser rubricado e carimbado em todas as páginas pela pessoa que o elaborou, devendo a última página conter a assinatura desta

pessoa, junto com sua qualificação, se possível. Tal atitude visa garantir a autenticidade do documento.

• **Data**: esta é uma informação fundamental para um documento de segurança, que deve sempre conter a data e, se possível, até a hora da sua elaboração ou divulgação.

• **Assunto**: esta é uma informação que deve estar muito clara em um documento de segurança e ser apresentada logo na primeira página ou no início do documento.

• **Origem**: também deve ficar bem evidente em um documento de segurança, expressando a pessoa ou o setor responsável pela autoria ou divulgação do documento.

• **Difusão**: aqui se deve estabelecer quem terá acesso ao documento de segurança, ou seja, a quais pessoas ele se destina ou deverão tomar conhecimento dele.

• **Anexos**: um documento de segurança deve conter uma referência explícita a outros documentos ou peças que o compõem ou o complementam, em termos de enumeração de anexos. Veja, na Figura 4.6, a seguir, um exemplo disso.

Figura 4.6 | Documento de segurança

CONFIDENCIAL

World Segurança S/A
Condomínio Residencial Vale Verde

RELATÓRIO DE OCORRÊNCIA Nº 017/2017

DATA: 20 de julho de 2017
ASSUNTO: Tentativa de Invasão do Condomínio
ORIGEM: Supervisor de Segurança
DIFUSÃO: Gerência de Segurança
ANEXOS: Fotografias e vídeos das câmeras de segurança

[Nestas linhas deverá ser redigído o conteúdo do documento em forma de texto com redação objetiva.]

Assinatura e identificação do autor

CONFIDENCIAL

Página 1/12

Fonte: adaptada de Soares (2008).

Agora que já conhecemos os documentos de segurança privada e como eles devem ser elaborados, nos aprofundaremos mais detalhadamente nos relatórios de segurança, procurando identificar a composição e a importância destes documentos dentro do contexto da atividade de segurança. Como apresentado anteriormente, relatórios são documentos destinados a apresentar descrições detalhadas sobre fatos relevantes em relação à atividade de segurança, que devem seguir os padrões de elaboração dos documentos de segurança. Nesse contexto, relatórios de segurança são excelentes ferramentas de controle que permitem o monitoramento da atividade de segurança, a fim de verificar se o que foi planejado está sendo cumprido ou se está ocorrendo algum desvio daquilo que deveria estar sendo executado. Assim sendo, eles podem ser elaborados a partir de diversas finalidades, dependendo dos objetivos planejados para a segurança ou da ocorrência de eventos que impeçam ou invalidem a consecução desses objetivos. Para Soares (2008), esses relatórios podem ser classificados da seguinte forma:

- Relatórios periódicos.
- Relatórios de situação.
- Relatórios de ocorrência.

Assimile

Os documentos de segurança privada e os relatórios de segurança cumprem uma dupla finalidade neste ramo de atividade, seja para registrar e comunicar fatos e circunstâncias relativas à segurança, seja para manter um banco de dados de informações sobre os procedimentos de segurança que possibilitam o estudo e a produção de conhecimento sobre a prática de segurança, gerando melhorias e inovações nos produtos e serviços oferecidos pelas empresas dessa área.

São documentos utilizados na segurança privada, uma vez que a segurança pública (forças armadas, polícias e guardas municipais), geralmente, normatiza e padroniza os tipos e modelos de documentos.

Vejamos, dessa forma, uma breve explanação sobre cada um desses relatórios, apresentando suas particularidades e informações básicas.

Os **relatórios periódicos** são uma forma de comunicação periódica e atualizada de informações sobre a atividade de segurança que permitem avaliar a execução das medidas estabelecidas no planejamento de segurança e que devem ser elaborados de acordo com uma rotina de regularidade, que pode ser diária, semanal, quinzenal, mensal, bimestral, trimestral, semestral, anual, bienal e assim por diante. Por serem relatórios elaborados sob uma rotina de periodicidade, não dependem da ocorrência de um fato que motive sua produção, mas sim da execução diária e permanente das rotinas de segurança.

