Tecnologias Aplicadas ao Sistema de Segurança

Tecnologias Aplicadas ao Sistema de Segurança

Ruy Flávio de Oliveira

Dados Internacionais de Catalogação na Publicação (CIP)

Oliveira, Ruy Flávio de
O48t Tecnologias aplicadas ao sistema de segurança / Ruy Flávio de Oliveira. – Londrina : Editora e Distribuidora Educacional S.A., 2018.
224 p.

ISBN 978-85-522-0639-2

1. Tecnologias. 2. Segurança. I. Oliveira, Ruy Flávio de. II. Título.

CDD 600

Thamiris Mantovani CRB-8/9491

2018
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

Quando Abraham Maslow publicou, em 1943, a hierarquia das necessidades humanas, tivemos a oportunidade de entender com clareza tanto o que nos move, quanto a prioridade que atribuímos àquilo que é importante em nossas vidas. Entendemos, por meio da hierarquia das necessidades de Maslow, que não há prioridade maior que as necessidades fisiológicas do indivíduo: se a escolha é entre oxigênio e, digamos, o novo modelo do iPhone, qualquer um de nós (em sã consciência) optaria pela possibilidade de continuar respirando, obviamente. A implicação é clara: sem a garantia daquilo que nos permite viver, quaisquer outras necessidades são secundárias.

Para fins desta disciplina, devemos dar um passo adiante na hierarquia das necessidades humanas, o que nos leva ao patamar que nos concerne: a segurança. Segundo Maslow, uma vez garantidas as necessidades de nossa fisiologia — respiração, alimentação, hidratação, descanso e reprodução —, nossas próximas preocupações concernem à segurança, ou seja, a manutenção da possibilidade de continuarmos vivos, em busca de nossos objetivos (SAMPAIO, 2009).

A segurança é, portanto, um dos assuntos mais importantes para o ser humano, e tanto a busca pela segurança quanto sua manutenção ocupam papel proeminente na história da humanidade.

O advento do computador digital, a partir da década de 1930, trouxe incontáveis benefícios para a vida moderna e hoje encontra-se na base de praticamente todo o desenvolvimento em curso em nosso planeta. A tecnologia digital, obviamente, hoje é central nos esforços de segurança empreendidos por nações, empresas, organizações governamentais e não governamentais, e indivíduos. E é exatamente sobre o papel da tecnologia nos esforços de segurança que trataremos ao longo desta disciplina.

Veremos, aqui, que, como no caso de qualquer ferramenta, podemos ser grandemente auxiliados ou até mesmo atrapalhados, dependendo de como a utilizamos. A ferramenta em si não faz nada, dependendo 100% de nossas ações em seu uso. O mesmo vale para segurança: a tecnologia pode ser de grande valor, desde que seja adequadamente utilizada.

Nesta disciplina, trabalharemos a capacidade de comunicação, bem como a iniciativa, a curiosidade e o raciocínio lógico e resolução de problemas, buscando aplicar essas atitudes em questões pertinentes ao conteúdo abordado.

Na primeira unidade, você vai conhecer as origens da tecnologia digital e vai entender como funcionam a ética e a segurança quando aplicadas a esse conceito. Na segunda unidade, você vai conhecer mais sobre as tecnologias de comunicação e informação, bem como sobre a aplicação dessas tecnologias na internet. Na terceira unidade você começará a encaixar esses conhecimentos adquiridos sobre tecnologia no campo da segurança, aplicando os conceitos obtidos até então para melhorar a proteção oferecida ao cidadão por sistemas, equipamentos e processos no contexto da segurança pública. Por fim, na quarta unidade, você vai aplicar os conceitos de tecnologia no campo da segurança privada.

Esperamos que você também possa se beneficiar bastante ao longo dessa aventura.

Tecnologias: origens, ética e segurança

Convite ao estudo

As tecnologias digitais estão entre as ferramentas mais potencialmente úteis à humanidade, sem dúvida. Desde sua introdução na sociedade moderna, a partir da década de 1930, temos podido observar que as tecnologias digitais têm auxiliado — como poucos outros elementos inventados pelo ser humano — a melhorar a vida das pessoas.

Ainda que seja assim, a tecnologia por si só não realiza nada, e, mal utilizada, pode ser até mesmo bastante nociva. Veja: uma enxada jogada em um canteiro não tem valor nenhum para o processo de plantar e colher. Essa mesma enxada, se usada como arma, pode machucar muito uma pessoa. Apenas quando é utilizada adequadamente pode trazer os benefícios que dela se espera. O mesmo se dá com as tecnologias digitais: podem não servir para nada, podem servir para causar dano — a exemplo dos vírus de computador — e podem trazer benefícios para a sociedade, quando bem utilizadas.

Isso implica que precisamos entender a sociedade que queremos beneficiar por meio da tecnologia antes de entrarmos no mérito da tecnologia em si. É útil entendermos (ou relembrarmos) conceitos acerca de democracia, cidadania e inclusão digital, bem como as responsabilidades do estado, do cidadão e das empresas para que possamos ter em mente que esses são conceitos mais importantes que a tecnologia, os quais, portanto, devem sempre ser servidos pela tecnologia (e nunca o contrário).

O objetivo principal (e mais geral) que buscamos atingir é conhecer as tecnologias criadas para o exercício da segurança pública e da segurança privada, aumentando-se a eficiência de

ambos os serviços por meio de sistemas e equipamentos com os quais seja possível extrair dados essenciais para o exame e a proteção social e do particular. Mais especificamente, buscamos conhecer e aplicar os equipamentos e programas básicos de computação na segurança do indivíduo, da organização e da própria sociedade.

Na primeira seção desta unidade, revisitaremos os conceitos de democracia, cidadania e inclusão social, formando o alicerce necessário para que, nas seções seguintes, possamos entender como a tecnologia poderá servir melhor a estes conceitos.

Na segunda seção, entenderemos historicamente como se deu o desenvolvimento do computador, que está no cerne das tecnologias digitais à nossa disposição.

Finalmente, na terceira seção dessa nossa primeira unidade, trataremos de uma questão fundamental: a ética no uso da tecnologia.

A prefeitura da cidade de Paraconé-Açu não esperava um crescimento populacional tão acirrado como vem acontecendo nos últimos anos. Em função de incentivos fiscais oferecidos pelo estado e pela prefeitura, duas multinacionais e seis empresas regionais mudaram suas sedes para a cidade. As grandes empresas atraíram outras empresas pequenas, fornecedores e outras empresas orbitantes. A oferta de emprego e o dinheiro extra na economia atraíram um grande contingente populacional e mais negócios de varejo variados para a cidade. O resultado é que a população — antes na casa dos 10 mil habitantes — já ultrapassa os 200 mil. A prefeitura está animada com o crescimento sustentado, mas está preocupada com a administração de todo o aparato municipal, que cresceu muito. Foi então que o prefeito decidiu contratar sua empresa para prestar consultoria ao município a fim de auxiliar no processo de automatização (informatização) dos processos administrativos, com uma preocupação grande no quesito segurança. A Guarda Municipal de Paraconé-Açu

será uma das grandes beneficiadas na implantação de projetos de automação, o que, com certeza, resultará em melhorias das atividades de guarda ao patrimônio e ao policiamento.

Auxiliar esse pessoal será um desafio e tanto, não? Ao trabalho!será uma das grandes beneficiadas na implantação de projetos de automação, o que, com certeza, resultará em melhorias das atividades de guarda ao patrimônio e ao policiamento.

Auxiliar esse pessoal será um desafio e tanto, não? Ao trabalho!

Seção 1.1

Segurança pública, inclusão digital, cidadania, democracia

Diálogo aberto

Nos dias de hoje, falamos muito acerca de ferramentas que podem auxiliar a sociedade, facilitando a vida de todos. Mas será que qualquer ferramenta deve ser adotada em qualquer situação só porque está disponível?

As câmeras de segurança, por exemplo, à disposição dos governantes, podem ser instaladas em qualquer lugar, ou deveriam ser limitadas aos locais públicos? Há argumentos interessantes, prós e contras, em ambos os casos. A tecnologia em si é neutra e flexível, podendo ser usada de uma maneira e de outra, obviamente. Mas, se a limitação do uso da tecnologia não é, em si e na vasta maioria das vezes, tecnológica, o que limita seu uso? Sob quais regras deve se pautar seu uso? É aí que entram alguns termos bastante simples mas fundamentalmente importantes: democracia, cidadania, segurança pública, inclusão social e inclusão digital. A tecnologia deve estar sempre atrelada a todos esses termos, a todos esses conceitos fundamentais, e a eles ser submissa.

Nesta aula, vamos revisitar todos esses conceitos, comprovando e ressaltando sua importância, e neles alicerçando o uso adequado e benéfico da tecnologia em geral, e da tecnologia digital em particular.

A primeira tarefa de sua empresa nessa nova empreitada da prefeitura de Paraconé-Açu em automatizar e informatizar suas operações é garantir que todos os funcionários conheçam os conceitos cívicos básicos e, em especial, sua ligação com a inclusão digital e com a segurança pública. Nesse sentido, você e seu time deverão proporcionar uma reciclagem do conhecimento entre os funcionários da prefeitura, desde o prefeito até o mais recente dos estagiários contratados.

O objetivo é que, ao final da reciclagem, todos tenham bem alicerçados os conceitos de segurança pública e de inclusão digital,

estabelecendo os requisitos básicos e inerentes à democracia e cidadania que vão auxiliar os funcionários a se situar na discussão. Seu desafio será apresentar os principais tópicos desse alicerce.

E, então, vamos a esse desafio?

Mãos à obra!

Não pode faltar

Para termos ideia de como o conceito de "democracia" é importante em nosso país, não precisamos ir mais longe do que o artigo primeiro de nossa Constituição (BRASIL, 2016a, p. 1): "A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em **Estado Democrático** de Direito" (grifo nosso).

O Brasil é (e luta constantemente por continuar sendo) uma democracia, e esse é o ponto mais fundamental de nossa identidade nacional. Todas as conquistas de nossa nação em mais de um século, toda a projeção que ganhamos, todas as conquistas nos âmbitos científico, econômico, cultural e esportivo foram alcançadas em (e, na maioria dos casos, facilitadas por) um Estado democrático.