Agora, vejamos os **relatórios de situação**, documentos de segurança que têm por finalidade reportar uma situação específica em relação ao trabalho da segurança, requerendo, normalmente, alguma providência ou comunicação peculiar por parte da chefia da segurança e que não pode aguardar, por exemplo, a periodicidade de um relatório diário.

Por último, caro aluno, falaremos dos **relatórios de ocorrência**, isto é, documentos muito particulares da segurança, que, via de regra, servem para registrar a ocorrência de acontecimentos que abalaram, de forma significativa, a atividade de segurança, colocando em risco os ativos sob proteção e até mesmo comprometendo a rotina das organizações vítimas dos acontecimentos. Geralmente, esse tipo de relatório envolve a descrição de roubos, assaltos, invasões, incêndios ou qualquer outro tipo de ataque ou revés sofrido por uma companhia. Na Seção 1, da Unidade 1, identificamos exatamente os dados necessários para a elaboração de um relatório de ocorrência exemplar. Você se lembra?

Exemplificando

Você pode obter um exemplo de Relatório de Ocorrência, acessando o endereço: <http://segurancaprivadadobrasil.blogspot.com.br/2015/01/modelo-de-relatorio-de-ocorrencia.html>. Acesso em: 19 jul. 2017.

A partir deste momento, prosseguiremos nossos estudos conhecendo os documentos de segurança pública. Assim como na segurança privada, os documentos também têm dupla finalidade na segurança pública, conforme já visto anteriormente.

Embora os documentos utilizados na segurança pública sejam praticamente os mesmos empregados na privada, a segurança pública, geralmente, normatiza e padroniza os tipos e modelos de documentos. Nesse contexto, destacaremos três documentos, os quais, além de serem os mais utilizados na segurança pública, são os mais importantes para o desenvolvimento desta atividade tão significativa para a sociedade. São eles: os boletins de ocorrência (B.O.), os relatórios e os planejamentos.

Como já sabemos e estudamos na Seção 1.1, um **boletim de ocorrência** é um documento muito importante porque contém todas as informações sobre a ocorrência de um crime, que comprometeu a atividade de segurança pública e que poderá gerar uma investigação policial ou um processo no judiciário. Na verdade, os dados contidos no B.O. passam a ter um valor significativo para os órgãos de segurança pública porque, além de dar origem a procedimentos legais de combate ao crime, somados a outras fontes de dados, servem como base de informações para a elaboração de documentos que contêm estudos sobre a criminalidade e que permitirão a estruturação de políticas públicas de segurança, objetivando uma melhor articulação dos órgãos de segurança pública para o combate ao crime e a manutenção dessa segurança.

Dando continuidade aos estudos, vejamos, nesse sentido, os **relatórios de segurança pública**, excelentes ferramentas para o monitoramento da atividade de segurança, justamente porque contêm informações levantadas a partir de um conjunto de dados sobre as situações que comprometerem a segurança; e já que a principal serventia da informação para a segurança pública é exatamente permitir o conhecimento sobre a criminalidade, fundamentando a formulação de estratégias e ações para combater o crime e manter a sociedade em segurança, como vimos na Seção 3.3, possamos talvez supor que os documentos mais importantes para a segurança pública sejam, de fato, os relatórios. Em uma busca despretensiosa pela web, conseguiremos rapidamente reunir uma infinidade de relatórios sobre as mais diversas situações que envolvem a segurança pública. Esses relatórios abordam temas, como violência nas escolas, assaltos à mão armada, latrocínios, tráfico de drogas, roubo de cargas, violência contra a mulher, sequestros, roubo de veículos e outros assuntos que afligem a

segurança pública em nosso país. Essa abundância de relatórios e estudos constitui a mais preciosa fonte de informação que servirá de apoio para que os tomadores de decisão possam determinar os caminhos a serem seguidos pelos órgãos de segurança pública no combate à criminalidade e que irão compor os planejamentos de segurança pública.

Exemplificando

Para exemplificar a quantidade e diversidade de relatórios que se pode encontrar em uma rápida busca pela web e que abordam temas de interesse para quem se dedica ao estudo da segurança pública, temos o Observatório de Segurança Pública da Unesp, um espaço na internet que procura disponibilizar informações sobre segurança pública no âmbito do Estado de São Paulo.

Disponível em: <http://www.observatoriodeseguranca.org/relatorios>. Acesso em: 5 set. 2017.

Encerrando a questão dos documentos de segurança pública, faremos, agora, uma explanação sobre os **planejamentos de segurança pública**. Normalmente, no Brasil, esses planejamentos são encargos das Secretarias de Segurança Pública dos estados e municípios, que os elaboram com base na situação em que se apresenta a segurança pública, geralmente descrita em algum relatório. Nesses planos, são definidos objetivos a serem alcançados, a articulação dos órgãos de segurança pública e as ações de combate ao crime e à violência a serem desenvolvidas. No âmbito da União foi lançado pelo Ministério da Justiça, em 2017, o Plano Nacional de Segurança em uma tentativa de integrar o governo federal, estados, municípios e sociedade nas ações de Segurança Pública.

Pesquise mais

Para conhecer mais sobre o Plano Nacional de Segurança, seus objetivos, suas ações, seus cenários e suas metas, acesse o link a seguir.

Disponível em: <http://www.justica.gov.br/noticias/plano-nacional-de-seguranca-preve-integracao-entre-poder-publico-e-sociedade>. Acesso em: 5 set. 2017.

Para finalizar o aprendizado desta seção, descreveremos, neste momento, o significado de *turnover* e do capital intelectual na segurança privada. Como já estudamos na Seção 4.1, o capital intelectual das empresas é formado pelo conjunto de conhecimentos e habilidades de seus colaboradores, além de outros componentes imateriais, que têm a capacidade de aumentar o valor organizacional, proporcionando vantagem competitiva para a organização. Grande parte do capital intelectual de uma empresa de segurança privada, portanto, está depositado em seus vigilantes, inspetores, supervisores e gerentes de segurança, e deve ser administrado com toda prudência, principalmente aqueles poucos funcionários que apresentam o conhecimento que compõe a base das expertises da companhia.

No Brasil, o mercado de segurança privada vem crescendo significativamente com o passar dos anos e, nesse movimento, há tanto o surgimento de novas empresas no mercado quanto o desaparecimento de outras, fato este que provoca uma movimentação intensa de entrada e saída entre os funcionários. Esta rotatividade de colaboradores também é chamada de *turnover* e vem se constituindo como um fator crítico de sucesso para as empresas de segurança privada no Brasil. Neste país, o *turnover* de mão de obra nas organizações privadas de segurança é alto, o que prejudica a qualidade dos produtos e dos serviços oferecidos pelas companhias deste ramo de atividade. Nesse cenário, algumas empresas vêm enfrentando o problema, oferecendo vantagens aos seus funcionários, como plano de saúde, assistência odontológica e até previdência privada, com a finalidade de FIDELIZAR o colaborador. O ideal seria manter uma certa estabilidade no quadro de vigilantes e colaboradores, buscando uma situação de manutenção dos funcionários e, consequentemente, um índice de rotatividade baixo, o que poderia ser traduzido em maior confiança e credibilidade por parte dos clientes. Mas, para isso, as organizações devem apresentar motivos de ordem financeira, como um nível salarial compatível, com mais benefícios, e outros aspectos motivantes, como um bom ambiente de trabalho, disponibilidade de materiais e instalações adequadas e, até mesmo, perspectivas de promoções e carreiras.