Mas o que é essa tal "democracia" a respeito da qual se fala tanto?

Rosenfield (2003) define o termo sob o ponto de vista etimológico: *governo do povo* (pois deriva do grego – *demo* significa "povo" e *kracia* significa "governo"), ou, como se exerce na prática, *governo da maioria*.

Esse conceito simples, mas profundo e poderoso, é o que está na base de nossa nação e deve ser compreendido em suas implicações pelo fato de ser provavelmente o maior tesouro de que dispomos em nosso país, quer sejamos capazes de perceber isso, quer não.

Em tempos antigos – na Atenas do século V a.C. em que foi desenvolvida – a democracia era exercida de forma bastante diferente do que nos dias de hoje. Naqueles tempos, como afirma Rosenfield (2003), a democracia era exercida de forma direta, por meio de assembleias em praça pública. O "povo", naquele caso, tinha uma definição bem mais restrita do que nos dias de hoje: podiam participar do processo democrático apenas os considerados "cidadãos", que no caso eram apenas a elite da sociedade ateniense. As decisões eram postas em pauta e decididas por todos os presentes, ali mesmo, diretamente e sem a presença de representantes de classes ou grupos.

Desse berço ateniense, a democracia evoluiu para o modelo representativo, uma vez que o direito de decisão se estendeu para além das elites, as populações cresceram, e os territórios se ampliaram para além da "cidade-estado". Nesse cenário, isto é, com uma população maior com direito de opinião (leia-se: voto), distribuída em amplos territórios geográficos, a democracia direta torna-se um exercício impossível, e o modelo deve evoluir.

Surge, assim, o modelo de democracia representativa, isto é, em que o cidadão vota mais não na ação em si, mas em representantes de sua confiança, que levarão suas opiniões e necessidades em conta nas decisões tomadas. Estamos aqui falando, obviamente, de um sistema democrático em que as instituições funcionam como deveriam. Há exemplos claros em que o "combinado" entre representante (o político eleito) e representado (o eleitor) não é cumprido, mas essa deve ser encarada como uma situação de exceção, devendo ser discutida em outros fóruns de discussão, uma vez que representam distorções no modelo, e não o modelo como foi programado para funcionar (e, a bem da verdade, funciona em vários países do mundo).

Mas será que a democracia é uma forma de governo que tem valor? Churchill (1947) afirma que a democracia é a pior forma de governo, exceto por todas as demais formas que já foram experimentadas. De fato, nela o cidadão tem a garantia de seus direitos, entre os quais o fundamental direito de decisão por meio do voto, apenas nos estados democráticos, uma vez que nas monarquias, autocracias, teocracias e várias formas de ditadura que já foram (ou continuam sendo) tentadas pelo mundo afora, a sociedade caminha na direção ditada por poucos, sem que a população tenha voz ou direitos.

É exatamente por seu caráter inclusivo e pela manutenção do estado de direito que a democracia, isto é, o governo democrático, deve ser vista como o maior bem de uma nação e por esta protegida a todo custo.

Democracia como alicerce para a tecnologia

Uma vez estabelecido que a democracia é o bem maior de uma nação, precisamos estabelecer qual é a relação da tecnologia com a democracia.

Mais uma vez, Rosenfield (2003) nos apoia quando afirma que o voto é a base da democracia. Podemos afirmar com segurança que o voto é a primeira ferramenta da democracia, isto é, a ferramenta que permite o efetivo exercício da democracia. Assim como o voto, a assembleia, o debate, o cargo eletivo, a divisão dos poderes (executivo, legislativo, judiciário) são ferramentas da democracia, todas a seu serviço, permitindo seu exercício em uma nação.

Justamente aí está o cerne da questão: quaisquer dessas ferramentas existem para servir à democracia. O voto faz sentido enquanto ferramenta de exercício de escolha em um ambiente democrático; os postos de presidente ou senador, ou qualquer outro, dão legitimidade a quem os ocupa, e quem os ocupa tem por dever zelar pela condução democrática de suas ações. Seria um erro inaceitável, por exemplo, um político eleito imaginar que a democracia deve servi-lo, pois foi eleito pela vontade do povo. Essa postura significaria uma inversão de valores que é absolutamente incompatível com a democracia. O político é eleito para servir à democracia, e não para servir-se dela. A ação do político eleito deve acontecer para manter e fortalecer a democracia. Assim como o direito de voto é exercido nesse sentido, a assembleia e o debate ocorrem de maneira a fortalecer os princípios democráticos, e assim sucessivamente.

Até mesmo as ferramentas de exceção à democracia devem ser regidas por mecanismos que lhes limitem a ação, para que não ponham em risco o processo democrático. Rosenfield (2003) nos remete à República Romana como exemplo. Entre os anos de 509 b.C. e 27 b.C, Roma foi uma república, com dois cônsules que regiam a cidade-estado, eleitos anualmente pelos cidadãos. Contudo, em tempos de guerra, poderia ser nomeado um tirano, isto é, um regente não limitado pelas leis romanas. O governo do tirano teria a vantagem de ser mais ágil, com decisões tomadas sem a morosidade do senado, o que poderia dar vantagem estratégica a Roma durante o conflito em questão. Ora, esse tirano, por definição, feria o estado democrático, uma vez que sua palavra era cumprida sem ser limitada pelo arcabouço regulatório da época — uma ferramenta de controle do governante, como é nos dias de hoje a Constituição. Ocorre que o tirano assumia esse posto por tempo determinado e corria o risco de ser condenado à pena capital caso buscasse por qualquer meio estender seu período de poder ou dele se aproveitar em benefício próprio. Dessa forma, a ferramenta de

exceção à democracia (a figura prevista do tirano) era limitada por ferramentas a serviço da própria democracia (tempo determinado, julgamento sobre os limites do exercício da tirania). Pronto: assim a ferramenta de exceção à democracia voltava a servir à democracia.

Ora, segue-se desse raciocínio que as ferramentas disponíveis em um ambiente democrático devem, sobretudo, servir à democracia, independentemente de sua natureza. O mesmo, obviamente, aplica-se às ferramentas de natureza tecnológica. Exemplo disso é a urna eletrônica, representada na Figura 1.1, a seguir, que em 2016 completou 20 anos e é reconhecida como "símbolo da democracia brasileira e principal empreendimento do Tribunal Superior Eleitoral" (BRASIL, 2016b, p. 6).

Figura 1.1 | Urna eletrônica

Fonte: <https://upload.wikimedia.org/wikipedia/commons/2/2a/Urna_eletrônica.jpeg>. Acesso em: 26 ago. 2017

Como qualquer ferramenta em uso em uma democracia, a urna eletrônica deve servir à democracia, e não por ela ser servida. Em outras palavras: a urna eletrônica deve facilitar o processo democrático, suas características de mobilidade, facilidade de uso e baixo custo devem servir — e servem — para facilitar o acesso do cidadão ao voto. Nesse mesmo sentido, a urna eletrônica não deve impor obstáculos ao processo democrático. Um dos desafios enfrentados nesse sentido é o desafio da segurança. A urna eletrônica deve ser protegida contra fraudes e acessos indevidos, pois, do contrário, seria uma ferramenta com enorme potencial de prejudicar o processo democrático: uma fraude nas eleições impõe à população um governante que não foi eleito, que é o posto da livre escolha proporcionada pelo voto. Foi pensando nisso, isto é, na criação de um dispositivo tecnológico que apoiasse a democracia, que foram criadas as diretrizes para a urna eletrônica (BRASIL, 2016b):

- **Solução universal** – uma única urna, com funcionamento único para todos os modelos e versões.
- **Aderência total à legislação** – a urna não deve violar nenhuma das leis eleitorais do país.
- **Fácil utilização** – a urna deve ser de simples operação, não demandando conhecimento técnico do eleitor.
- **Baixo custo** – tanto a urna quanto o processo completo de sua operação não devem onerar os cofres públicos.
- **Solução duradoura** – cada equipamento em si deve durar por várias eleições sem apresentar defeito.
- **Facilidade logística** – o equipamento deve ser pequeno e leve, facilitando seu transporte durante as eleições e seu armazenamento em períodos entre eleições.
- **Autonomia** – presença de bateria interna para operação em locais e/ou períodos sem eletricidade.
- **Segurança** – eliminação de fraudes conhecidas no processo de voto com cédulas de papel, e prevenção de fraudes no processo de votação eletrônica.

Assimile

Por ser pautada nessas diretrizes, é possível afirmar que a urna eletrônica é, de fato, uma tecnologia a serviço da democracia, alicerçada sobre o próprio processo democrático. Todas as ferramentas adotadas pelo estado – tecnológicas ou não – devem colaborar para o fortalecimento da democracia.

Cidadania como alicerce para a tecnologia

Então, agora que foi estabelecida a relação que a tecnologia deve sempre guardar para com a democracia, podemos ampliar a discussão, desta vez estudando a relação da tecnologia para com outro conceito fundamental ao estado moderno: a cidadania.

Botelho e Schwarcz (2013) buscam em Aristóteles a primeira definição de cidadania que a história nos proporciona. Para o filósofo grego, ser cidadão é ser reconhecido pelo Estado como alguém dotado de direitos perante esse Estado, entre os quais, o direito de participar das decisões coletivas. Essa primeira definição era restritiva em quem poderia ser considerado cidadão, uma vez que excluía os homens que

viviam do próprio trabalho (artesãos e trabalhadores braçais de toda sorte) e mulheres, restringindo o título de "cidadão" aos proprietários de terras e de escravos. Outra restrição importante – e que permanece até os dias de hoje no conceito moderno de cidadania – é a exclusão dos estrangeiros: o cidadão deve ser natural do Estado que lhe confere esse título. Tempos depois dessa primeira definição de Aristóteles, o Estado passou a considerar também como cidadãos aqueles a quem atribuía a condição de naturalização, isto é, o direito de residência permanente.