O *turnover* de profissionais de segurança privada é um ponto sensível que pode deixar o cliente exposto e inseguro, uma vez

que, com sua saída, esse profissional leva consigo todo um conhecimento sobre a segurança do cliente. Um alto índice de rotatividade, ou *turnover* elevado, acarreta em um grande revezamento de vigilantes, fato este que afeta as empresas de segurança, os clientes e os próprios funcionários. Os altos índices de rotatividade dos vigilantes das empresas de segurança privada tanto comprometem a qualidade dos produtos e serviços oferecidos pelas empresas quanto elevam significativamente os custos com rescisões de contratos de trabalho, recrutamento e preparação de novos vigilantes (CHRISTENSEN, 1996). É uma opinião comum para as empresas de segurança privada e para os clientes que um *turnover* elevado é prejudicial à segurança e deve ser evitado. Essa rotatividade é entendida ainda pelos clientes como um fator que depõe negativamente para a qualidade dos serviços prestados, uma vez que a alternância de vigilantes produz uma sensação de insatisfação e insegurança nas pessoas (CHRISTENSEN, 1996).

De acordo com Christensen (1996), os fatores que mais contribuíram para o alto índice de rotatividade dos vigilantes, na época da realização de sua pesquisa, foram as condições ruins de trabalho no posto de vigilância; a natureza desgastante das tarefas do vigilante; a grande quantidade de profissionais nos quadros das empresas, gerando conflitos de relacionamento; a má qualidade e as condições das refeições oferecidas aos vigilantes; a distância do domicílio do profissional para o local de trabalho; e o tratamento ríspido dispensado pelos supervisores aos vigilantes. Christensen (1996) também aponta que, existindo múltiplas causas para o elevado *turnover* de vigilantes, torna-se necessário a adoção de diversas ações para mitigar este fenômeno, sendo este o grande desafio a ser enfrentado pelas empresas de segurança privada na busca pela qualidade de seus serviços e vantagem competitiva.

Reflita

Esse problema do *turnover* de vigilantes é, realmente, tão sério? As empresas de segurança privada estão mesmo preocupadas com isso? Existem, de fato, múltiplos fatores para essa rotatividade de vigilantes?

Sendo assim, terminamos mais uma unidade de ensino, finalizando, com ela, a aprendizagem na disciplina de Sistemas de Informação em Segurança. Esperamos que você tenha aproveitado bastante esta oportunidade para obter os conhecimentos necessários à sua preparação técnico-profissional e que, com todos esses saberes, você consiga atingir seus objetivos profissionais e suas aspirações individuais.

Sem medo de errar

Partiremos, agora, para a solução da nossa situação-problema, na qual Mônica, aproveitando-se dos conhecimentos que Marilinda tinha em segurança privada, precisa resolver os problemas de documentação de segurança e rotatividade de vigilantes que estava enfrentando na sua função de inspetora de segurança.

Nesse sentido, poderemos auxiliar Mônica na questão da padronização da transmissão das ocorrências acontecidas por ocasião do término de turno de trabalho dos vigilantes, recordando, primeiramente, os principais documentos de segurança que os vigilantes de uma equipe de segurança patrimonial devem conhecer e manipular, isto é: o livro diário, o registro de ocorrência, o arquivo de correspondência, os planejamentos e os relatórios. Sendo assim, Mônica deveria orientar e treinar os vigilantes de sua equipe a preencherem, corretamente, o documento para a ocasião, qual seja, um registro ou um relatório de ocorrência. Ela pode também passar a adotar a elaboração de um relatório diário ou de situação, visando obter os dados e as informações necessários para aperfeiçoar o sistema de segurança e combater, definitivamente, essas práticas inadequadas em sua equipe.

Já na questão da rotatividade de vigilantes, Mônica deveria, em um primeiro momento, entender que as principais causas para os vigilantes deixarem seus empregos, segundo Christensen (1996), são as condições ruins de trabalho no posto de vigilância; a natureza desgastante das tarefas do vigilante; a grande quantidade de profissionais nos quadros das empresas, gerando conflitos de relacionamento; a má qualidade e as condições das refeições oferecidas aos vigilantes; a distância do domicílio do profissional para o local de trabalho; e o tratamento ríspido dispensado pelos

supervisores aos vigilantes. A partir daí ela deveria elaborar múltiplas ações para eliminar ou atenuar essas causas, que, por ventura, existam em seu ambiente de trabalho.

Normalmente, este é um grande desafio para as empresas de segurança privada, no entanto, algumas delas têm obtido sucesso na redução do *turnover* de vigilantes ao oferecer vantagens extras aos funcionários, tais como transporte, assistência médica e odontológica e até planos de previdência privada. Se Mônica apresentasse uma proposta com esse conteúdo para a diretoria da empresa, ela conseguiria, dessa forma, resolver o problema de *turnover* de vigilantes, reduzindo a demanda por treinamentos e orientações e melhorando a qualidade dos serviços prestados pela empresa em que trabalha.

Avançando na prática

Redigindo o documento certo: uma prática imprescindível

Descrição da situação-problema

Vamos, agora, resolver mais uma situação-problema?

Para tanto, ajudaremos, neste momento, Renata Rizatto, uma inspetora de segurança da empresa SPI Segurança Ltda, que trabalha no Condomínio Residencial Floresta, na região metropolitana de Belo Horizonte, e que, no dia 24 de maio de 2017, por volta das 8h30, atendeu a uma ocorrência no interior do condomínio, na qual o alarme da casa nº 84 havia sido disparado depois de o sr. Antônio, jardineiro, ter entrado no imóvel.

Essa situação aconteceu da seguinte forma: os moradores foram fazer uma pequena viagem e, como já era de costume, deixaram combinado com o jardineiro para ele ir cortar a grama enquanto estivessem fora, porém, desta vez, os donos da casa esqueceram de desligar o sistema de alarme, causando todo o mal-entendido e um grande reboliço no residencial. Para agravar a situação, o alarme só foi ser desarmado quase uma hora depois, após contato telefônico com os proprietários do imóvel.

A partir disso, caro aluno, elabore o documento de segurança adequado para esta situação, exercendo a função da inspetora

Renata. Não se esqueça de seguir todas as características importantes, aprendidas nesta seção.

Mãos à obra e boa sorte!

Resolução da situação-problema

Para solucionar a situação proposta, precisamos esclarecer, primeiramente, que o documento mais adequado, neste acontecimento, é o registro de ocorrência, por se tratar de um evento que impactou, de alguma forma, a segurança do condomínio, na hora apresentada, do dia 24 de maio de 2017. Dessa forma, o documento poderia ficar da seguinte maneira:

RESERVADO

SPI Segurança Ltda

Condomínio Residencial Floresta

REGISTRO DE OCORRÊNCIA Nº 57/2017

DATA: 24 de maio de 2017.

ASSUNTO: Alarme disparado na casa nº 84.

ORIGEM: Inspetor de segurança.

DIFUSÃO: Gerência de segurança.

ANEXOS: Não é o caso.

Por volta das 8h30 da manhã, o alarme da casa nº 80 disparou, após a entrada do sr. Antônio, jardineiro, que havia combinado com os proprietários de cortar a grama enquanto eles estivessem fora do imóvel. Tal fato ocorreu devido ao esquecimento do dono da casa de desligar o alarme da residência após sua saída. Com essa situação, houve certo transtorno entre os moradores, mas tudo se resolveu quase uma hora depois, após contato telefônico com o proprietário do imóvel, que providenciou o desligamento do alarme e a rotina do residencial voltou ao normal.

RESERVADO

Página 1/1

Faça valer a pena

1. Um documento de segurança privada deve ter algumas características que o diferenciam dos demais documentos comuns. Um exemplo disso é que, em sua formatação, deve aparecer, logo na primeira página, informações como o(a) _____, que deve estar muito claro no documento; o(a) _____, que expressa a pessoa ou o setor responsável pela autoria ou divulgação do documento; e o(a) _____, na qual se deve estabelecer quem terá acesso ao documento de segurança.