Aqui faz-se necessário um parêntese: mesmo não sendo cidadão, o estrangeiro legalmente presente em um estado guarda alguns direitos, tais como (mas não restritos a) o direito de proteção pelo estado, o direito de livre trânsito nos locais em que assim é permitido, o direito à privacidade, o direito à posse dos bens que traz consigo, entre outros. Já outros direitos disponíveis aos cidadãos são vetados aos estrangeiros, como o direito de residência permanente.

O conceito de cidadania abriga em si, além dos direitos, os chamados deveres do cidadão. No Brasil, cada cidadão tem o compromisso inato (assumido à sua revelia antes do nascimento, por ter nascido em nosso país) com vários aspectos da nação, entre eles:

- Cumprir as leis vigentes no país.
- Votar nas eleições a partir do momento que atingir a idade legal mandatória (18 anos).
- Respeitar os direitos das outras pessoas.

Aqui é importante observar que cada nação determina quais devem ser os direitos e deveres de seus cidadãos. Como exemplo, podemos citar o serviço militar. Observe no Quadro 1.1, a seguir, como o serviço militar é encarado em três nações diferentes:

Quadro 1.1 | Comparativo do serviço militar em três diferentes nações

País	É dever? Para quem?	Período de serviço
Brasil	Sim; para todos os homens considerados aptos, que completam 18 anos	1 ano
EUA	Não	1 ano, para os que decidem se alistar, renovável indefinidamente
Israel	Sim; para todos os homens e mulheres considerados aptos que completam 18 anos	3 anos para os homens, 2 anos para as mulheres

Fonte: elaborado pelo autor.

O voto é outro exemplo de diferença entre as nações. Em nações não democráticas, o voto é inexistente ou tende a ser altamente limitado. Na China, por exemplo, vigora o modelo de partido único (apenas o Partido Comunista Chinês tem o direito de operar em território chinês). O partido determina quem assume os cargos públicos (governantes e funcionários do governo) nos níveis estadual (no caso, no nível das províncias chinesas) e federal, e o cidadão tem direito a voto apenas na esfera municipal. Já nos EUA, Inglaterra, Portugal, Espanha, Itália e demais países democráticos da Europa, à exceção de Grécia, Bélgica e Luxemburgo, o voto é facultativo, isto é, é um direito do cidadão, que pode optar por exercê-lo ou não. Já no Brasil, México, Argentina, Paraguai, Peru, Grécia, Bélgica, Luxemburgo, Austrália e várias repúblicas africanas, americanas e asiáticas, o voto é obrigatório, ou seja, um dever do cidadão para com o estado.

Segundo Rosenfield (2003), os países que adotam o voto facultativo entendem que esse mecanismo de escolha é um direito do cidadão e uma expressão de sua liberdade, que é um fator fundamental ao estado democrático de direito. Já nos países em que o voto é obrigatório, o raciocínio é de que o dever maior do cidadão é zelar pela democracia, e a democracia depende diretamente do exercício de escolha de seus cidadãos. A obrigatoriedade do voto sinaliza que aquela nação entende que todos os cidadãos são responsáveis pelos rumos tomados, e essa escolha se realiza nas urnas. Segundo esse raciocínio, se o bem maior de uma nação é a democracia, é dever de todo cidadão colaborar pela manutenção dela, e o voto faz parte integral desse dever para com o Estado.

Reflita

É possível afirmar que as democracias em que o voto é obrigatório são menos "democráticas" do que as democracias em que o voto é facultativo? Quais são os argumentos que corroboram ou combatem esse ponto de vista?

Assim como no caso da democracia, existem várias ferramentas que auxiliam na manutenção da cidadania. As várias autarquias públicas, por exemplo, são ferramentas necessárias para garantir os direitos e cobrar os deveres do cidadão.

Contudo, diferentemente da democracia, as ferramentas ligadas à cidadania devem apoiá-la até o limite em que a defesa da democracia

tenha início. Em outras palavras: a democracia deve ocupar posição hierarquicamente superior à cidadania, e as ferramentas que lidam com a cidadania devem agir de acordo com essa hierarquia. Daí segue-se logicamente que toda ferramenta a serviço da cidadania deve, também, estar a serviço da democracia. Não haveria, pois, sentido, atribuir à cidadania (ou mesmo classificar como parte da cidadania) um direito que viesse a ferir a democracia.

É importante observar, nesse sentido, que as ferramentas que a nação põe à disposição da cidadania colaboram ativamente para o fortalecimento democrático dessa mesma nação. Dispositivos de amparo social, tais como a previdência e a assistência social, que são programas federais, bem como os sistemas de educação, transporte e saúde postos à disposição da população têm por objetivo auxiliar o cidadão em sua vida no país. São ferramentas fundamentais a serviço da cidadania.

De maneira análoga, as ferramentas tecnológicas devem servir a cidadania, que lhes fornece o alicerce, sempre. Mecanismos tais, como o cadastro informatizado em serviços como a Previdência Social e o SUS (Sistema Único de Saúde) tendem a facilitar sobremaneira a vida do cidadão, que passa a ter acesso mais ágil aos serviços oferecidos pelo Estado.

Outro exemplo é o processo de informatização dos serviços oferecidos pelos estados, e um caso que se destaca é o estado de São Paulo, que criou o Poupatempo, com o intuito de unir em um só local serviços municipais estaduais e federais ao cidadão. Criado em 1996, na primeira gestão do então governador Mario Covas, o Poupatempo já vem há mais de duas décadas facilitando a vida do cidadão. A integração dos serviços e a informatização têm um papel preponderante no sucesso desse esforço do estado.

Segurança Pública como alicerce para a tecnologia

É sempre bom reforçar a você, caro aluno, que um aspecto fundamental da vida democrática e do dia a dia do cidadão é a segurança. No que concerne ao Estado, o assunto segurança pode ser dividido em dois grandes motes:

- **Segurança nacional** – assuntos de segurança ligados ao país em si, suas fronteiras, suas relações com os países vizinhos e

com a comunidade internacional, bem como com as ameaças externas, ou seja, a defesa da nação e a manutenção da paz

- **Segurança pública** – assuntos de segurança ligados à população e aos acontecimentos internos do país que não ponham a segurança nacional em risco, ou seja, a defesa do cidadão e a manutenção da ordem.

Exemplificando

Uma revolta, por exemplo, seria um assunto pertinente à segurança pública por colocar o cidadão em risco, mas seria um assunto a ser tratado no nível da segurança nacional, uma vez que a revolta colocaria a própria democracia em risco.

É importante frisar que, em assuntos de segurança pública, a segurança coletiva tem precedência sobre a segurança individual. Em outras palavras, as ações de segurança pública visam a beneficiar a população como um todo e devem "pesar" o benefício coletivo em todos os momentos. No Brasil, por exemplo, o porte de armas de fogo é vetado ao cidadão comum, pois, apesar de muitos acreditarem que as armas são importantes para sua proteção, o Estado brasileiro entende que, coletivamente, a liberação do porte seria algo nocivo para a segurança da população como um todo.

Fica claro, pelo que já foi visto nos itens anteriores, que é muito positivo quando a tecnologia serve à segurança pública, uma vez que a segurança é, em si, um mecanismo a serviço da democracia e do cidadão.

É aqui que surgem alguns dos paradoxos por conta das possibilidades que a tecnologia oferece. A tecnologia em si é "agnóstica", isto é, não se limita a conceitos humanos e/ou sociais, tais como as noções de democracia, cidadania e outras que tais. Para entender como isso funciona, podemos pensar em uma ferramenta mais simples: a enxada. Essa ferramenta foi criada nos primórdios do desenvolvimento agrário da civilização, e é útil (indispensável, até) no trato com a terra. Contudo, a enxada não tem poder de decisão: se quem a empunha a utilizar para ferir outra pessoa, a responsabilidade não será nunca da enxada. Em suma, ela pode ser usada tanto para revolver a terra, quanto como arma, a critério de quem a empunha.

O mesmo pode ser dito acerca da tecnologia, que pode servir à segurança ou atuar contra ela, dependendo de como é usada. Programas de computador podem ser usados para facilitar a vida do cidadão, mas também podem ser usados para ferir-lhe a privacidade, roubar-lhe os bens ou mesmo colocá-lo em risco físico.

Exemplificando

Um exemplo de programa de computador que é patentemente nocivo ao público é o vírus de computador.

Nesse sentido, sempre ficará a cargo da segurança pública reger o uso da segurança em uma nação, de forma que seja útil e não nociva à democracia e ao cidadão.

Ao longo de todas as seções desta disciplina, veremos essa ligação intrínseca entre tecnologia e segurança.

Inclusão digital como alicerce para a tecnologia

Por fim, desde o advento da internet, no início da década de 1990, temos vivenciado um mundo cada vez mais conectado, em que a informação flui cada vez mais rapidamente por todos os cantos do planeta.

Essa característica do mundo moderno realmente tem o potencial de facilitar e engradecer sobremaneira a vida do cidadão. Isso, claro, desde que esse cidadão tenha acesso a todo esse fluxo de informações.

E como isso se dá? Como garantir que o cidadão tenha acesso à tecnologia da informação a fim de poder derivar benefícios por ela oferecidos? A resposta é simples: por meio da inclusão digital. O Estado brasileiro vem empreendendo esforços para facilitar o acesso de seus cidadãos à tecnologia digital, e quem toma a frente das ações é o Ministério da Ciência, Tecnologia e Inovação (MCTI). Veja algumas das ações do governo brasileiro nesse sentido (BRASIL, 2016c):

- **Banda larga nas escolas** – provisão de canais rápidos de comunicação com a internet nas escolas de ensino fundamental e médio.
- **Computadores para inclusão** – facilitação de compra e acesso de populações carentes a computadores, por meio de subsídios e acordos de isenção com fabricantes.

- **Oficina para inclusão digital** – grupo permanente de discussão de estratégias e ações para inclusão digital.
- **Um computador por aluno** – programa de disponibilização de laptops de baixo custo para estudantes do ensino fundamental e médio.