A partir da frase anterior, assinale a alternativa que contém as palavras adequadas às lacunas.

a) assunto – difusão – origem.

b) numeração – assunto – difusão.

c) assunto – data – numeração.

d) data – assunto – classificação sigilosa.

e) assunto – origem – difusão.

2. Os relatórios de segurança são documentos largamente empregados na rotina das atividades de segurança, seja pública ou privada. Sempre que é necessário fazer o registro de uma situação específica em relação ao trabalho da segurança e que foge à rotina de normalidade da atividade, elabora-se um relatório de segurança.

A partir do texto apresentado anteriormente, pode-se afirmar que se trata de um relatório de segurança classificado como:

a) Relatório de situação.

b) Relatório semanal.

c) Relatório de ocorrência.

d) Relatório especial.

e) Relatório periódico.

3. O capital intelectual das empresas de segurança privada é formado pelo conjunto de conhecimentos e habilidades de seus colaboradores, além de outros componentes imateriais, e tem a capacidade de aumentar o valor organizacional, proporcionando vantagem competitiva para a empresa. Por isso, deve ser administrado com toda prudência, principalmente aqueles poucos funcionários que têm o conhecimento que compõe a base das expertises da organização.

Com base no texto anterior, assinale a alternativa a seguir que melhor identifica a composição do capital intelectual de uma empresa de segurança privada.

a) Os funcionários de maior valor para o capital intelectual de uma empresa de segurança privada são, de fato, os administrativos, uma vez que eles controlam toda a empresa.

b) As viaturas, os equipamentos, as armas e os sinalizadores são componentes imateriais do capital intelectual das empresas de segurança privada.

c) Grande parte do capital intelectual de uma empresa de segurança privada está depositado em seus vigilantes, inspetores, supervisores e gerentes de segurança.

d) Os vigilantes são funcionários do nível operacional da segurança privada, não sendo, portanto, componentes do capital intelectual das empresas.

e) Os dispositivos empregados no controle de acesso, monitoramento de perímetro e rastreamento de veículos são exemplos de componentes do capital intelectual que proporcionam vantagem competitiva para as empresas de segurança privada.

Referências

BRASILIANO, A. C. R.; BLANCO, L. **Manual de planejamento tático e técnico em segurança empresarial**. São Paulo: Sicurezza, 2003. 174 p.

CHRISTENSEN, E. M. **Rotatividade dos vigilantes das empresas especializadas**: Causas e Consequências. 1996. 132 f. Dissertação (Mestrado) - Curso de MBA, Escola de Administração de Empresas, Fundação Getúlio Vargas, São Paulo. 1996. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/5567/1199800123.pdf>. Acesso em: 5 set. 2017.

FRANCO, D. H.; RODRIGUES, E. de A.; CASELA, M. M. **Tecnologias e Ferramentas de Gestão**. Campinas: Alínea, 2013. 361 p.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informação Gerencial.** 7. ed. Tradução de Thelma Guimarães; Revisão técnica de Belmiro N. João. São Paulo: Pearson Prentice Hall, 2007. 452 p.

TAKEUCHI, H.; NONAKA, I. **Gestão do Conhecimento**. Porto Alegre: Bookman, 2008. 320 p.

ROSSETTI, A.; MORALES, A. B. O papel da tecnologia da informação na gestão do conhecimento. **Ciência da Informação**, Brasília, v. 36, n. 1, p. 124-135, jan./abr. 2007. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652007000100009&lng=pt&tlng=pt>. Acesso em: 23 jun. 2017.

SOARES, P. L. **Segurança patrimonial**. São Paulo: Sicurezza, 2008. 65 p.

STAIR, R. M.; REYNOLDS, G. W. **Princípios de Sistemas de Informação**. 11. ed. Tradução de Noveritis do Brasil; Revisão técnica de Tânia Fátima Calvi Tait. São Paulo: Cengage Learning, 2015. 719 p.

ISBN 978-85-522-0225-7