Pesquise mais

Para conhecer mais de perto todas as ações de inclusão digital do governo federal você pode ir até a página do MCTI que versa sobre esse assunto e explana todas as ações planejadas e em curso:

Disponível em: <https://www.governoeletronico.gov.br/eixos-de-atuacao/cidadao/inclusao-digital>. Acesso em: 28 ago. 2017.

Sem medo de errar

A fim de auxiliar a prefeitura de Paraconé-Açu a automatizar e informatizar suas operações, você, nessa primeira etapa, deverá estabelecer os conceitos básicos inerentes à democracia e à cidadania que vão auxiliar os funcionários a se situar na discussão, servindo de alicerce para que as soluções se construam de maneira produtiva nas etapas que estão por vir.

Os quatro conceitos a serem pontuados para os funcionários da prefeitura de Paraconé-Açu são os seguintes:

- Democracia.
- Cidadania.
- Segurança pública.
- Inclusão digital.

Você poderá apresentar os assuntos da seguinte forma

- Democracia
  - ◊ Definição
    - Governo do povo ou, na prática, governo da maioria.
  - ◊ Características
    - Criada na Grécia, no século V a.C.

- Era exercida diretamente pelos poucos considerados "cidadãos".
- Hoje não é mais exercida diretamente, sendo chamada de "democracia representativa", uma vez que o cidadão elege aqueles que o representarão nas decisões.
- É o bem maior de uma nação, devendo ser preservada acima de tudo.

◊ Relação com a tecnologia

- Toda ferramenta à disposição da democracia deve servi-la, fortalecê-la, colaborando para sua longevidade.
- As ferramentas tecnológicas são um subconjunto das ferramentas à disposição da democracia e, da mesma forma, devem colaborar para seu fortalecimento.

• Cidadania

◊ Definição

- Ser cidadão é ser reconhecido pelo Estado como alguém dotado de direitos perante este Estado, entre os quais, o direito de participar das decisões coletivas.
- Ter direitos de naturalidade, por ter nascido em um país e por este país ser reconhecido como cidadão.

◊ Características

- A cidadania atribui ao cidadão direitos e deveres, tais como o direito ao livre trânsito, o direito de propriedade, o direito de constituir família e o direito de constituir empreendimento, entre outros. Entre os deveres, temos o dever de cumprir as leis vigentes, o dever de votar (um dever aqui no Brasil), o dever de respeitar os direitos dos demais cidadãos.
- No que concerne à sua relação com a democracia, a cidadania deve ter em si apenas elementos que fortaleçam a democracia, obviamente.

◊ Relação com a tecnologia

- Sob o ponto de vista da cidadania, a tecnologia é neutra, isto é, não necessariamente apoia nem se opõe à

cidadania, devendo ser adotada aquela tecnologia que apoie a agenda cidadã. O uso da tecnologia pelo Estado deve ser pautado pelo fortalecimento da cidadania, ou seja, da facilitação que a tecnologia proporciona à vida de seus cidadãos

- **Segurança pública**

◊ Definição

- Assuntos de segurança ligados à população e aos acontecimentos internos ao país que não ponham a segurança nacional em risco – uma revolta, por exemplo, seria um assunto pertinente à segurança pública por colocar o cidadão em risco, mas seria um assunto a ser tratado no nível da segurança nacional, uma vez que a revolta colocaria a própria democracia em risco.

◊ Características

- Ações tomadas pelo estado para proteger o cidadão.
- A segurança coletiva tem precedência sobre a segurança individual.

◊ Relação com a tecnologia

- A tecnologia também é agnóstica no que tange à segurança pública: tanto pode contribuir para com a segurança, como pode ameaçá-la, dependendo de como é utilizada. É, portanto, função do estado adotar as tecnologias que apoiarão a segurança pública, utilizando-as adequadamente para esse fim.

- **Inclusão digital**

◊ Definição

- Ações tomadas pelo estado para garantir o acesso de seus cidadãos às tecnologias digitais disponíveis

◊ Características

- Programas de inclusão.
- Ações oferecidas a toda a população.
- Ações descentralizadas e dirigidas, mas que, no geral, visam atender a todos.

◊ Relação com a tecnologia

- Sob o ponto de vista do estado, não ferindo a democracia, a cidadania e a segurança pública, o cidadão tem direito de acesso à tecnologia, e é função do Estado fornecer esse acesso.

Assim, com a lista de tópicos acima, apresentada de maneira estruturada, clara, os funcionários da prefeitura de Paraconé-Açu terão o alicerce necessário para discutir as questões da tecnologia e da segurança no município, estando disponível para auxiliar nessa empreitada.

Avançando na prática

Permitir ou não o uso da tecnologia?

Descrição da situação-problema

O senhor Morlow da Silva é morador de um bairro de classe alta na capital de um determinado estado. Preocupado com a escalada do crime, ele decide que a melhor prevenção é a informação, e decide investir em um projeto pessoal arrojado: um sistema de vigilância baseado no novíssimo conceito de "enxame de microdrones". Um conjunto de 100 microdrones – pequenos drones silenciosos do tamanho de uma abelha, equipados com transmissores de radiofrequência, câmeras de vídeo de alta resolução que filmam até em infravermelho, e baterias que duram 6 horas de voo e transmissão ininterruptas – conecta-se via rádio a um sistema de monitoramento que pode ser instalado em um *notebook* de mercado.

Com esse equipamento, Morlow conseguirá saber o que se passa em praticamente todo o bairro, tanto no perímetro das residências quanto dentro das casas, pois entende que ninguém vai se opor aos pequenos drones, uma vez que são praticamente invisíveis e facilmente confundidos com insetos quando são vistos.

Morlow procura você, um consultor de segurança pública, para saber se esse projeto é viável e se vai conseguir autorização do governo para fazer a importação e implantação da solução. O que você pode dizer a Morlow? Em sua opinião, esse projeto é viável? Ele fere algum princípio democrático? Quais são as vantagens e desvantagens?

Resolução da situação-problema

Como consultor, você deverá encarar essa questão não apenas sob o ponto de vista da tecnologia e de sua eficiência em angariar informações audiovisuais de maneira discreta, mas também sobre todas as implicações à cidadania e à segurança pública que a permissão de uso de uma solução dessas acarretaria não só a esse cidadão, mas à comunidade e ao próprio país.

Nesse contexto temos:

- Vantagens
    - ◊ Vigilância em ampla região, com detalhes de tudo o que ocorre: quem entra e quem sai do bairro, e mesmo o que ocorre nas casas.
    - ◊ Em situação de uma invasão com reféns, informações de quem está na casa, quantos invasores, onde se encontram podem ser passadas para a polícia, que pode ser mais eficaz em suas ações.

- Desvantagens
    - ◊ A solução tem o potencial de violar explicitamente o direito a privacidade dos cidadãos que residem no raio de ação dos microdrones.
    - ◊ A solução, se for liberada para uso pela população, também estará ao alcance dos bandidos, que a poderão usar para averiguar quais as residências são mais vulneráveis a assaltos e quais os residentes são mais passíveis de sequestros, por exemplo, inclusive com drones podendo avisar com antecedência da chegada da polícia.

Quanto à questão de ferir algum princípio democrático, a utilização de *drones* é regulada pela Agência Nacional de Aviação Civil, a qual fixa regras que devem ser observadas para operação do equipamento, inclusive quando à distância mínima que pode se aproximar das pessoas.

Diante desse quadro, você deverá sugerir fortemente que Morlow opte por alguma solução diferente, pois essa não se mostra adequada, e a busca de sua liberação para uso de cidadãos comuns causará mais mal do que bem.

Faça valer a pena

1. O Brasil é (e luta constantemente por continuar sendo) uma democracia, e esse é o ponto mais fundamental de nossa identidade nacional. Todas as conquistas de nossa nação em mais de um século, toda a projeção que ganhamos, todas as conquistas nos âmbitos científico, econômico, cultural e esportivo foram alcançadas em (e, na maioria dos casos, facilitadas por) um Estado democrático.

Assinale a alternativa correta com relação à democracia brasileira

a) Pelo estipulado em nossa Constituição, o Brasil não é uma democracia.
b) A democracia brasileira teve início a partir de nosso descobrimento, em 1500.
c) A democracia brasileira teve início na Independência, em 1822.
d) No Brasil, a exemplo de Atenas, praticamos a democracia direta.
e) No Brasil praticamos a democracia representativa.

2. A primeira definição de cidadania que a história nos proporciona, ainda na Antiguidade, especifica que ser cidadão é ser reconhecido pelo Estado como alguém dotado de direitos perante este Estado, entre os quais, o direito de participar das decisões coletivas.

Essa definição, por mais restritiva que fosse, foi enunciada por:

a) Péricles.
b) Sócrates.
c) Platão.
d) Aristóteles.
e) Aristófanes.

3. Observe as asserções a seguir:
I. Uma revolta é um assunto do âmbito de segurança nacional.
PORQUE
II. Uma revolta, apesar de pôr em risco a segurança da população e, portanto, também ser pertinente à segurança pública, põe em risco a própria democracia.

Avalie as asserções anteriores e assinale a alternativa correta:

a) I e II são verdadeiras, e II justifica I.
b) I e II são verdadeiras, porém II não justifica I.
c) I é verdadeira, e II é falsa.
d) I é falsa, e II é verdadeira.
e) I e II são falsas.

Seção 1.2

Desenvolvimento tecnológico e a evolução do computador

Diálogo aberto

Olá! Vamos iniciar mais uma seção em nosso estudo acerca das tecnologias aplicadas aos sistemas de segurança.

Imagine o seguinte cenário: por alguma razão desconhecida, acaba a energia elétrica no planeta Terra, e essa situação se estende por dias a fio. É óbvio que o inconveniente seria terrível: sem iluminação à noite, estaríamos reduzidos a usar velas; elevadores deixariam de funcionar de imediato; semáforos ficariam desligados, contribuindo para o caos no trânsito; o caos no trânsito teria tempo curto de vida, uma vez que, sem eletricidade, é impossível tirar combustível da bomba para colocar no tanque do carro; as baterias se descarregariam em poucos dias e, a partir daí, até dispositivos móveis também seriam inúteis.

Em um cenário assim, podemos alegar que o próprio tecido social seria rompido, e o caos se instalaria. E qual dispositivo teria sua ausência mais sentida pela população? Podemos argumentar com bastante ênfase que seria o computador. Não porque não teríamos como publicar fotos de nossas dificuldades nas redes sociais, claro, mas sim porque a vasta maioria dos serviços dos quais dependemos nos dias de hoje está alicerçada sobre insubstituíveis redes de computadores.

Sistema de iluminação pública e rede de semáforos? Gerenciados por computadores. Sistema de abastecimento de água? Controlado por computadores. Sistema federal de apoio a emergências? Computadores, de novo. Sistema de monitoração nacional por satélite? Computadores e mais computadores. Hospitais, polícia, bombeiros? Todos dependem pesadamente de computadores para prestar seus serviços. Em suma: sem computadores, não teríamos como sustentar a vasta maioria dos serviços dos quais dependemos. Essa é a importância do computador em nossas vidas.

Depois dessa ênfase da presença do computador em nossas vidas, vamos retornar ao contexto de Paraconé-Açu. A fim de auxiliar a

prefeitura da cidade na adoção de tecnologia da informação (TI) com o objetivo de facilitar seus processos administrativos, sua empresa foi contratada, uma vez que tem grande expertise na área. Embora o policiamento da Guarda Municipal tenha atendido às questões de segurança, pode-se perceber que os agentes da Guarda ainda não dominam os pontos fundamentais da TI. Sua primeira tarefa será orientar o pessoal da prefeitura e da Guarda em conceitos introdutórios acerca de TI, de maneira que conheçam os conceitos de computador e programa de computador, sabendo situar-se mais adequadamente no assunto ao longo do cumprimento de suas funções, bem como do potencial de benefícios que essa ferramenta pode trazer aos cidadãos e às organizações. Ao final, a ideia é que se produza uma cartilha com tais conceitos, a qual auxiliará sobremaneira no desenvolvimento dos funcionários quanto às novas tecnologias.

Na presente seção, vamos entender um pouco mais sobre a importância do computador na vida moderna bem como seu histórico. Primeiramente, vamos fazer uma pequena introdução às tecnologias digitais, seguida de uma análise do desenvolvimento do histórico da computação, das noções básicas de comandos e algoritmos, e terminando com a utilização da tecnologia e sua repercussão social.

Vamos em frente!

Não pode faltar

Nossa relação com a tecnologia teve início no momento em que o primeiro hominídeo tomou em sua mão uma pedra para usar como ferramenta em alguma tarefa qualquer. Por mais que hoje não associemos as palavras "pedra" e "tecnologia", naquele longínquo momento da aurora da humanidade, estávamos buscando fora de nós mesmos algo que nos auxiliasse a ganhar vantagem na luta contra o ambiente que nos cercava. A tecnologia, portanto, iniciou-se aí: na Idade da Pedra.

Em uma definição mais ampla, Karasinski (2013, p. 1) afirma que "tecnologia é o uso de técnicas e do conhecimento adquirido para aperfeiçoar e/ou facilitar o trabalho com a arte, a resolução de um problema ou a execução de uma tarefa específica". Sim, é uma definição bem ampla, que engloba todas as ferramentas, processos e conhecimentos desenvolvidos desde os tempos da pedra lascada.

À medida que a humanidade progrediu, porém, as tecnologias foram se desenvolvendo, uma vez que o conhecimento acumulado foi permitindo o refinamento das técnicas e dos processos. Nos dias de hoje, basta abrirmos os olhos para enxergarmos que somos cercados de tecnologia por todos os lados. Do tecido que nos cobre a pele até os satélites que nos observam do espaço, somos cercados de tecnologia, e aqueles que, de alguma maneira, querem se afastar desse caldeirão tecnológico devem fazer um esforço consciente para tanto, buscando na natureza os locais em que a tecnologia ainda é ausente. Mesmo nesses casos, eles levarão consigo os elementos tecnológicos que lhes permitam facilidades no lidar com a natureza, tais como barracas, lanternas, botas apropriadas para a caminhada no mato etc.

A partir de agora, vamos observar mais de perto esse desenvolvimento tecnológico.

Introdução às tecnologias digitais

Para falarmos acerca das tecnologias digitais precisamos, primeiramente, dar um pequeno passo atrás e observar suas "irmãs mais velhas", as tecnologias analógicas.

Garratt (1994) nos mostra que as tecnologias analógicas têm início nos anos 1820, com os experimentos de Oeste, mas que o impulso maior para esse campo de estudo veio com a descoberta da indução eletromagnética, obtida nas pesquisas de Faraday, em 1831. Os conhecimentos trazidos à tona por Faraday permitiram o nascimento da comunicação via rádio e gerou – quase um século depois – o mecanismo de transmissão e recepção de ondas eletromagnéticas desenvolvido independentemente por Nikola Tesla e Guilhermo Marconi. Nascia, ali, o mecanismo analógico de comunicação. Os elementos analógicos admitem fracionamento e somente em condições raras assumem valores inteiros. Entre um valor e outro há infinitos estados (valores) intermediários. É o caso do tempo e do espaço, que podem ser fracionados infinitamente.

Este mecanismo, ainda segundo Garratt (1994), introduziu a possibilidade da comunicação por meio de sinais analógicos. Os transmissores podiam codificar sinais diferentes em pequenas variações das ondas eletromagnéticas. O som é particularmente adequado de ser codificado usando esse método, mas vários outros tipos de sinal podem se beneficiar do mecanismo analógico de codificação. Alguns

exemplos de tipos de informação que são comumente codificados utilizando o mecanismo analógico:

- Som.
- Imagem.
- Imagem em movimento (sinal de televisão).
- Comandos de controle para maquinário.

Os exemplos são muitos, e o mecanismo analógico de comunicação deu início à revolução eletrônica, cujos benefícios colhemos até os dias de hoje.

O mecanismo analógico de comunicação se baseia na manipulação de ondas eletromagnéticas que são, por natureza, entidades analógicas, isto é, contínuas. As curvas geradas por essas ondas são de origem senoidal, ou seja, ondas que suavemente ascendem e descendem sem "quebras", continuamente.

Assimile

Os dispositivos analógicos foram os que proporcionaram a revolução eletrônica.

Curiosamente, Garratt (1994) nos conta que o mecanismo analógico de comunicação foi usado primeiramente para transmitir um sinal que é, em essência, digital: o Código Morse.

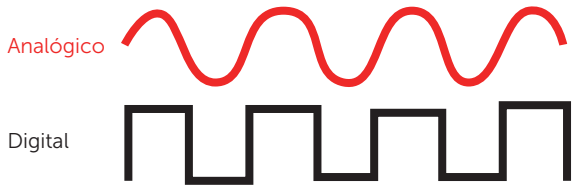
Em 1836, Samuel Morse desenvolveu uma maneira de codificar o alfabeto e sinais de pontuação em um código composto por dois sinais e um separador:

- O "ponto", um sinal de curta duração.
- O "traço", um sinal de longa duração.
- O "silêncio", a ausência de sinal que indica a separação entre palavras.

O Código Morse não admite mudanças suaves entre um sinal e outro; essas mudanças são abruptas, e o sistema permite a existência de apenas esses três elementos. Não existe, por exemplo, variação no "tamanho" do traço. Um sinal ou é um traço ou é um ponto, ou é silêncio (sinal ausente).

Essa é a principal característica do mecanismo digital de comunicação: não há "suavidade" na mudança de um sinal para outro. Os estados possíveis são atingidos de maneira abrupta, sem permitir estados intermediários. A Figura 1.2, a seguir, ilustra a diferença entre um sinal analógico e um sinal digital:

Figura 1.2 | Diferença visual entre sinal analógico e sinal digital



Fonte: elaborada pelo autor.

O termo "digital" vem de "dígito" (dedo, em sua acepção mais simples). É uma medida que varia abruptamente, de um número inteiro para outro, sem as inúmeras fracionárias que temos com, por exemplo, elementos contínuos tais como o tempo (que pode ser fracionado em partições infinitamente pequenas) ou o espaço. Os elementos de característica digital são inteiros e não admitem estados intermediários.

As principais vantagens do mecanismo analógico sobre o digital são:

- Processamento em tempo real dos sinais (no mecanismo analógico há a necessidade de pré-processamento).
- Menos consumo de banda para transmissão de mensagens.
- Custo menor para a transmissão de mensagens.
- Deterioração de sinal por conta de ruídos ainda permite a identificação da mensagem.

Em contrapartida, o mecanismo digital tem as seguintes vantagens:

- Sinal mais imune a ruídos que os sinais analógicos.
- Dispositivos digitais consomem menos energia que seus pares analógicos.
- Dispositivos de eletrônica analógica são mais raros, de mais complexa fabricação e, portanto, são mais caros que seus pares digitais.
- Calibração de dispositivos digitais é mais simples e duradoura (quando necessária, o que muitas vezes não ocorre), enquanto

a calibração de dispositivos analógicos é mais complexa, dura menos e quase sempre é necessária.

No que concerne às tecnologias baseadas em computadores, todas são altamente dependentes dos mecanismos digitais de transmissão de sinais e processamento de dados.

Reflita

Seria possível o desenvolvimento do computador sem a adoção de tecnologias digitais?

Desenvolvimento histórico da computação

Agora que você entendeu os primeiros conceitos sobre as tecnologias digitais, lançamos a você uma pergunta: o que é computar? Segundo Fonseca Filho (2007), computar vai além de calcular; embora obviamente englobe o cálculo, também envolve as ações necessárias para se realizar a avaliação e a resolução de um problema computável qualquer. O autor ainda nos informa que o matemático inglês Alan Turing definiu formalmente quais tipos de problemas são computáveis e, como resultado de suas pesquisas, temos hoje a definição do computador (qualquer computador) como a expressão de uma "Máquina de Turing".

Na prática, ainda segundo o autor, um computador é um dispositivo que consegue resolver problemas lógicos por meio de cálculos matemáticos.

Levando em consideração essa definição, a história dos dispositivos computacionais é bem antiga, antecedendo (e muito) os computadores eletrônicos, mesmo os desenvolvidos no início do século XX.

Um dos primeiros dispositivos computacionais de que se tem notícia é o ábaco, em uso há milhares de anos na Ásia, ilustrado na Figura 1.3.

Figura 1.3 | Ábaco

Fonte: <https://goo.gl/rqWdD2>. Acesso em: 12 set. 2017.

Com o ábaco, o usuário realiza cálculos (isto é, computa resultados) por meio de seu próprio raciocínio e do posicionamento das peças no dispositivo. Pode ser usado tanto para operações simples, tais como somas e subtrações, quanto para cálculos mais complexos, como logaritmos e raízes. É um dispositivo que demanda muito conhecimento do usuário, e podemos argumentar inclusive que quem faz a maioria dos cálculos é esse usuário, sendo que o dispositivo é usado para conter os resultados intermediários e o resultado final.

No século XVII, outro dispositivo mecânico de computação surgiu: a Pascalina, criada pelo matemático francês Blaise Pascal.

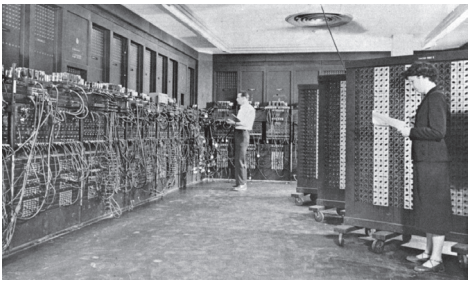
A Pascalina, bem como a "Roda de Leibniz" – essa segunda uma máquina de calcular inventada pelo matemático alemão Gottfried Leibniz no século XVIII – já difere do Ábaco pelo fato de a própria máquina realizar mecanicamente todo o processo de computação, uma vez que o usuário precisa meramente introduzir os dados e operar mecanicamente as manivelas, girando-as.

O dispositivo computacional mecânico que mais se aproxima do computador moderno, a Máquina Diferencial, foi projetado pelo matemático inglês Charles Babbage na primeira metade do século XIX, mas só foi construído efetivamente (apenas como conceito histórico) no fim do século XX. Se tivesse sido construída no tempo de Babbage – que jamais conseguiu levar seus projetos à fruição, ou seja, ao aproveitamento – pode-se argumentar que teríamos a revolução computacional do século XX ocorrendo com um século de antecedência!

Com a evolução da teoria da eletricidade no século XIX e o descobrimento do efeito eletrônico, explorado a partir do início do século XX, os pesquisadores deixaram de lado os dispositivos meramente mecânicos e passaram a explorar componentes elétricos e eletrônicos para construir máquinas dedicadas à computação. O primeiro dispositivo dessa primeira geração de computadores modernos, o Z1, foi projetado e construído pelo engenheiro alemão Konrad Zuse entre 1935 e 1936. Mas certamente o computador mais conhecido dessa época é o ENIAC – sigla que significa Electronic Numerical Integrator and Computer (Integrador e Computador Numérico Eletrônico) –, projetado nos EUA durante a Segunda Guerra Mundial com o objetivo de calcular trajetórias balísticas, mas que só ficou pronto e operacional em 1946. Era um computador composto

por 20 mil válvulas a vácuo que ocupava uma sala de mais de 100m^2, cujo poder computacional é menor que uma calculadora de bolso dos dias atuais. A Figura 1.4, a seguir, ilustra o ENIAC.

Figura 1.4 | O computador ENIAC



Fonte: <https://goo.gl/BY3VYc>. Acesso em: 12 set. 2017.

Os computadores baseados em válvulas a vácuo constituem a primeira geração de computadores eletrônicos, a partir dos quais podemos construir uma tabela com as várias gerações históricas, até chegarmos à geração atual. O Quadro 1.2, a seguir, ilustra as gerações de computadores:

Quadro 1.2 | As cinco gerações de computadores

Geração	Período	Característica	Observações
Primeira Geração	1936-1956	Válvulas e componentes analógicos	Computadores enormes, desenvolvidos pelos governos, para as forças armadas
Segunda Geração	1956-1963	Transistores	Universidades de ponta desenvolvem computadores. Tamanho e consumo de energia diminuem
Terceira Geração	1963-1971	Circuitos integrados	Grandes empresas (bancos, indústrias) adotam computadores
Quarta Geração	1971-presente	Microprocessadores	Revolução digital. Ampla adoção de computadores para uso profissional e pessoal. Miniaturização.
Quinta Geração	Presente-Futuro	SoC (Sistema em um chip, tecnologias ópticas, processador quântico, internet das coisas	Novas tecnologias digitais tendem a levar inteligência artificial a todos os dispositivos e aspectos da vida moderna. O computador desaparece, e fica a inteligência artificial em tudo o que nos cerca.

Fonte: adaptado de Fonseca Filho (2007).

Noções básicas de comandos e algoritmos

Como nos comunicamos com os computadores?

A bem da verdade, o computador só compreende um tipo de linguagem: a linguagem de máquina, composta por "0" e "1". Nada mais. Todas as formas de "falarmos" com o computador, atribuir-lhe comandos, dar-lhe ordens, direcionar-lhe as ações são traduzidas para a linguagem binária. Por isso usamos a expressão "digital binário", ou seja, de apenas dois dígitos definidos.

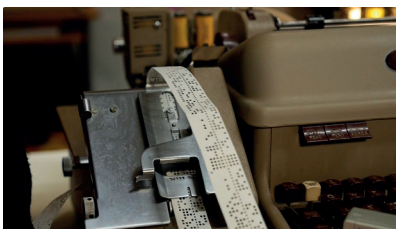
Ocorre que "falar" com o computador usando apenas os símbolos "0" e "1" é inaceitavelmente complexo para nós humanos e é algo que foi feito apenas lá no início da história da computação digital, na primeira geração, e mesmo assim, exclusivamente, porque não tínhamos alternativa.

Muito rapidamente, passamos a criar formas mais adequadas de nos comunicarmos com o computador, e daí surgiram as linguagens de programação. Fonseca Filho (2007) nos aponta esse caráter facilitador das linguagens de programação, já trazendo o computador para mais próximo do ser humano. É claro que uma linguagem de programação é apenas marginalmente palatável, equivalendo a exigir que uma pessoa saiba uma língua estrangeira ao mesmo tempo em que tem conhecimentos robustos de álgebra e lógica, para conseguir falar com um tipo diferente e especial de "estrangeiro" – no caso, esse estrangeiro é o computador.

Exemplificando

Em alguns dos computadores da terceira geração eram usadas longas fitas de papel com o código binário do sistema operacional, que era carregado no momento em que o computador era ligado. Essas fitas continham o código de máquina que o computado compreendia.

Figura 1.5 | Fita com código de máquina



Fonte: <https://goo.gl/YhgVDn>. Acesso em: 13 set. 2017.

O computador entende as linguagens que para ele criamos, mas as traduz todas para a linguagem de máquina, binária, e só por meio dela realiza as ações que dele demandamos. E como o computador é basicamente um "serviçal", não usamos essa linguagem para perguntar o que ele achou do capítulo de ontem da novela: usamos as linguagens para lhe entregar comandos, os quais esperamos que sejam realizados. Ele, por sua vez, não tem nem sentimentos nem consciência e realiza nossos comandos sem questionar. Se pedimos a ele para dividir um número por zero, por exemplo (um absurdo matemático), ele não vai rir de nós nem nos ensinar que está errado: vai simplesmente tentar realizar o comando e nos devolver uma mensagem de erro, dizendo que aquela operação não é possível. Se pedirmos a ele que realize a mesma operação infinitas vezes, ele não vai nos dizer que esta ordem não tem sentido: vai realizar a operação até que interrompamos o processo. Simples assim: o computador realiza, dentro de suas possibilidades, aquilo que o direcionamos a realizar. Em suma, como nos mostra Fonseca Filho (2007), o computador faz o que o mandamos fazer, que nem sempre é o que desejamos que ele faça. Ele consegue ler e realizar os comandos, mas não consegue ler nossas intenções.

Os comandos podem ser encadeados naquilo que chamamos de algoritmos. Os algoritmos são sequências de comandos que realizam uma tarefa mais complexa. Uma analogia interessante para os algoritmos é a receita de bolo: quando vamos fazer um bolo, sacamos a receita na qual encontramos os ingredientes, bem como as instruções sequenciais de como devemos misturar e processar esses ingredientes para obter o resultado desejado: o bolo.

Nesse sentido, um algoritmo, digamos, de ordenação de um conjunto de números, deve conter os insumos necessários para a ordenação (sequência de números desordenados, variáveis de trabalho e repositórios de dados, por exemplo) e uma sequência de comandos que, quando realizados, vão colocar os números em ordem.

Exemplificando

Um exemplo de algoritmo simples é o algoritmo de separação de uma lista de números entre pares e ímpares. Podemos expressar esse algoritmo, em linhas gerais, assim:

1. Tome o próximo número da lista, caso exista (se não existir, termine a execução).

2. Realize uma divisão inteira do número em questão por 2.

3. Se o resto da divisão inteira for "1", coloque o número na bacia dos "ímpares".

4. Caso contrário, coloque o número na bacia dos "pares".

5. Retorne ao passo 1.

Esse algoritmo vai fazer a separação dos números como desejado, pois só há duas possibilidades para o resto: "1", para o caso dos números ímpares, e "0", para o caso dos números pares.

Todo programa de computador, de qualquer tipo de computador (desde os supercomputadores, até os microcontroladores presentes em eletrodomésticos, passando por computadores pessoais, smartphones, tablets, computadores de bordo de automóveis e outros que tais) são implementados com base em algoritmos, isto é, com base em sequências de comandos que visam a atingir objetivos específicos.

Ou seja, sem os algoritmos, não haveria programas de computador e, sem os programas, os computadores seriam apenas pesos de papel caros e pouco eficientes.

Utilização da tecnologia e repercussão social

Você pode observar, segundo Rooksby e Weckert (2006), que o crescimento repentino e amplo das tecnologias de comunicação e processamento de dados levanta questionamentos profundos acerca do significado ético desse crescimento para a sociedade. Se, por um lado, temos a capacidade de reduzirmos ou mesmo de eliminarmos distâncias em função da internet e dos computadores pessoais e smartphones, por outro, não seria aceitável se essas tecnologias fossem utilizadas para aumentar as distâncias entre aqueles que têm recursos que lhes permitem o acesso à tecnologia e aqueles que não têm.

Felizmente, a tecnologia age, nos dias de hoje, como um elemento de nivelação, não impondo grandes barreiras para que todos possam participar de seus benefícios. Já se vai longe o tempo da primeira

geração de computadores, quando, para um destes, fazer operações matemáticas hoje consideradas simples (mas trabalhosas) custava centenas de milhões de dólares. Segundo a Lei de Moore – que é uma lei empírica, observada na indústria de informática, estabelecendo que a cada 18 meses o poder de processamento dos dispositivos dobra, mantendo o mesmo preço –, o que temos é uma difusão das tecnologias digitais pelo mundo afora (NERI et al., 2003).

A cada ano que passa, os dispositivos computacionais ganham em poder de processamento, velocidade e capacidade de armazenamento de informações, e o preço final continua mais ou menos o mesmo. Sim, é verdade que os programas se tornam mais complexos também, exigindo mais poder de processamento e consumindo mais capacidade de armazenamento. Contudo, a complexidade dos programas e a quantidade de dados não crescem com a mesma velocidade dos dispositivos, e esse excedente de processamento acaba permitindo a criação de dispositivos mais baratos, mais acessíveis às populações de baixa renda (NERI et al., 2003).

O melhor exemplo que vemos dessa disseminação é o das tecnologias digitais móveis. Segundo a Folha de S. Paulo (2016), já ultrapassamos, no Brasil, os 168 milhões de aparelhos do tipo smartphone, que essencialmente é um computador com a capacidade de realizar chamadas telefônicas (diferentes dos antigos aparelhos celulares, que não eram capazes de adicionar e executar diferentes programas). Ainda, segundo o artigo, somando-se os aparelhos móveis com os computadores pessoais, já atingimos a densidade de 1,6 dispositivos computacionais para cada habitante do país.

Isso não significa, claro, que não precisamos mais nos preocupar com programas de inclusão digital: de fato, ainda há um contingente apreciável de cidadãos sem acesso digital. O que os dados mostram é que:

- A tecnologia em si vem tendo redução de preço, o que permite cada vez mais o acesso a populações de baixa renda à revolução digital.
- O acesso fácil já pode ser verificado na difusão de aparelhos em uma população tão grande e diversificada como a população brasileira.
- O fato de haver mais pessoas tendo acesso digital pode significar maior chance de usufruto de benesses que a

tecnologia propicia às pessoas, como a facilidade a uma gama de informações e a melhoria no aprendizado, entre outros aspectos.

Enfim, muito trabalho para aumentar o acesso digital ainda tem de ser feito, mas a tecnologia em si não é barreira para isso.

Pesquise mais

Uma das ferramentas mais importantes a serviço da inclusão digital é o software livre. O software livre é aquele software de domínio público, por cujo uso os criadores não cobram, disponibilizando, para isso, suas fontes. Conheça mais sobre o software livre no artigo do pesquisador Sergio Amadeu da Silveira, cujo link é apresentado a seguir por Silveira (2003):

Inclusão digital, software livre e globalização contra hegemônica. Disponível em: <http://files.lnandrade.webnode.com/200000338-b6087b8f60/Inclusaodigital_1.pdf>. Acesso em: 13 set. 2017.

Sem medo de errar

Com o objetivo de auxiliar os funcionários da prefeitura de Paraconé-Açu a compreender melhor os fundamentos acerca do computador e da tecnologia da informação, você poderá resumir os conceitos básicos em sua cartilha, apresentando os assuntos da seguinte maneira:

PREFEITURA MUNICIPAL DE PARACONÉ-AÇU 2017
CARTILHA DE ASPECTOS BÁSICOS DA TECNOLOGIA DA INFORMAÇÃO
Caro colaborador, esta cartilha tem por finalidade apresentar aspectos que facilitem o seu entendimento sobre a tecnologia da informação e comunicação. Procure entender alguns importantes significados. ***Lembre-se:*** • Os dispositivos computacionais não são nada novos, uma vez que, na antiguidade, já tínhamos ábacos e ferramentas mecânicas semelhantes para ajudar na realização de cálculos matemáticos • Esses dispositivos mecânicos cresceram em complexidade, entre os quais podem ser citados:

- ◊ Pascalina – dispositivo mecânico de contas aritméticas criado pelo matemático francês Blaise Pascal.
- ◊ Roda de Leibniz – dispositivo complexo para cálculos aritméticos avançados criado pelo matemático alemão Gottfried Leibniz.
- ◊ Máquina Diferencial – computador digital mecânico projetado (mas nunca construído) por Charles Babbage.

- Os computadores modernos começaram a ser possíveis a partir dos estudos da eletricidade e do magnetismo, em pesquisas extensas realizadas no século XIX e no início do século XX.
- Hoje em dia, os computadores são, historicamente, divididos em cinco gerações:

  - ◊ **Primeira Geração** – computadores feitos com válvulas a vácuo. Desenvolvidos especificamente com fins militares (cálculo de trajetória de obuses durante a Segunda Guerra) eram enormes e consumiam grandes quantidades de energia. O ENIAC é um dos exemplos mais clássicos de computadores da primeira geração
  - ◊ **Segunda Geração** – computadores feitos com transistores. Já eram menores e consumiam menos energia, mas ainda assim eram de baixíssima capacidade se comparados a computadores modernos
  - ◊ **Terceira Geração** – computadores feitos com base em circuitos integrados: a integração de vários transistores e outros componentes em um único *chip* adicionou muita velocidade e reduziu bastante os custos dos computadores. Foi a partir da terceira geração que começaram a se popularizar na indústria e nas grandes empresas financeiras.
  - ◊ **Quarta Geração** – computadores feitos com microprocessadores. De certa forma, ainda vivemos esta geração, uma vez que nossos computadores são, de fato, baseados em microprocessadores. Essa geração popularizou os computadores em meio ao público em geral, melhorou bastante as interfaces de software (por meio das quais interagimos com os computadores) e barateou os dispositivos, tornando-os acessíveis à população.

- ◊ **Quinta Geração** – computadores baseados em SoC (System on a Chip: essencialmente todos os componentes em um único chip), tecnologias ópticas, chips quânticos e novas tecnologias em desenvolvimento. Representam o futuro dos computadores. Os SoC possibilitam a revolução da computação móvel que vivemos nos dias de hoje.

- Os computadores só conhecem, em termos de linguagem, a linguagem de máquina, baseada em "0" e "1".
- Todas as demais linguagens de programação devem ser traduzidas para o código de máquina antes de serem executadas pelo computador.
- As instruções que passamos ao computador são chamadas de comandos.
- Um conjunto de comandos que realiza uma tarefa ou gera um resultado mais complexo se chama "algoritmo", que é comparável a uma receita para se produzir um resultado.

Pronto, agora os funcionários da prefeitura já têm a base necessária para o desenvolvimento dos próximos conteúdos!

Avançando na prática

"Solução dos sonhos" versus "solução possível"

Descrição da situação-problema

Sandroval Xerxes, um jovem de baixa renda que, com muito esforço e empenho, formou-se em um curso de tecnologia da informação (TI). Seu sonho era empreender um negócio próprio, criando uma empresa de entregas com o apoio da tecnologia da informação para planejamento e operação de seus trabalhos.

Ao confeccionar o plano de negócios, veio a decepção: os custos para aquisição do equipamento mais moderno (que era seu sonho) e, sobretudo, do software necessário para executar as tarefas demandadas excediam (em várias ordens de grandeza) os valores que Sandroval tinha disponíveis, os quais eram substancialmente insuficientes para a aquisição da solução desejada.

Diante desse dilema, Sandroval ligou para você, um renomado consultor que conhece bastante soluções de TI, para pedir ajuda. E,

então, há alguma solução para a dificuldade em que Sandroval se encontra? Há alternativa para fazer um empréstimo a juros altos e pagar pela solução "dos sonhos"?

Resolução da situação-problema

O problema apresentado por Sandroval não é novo nem único. Na verdade, muitas empresas em início de atividade sonham mais alto do que conseguem realizar em termos de investimentos. Você sabe muito bem disso, e sabe também que há oportunidades fora do "melhor do melhor". Há equipamentos e alternativas de software que resolvem os problemas de TI de uma empresa sem estarem no topo de linha (que geralmente estão no topo dos preços também).

No que concerne à máquina em si, Sandroval não precisa do hardware mais novo. Uma máquina de dois ou três anos de uso vai custar muito mais barato, vai ser um pouco mais lenta, mas com um complemento de memória e disco vai oferecer o desempenho que se espera, por uma fração do custo.

Quanto ao quesito sistema operacional, o software básico que faz a máquina funcionar, você pode sugerir ao Sandroval o uso do Linux, que é programa de código aberto e gratuito para uso. Trata-se de um sistema operacional de primeiríssima qualidade pelo melhor dos preços: zero.

Quanto ao software em si, em vez de comprar uma solução "de grife", Sandroval poderá buscar o apoio de uma empresa local de desenvolvimento que, a partir de uma entrevista com o empreendedor, consegue criar um algoritmo e dele gerar um programa que realiza as funções desejadas. Assim, Sandroval consegue seu sistema e, ao mesmo tempo, economiza muito dinheiro, que poderá investir em outras áreas da empresa nascente.

E, depois de seu negócio "decolar", começando a faturar e a gerar lucro, ele poderá investir no sistema de seus sonhos sem precisar contrair empréstimos a juros altos.

Faça valer a pena

1. Observe o texto a seguir:
Nossa relação com a tecnologia teve início no momento em que o primeiro hominídeo tomou em sua mão uma pedra para usar como ferramenta em

alguma tarefa qualquer. Por mais que hoje não associemos as palavras "pedra" e "tecnologia", naquele longínquo momento da aurora da humanidade, estávamos buscando fora de nós mesmos algo que nos auxiliasse a ganhar vantagem na luta contra o ambiente que nos cercava.

De acordo com o texto anterior, quando começou o desenvolvimento tecnológico da humanidade?

a) Na Idade Média, sob tutela da Igreja.
b) No Renascimento, quando voltamos a pensar cientificamente.
c) Na Idade da Pedra, quando passamos a manipular ferramentas rudimentares.
d) No Iluminismo, quando a filosofia permitiu voos mais altos do pensamento humano.
e) Na Revolução Industrial, quando passamos a automatizar os processos produtivos.

2. Com a evolução da teoria da eletricidade no século XIX e o descobrimento do efeito eletrônico, explorado a partir do início do século XX, os pesquisadores deixaram de lado os dispositivos meramente mecânicos e passaram a explorar componentes elétricos e eletrônicos para construir máquinas dedicadas à computação.

Com a evolução da computação digital de uma geração para a seguinte, é correto afirmar que:

a) O poder computacional cresce, o consumo de energia cresce, os custos crescem.
b) O poder computacional diminui, o consumo de energia diminui, os custos diminuem.
c) O poder computacional diminui, o consumo de energia diminui, os custos crescem.
d) O poder computacional cresce, o consumo de energia diminui, os custos diminuem.
e) O poder computacional cresce, o consumo de energia cresce, os custos diminuem.

3. Observe o algoritmo a seguir:
1. Leia idade da pessoa
2. Se idade for maior ou igual a dezoito anos, responda "sim"
3. Caso contrário, responda "não"
Imagine que esse algoritmo seja transformado em um programa de computador a ser usado para resolver um tipo de problema específico.

O algoritmo mencionado pode ser utilizado para:

a) Identificar se a pessoa é do sexo feminino ou masculino.
b) Identificar se a pessoa está na idade de aposentadoria ou não.
c) Identificar se a pessoa é brasileira ou estrangeira.
d) Identificar se a pessoa está apta a dirigir um automóvel.
e) Identificar se a pessoa tem o direito de requisitar uma carteira nacional de habilitação.

Seção 1.3

Introdução à TIC

Diálogo aberto

Começamos nosso estudo entendendo os fundamentos da democracia, da cidadania e da segurança pública. Esses conceitos são sempre os alicerces para estudos que envolvem nossa sociedade, como é o caso em tecnologias aplicadas aos sistemas de segurança.

Em seguida, mergulhamos na história das tecnologias digitais, entendendo como se deu seu desenvolvimento até os dias atuais.

A partir de agora, vamos nos aprofundar em dois assuntos que são fundamentais no contexto de tecnologia digital: as teorias da comunicação e da informação. Vamos ver os seus fundamentos, a questão da infraestrutura da tecnologia da informação, bem como as diferenças e semelhanças desta para com os sistemas de informação.

Você já percebeu que tudo o que nos cerca nos dias de hoje é absolutamente dependente da comunicação e da informação? Nós nos comunicamos sem parar o dia todo, profissional e pessoalmente. E em nossas comunicações o bem mais precioso é a informação que é transmitida e recebida. Esse quadro tem evoluído desde que o primeiro ser foi capaz de transmitir informação ao seu semelhante, mas nunca na história da humanidade tivemos tanta facilidade de comunicação nem tanto acesso à informação quanto nos dias de hoje. As facilidades providas pela tecnologia da informação e da comunicação reduzem distâncias de comunicação e facilitam o acesso à informação como em nenhuma outra época foi possível.

Retomando o nosso contexto de aprendizagem, dando sequência à preparação para a informatização da prefeitura de Paraconé-Açu, agora que todo o pessoal envolvido já conhece um pouco mais sobre as possibilidades da informática e está reciclado nos conceitos de democracia, cidadania, segurança pública e inclusão digital, é hora de aprenderem sobre informação e comunicação, conceitos básicos para os sistemas de informação. Os sistemas informatizados permitem que o usuário credenciado tenha acesso a informações sigilosas, sensíveis,

ou simplesmente pessoais. O acesso a essas informações e também seu uso são alicerçados sobre os conceitos da teoria da comunicação e da teoria da informação. Esses conceitos são fundamentais aos funcionários da Prefeitura de Paraconé-Açu para que possam começar a compreender os conceitos dos sistemas de informação. Lembrando que vamos apresentar ao final desta seção e unidade uma cartilha com os fundamentos da TIC. Nessa etapa da composição da cartilha, você deverá incluir uma seção que verse sobre os conceitos principais da teoria da comunicação e seus principais conceitos, bem como sobre a teoria da informação e seus principais conceitos. Em seguida, deverá fazer a ligação entre esses conceitos e o setor de TIC, hoje tão importante à nossa nação, bem como fazer uma ligação desses conceitos com os sistemas de informação.

Vamos, então, ao trabalho? Em frente!

Não pode faltar

Comunicação e informação: dois pilares da sociedade moderna. O mundo que nos cerca depende profundamente desses dois conceitos e da tecnologia que os operacionaliza.

A partir de agora, vamos entender como funcionam e como eles dão apoio aos sistemas de informação, em especial os sistemas de segurança.

Introdução à teoria da comunicação

Shannon (1948), em seu artigo seminal sobre o qual se alicerça toda a teoria moderna da comunicação, define comunicação como o ato de se transmitir significados intencionais de uma entidade ou grupo para outra entidade ou grupo, utilizando-se de sinais mutuamente compreendidos e regras para interpretação desses sinais.

Os elementos que compõem o processo de comunicação são (SHANNON, 1948):

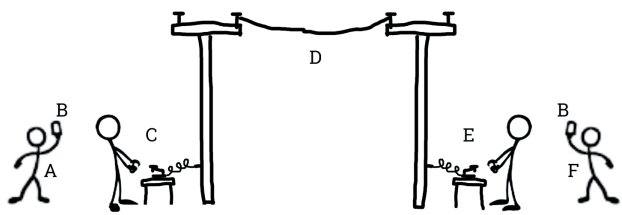
- **Fonte** – (também chamado de remetente) elemento que produz a mensagem sendo comunicada. Representado por "A" na Figura 1.6
- **Emissor** – (também chamado de transmissor) é o elemento que opera sobre a mensagem de alguma forma, transformando-a

em um formato adequado (sinal) para que atravesse o canal de comunicação, e a submete a esse canal de comunicação, provocando seu tráfego. Representado por "C" na Figura 1.6.

- **Sinal** – conjunto de códigos que traduzem a mensagem de forma que possa trafegar adequadamente pelo canal.
- **Canal** – meio utilizado para o tráfego do sinal que compõe a mensagem. Representado por "D" na Figura 1.6.
- **Receptor** – elemento que transforma o sinal de volta ao formato original, reconstruindo a mensagem. Representado por "E" na Figura 1.6.
- **Destino** – (também chamado de destinatário) elemento para o qual se tem a intenção de que a mensagem chegue. Representado por "F" na Figura 1.6.
- **Mensagem** – conceito (ou informação) gerado pela fonte e que esta deseja ser do conhecimento do destino. Representado por "B" na Figura 1.6.
- **Ruído** – situação inerente ao canal que adiciona à mensagem elementos não intencionados pela fonte e que tendem a confundir-se com o sinal, deteriorando a qualidade deste.

A Figura 1.6, a seguir, representa graficamente alguns desses conceitos:

Figura 1.6 | Representação dos elementos da comunicação



Fonte: elaborada pelo autor.

É importante observar que, como representado na Figura 1.6, a mensagem enviada pelo remetente (B) deve ser idêntica à mensagem recebida pelo destinatário (também B). Outro ponto interessante é que todo o aparato de emissão (equipamento mais operador) é chamado de "transmissor". De maneira análoga, todo o aparato de recepção (equipamento mais operador) é chamado de "receptor".

Os canais de comunicação podem variar bastante, dependendo do tipo de sinal e do equipamento de transmissão/recepção desse sinal. Os exemplos mais comuns são:

- **Ar** – bastante utilizado para a comunicação falada entre pessoas em um mesmo ambiente. Os equipamentos de transmissão e recepção sonoros são adequados para utilizar esse meio. Cordas vocais e alto-falantes são exemplos de elementos de transmissão; e ouvidos são exemplos de elementos de recepção.
- **Espaço (vácuo)** – bastante utilizado para a comunicação de sinais eletromagnéticos. Antenas são utilizadas tanto para a transmissão quanto para a recepção dos sinais.
- **Cabeamento metálico** – usado na telefonia para a comunicação dentro de edificações. No passado, era usado em todo o caminho da mensagem, tendo sido um meio substituído pelo espaço e pela fibra óptica em quase todo esse caminho, em função de custos e eficiência.
- **Fibra óptica** – usada amplamente nos dias de hoje para telecomunicações, tanto em longa distância quanto em regiões metropolitanas (dentro de uma cidade). Meio mais rápido, mais barato e mais imune aos ruídos que o cabeamento metálico.

Pesquise mais

O livro *Os meios de comunicação como extensões do homem*, de Marshall Ocluam, foi escrito em 1964 e ainda hoje é uma obra seminal sobre comunicação, seus aspectos técnicos e suas implicações para a vida moderna. O capítulo "O meio é a mensagem" contém uma discussão acerca de como o meio de comunicação influencia todo o processo de comunicação, determinando o significado da mensagem. O livro foi escrito décadas antes da internet, e esse capítulo ainda continua sendo tão relevante e preciso como se tivesse sido escrito ontem.

MCLUHAN, M. **Os meios de comunicação como extensões do homem**. 3. ed. São Paulo: Cultrix, 1964.

Fundamentos da tecnologia da informação

A definição de "mensagem" oferecida por Shannon (1948) nos mostra que ela é o objeto a ser comunicado, o elemento fim do

processo de comunicação. A mensagem é a informação que o remetente pretende que seja de conhecimento do destinatário.

De acordo com Shannon (1948), a informação é o significado da mensagem, ou seja, o dado ou conhecimento que se deseja transmitir na mensagem. Para esse autor, o problema fundamental da comunicação — quando analisamos o assunto na perspectiva quantitativa — é a reprodução da mensagem no ponto de destino de maneira exata ou aproximada, de forma que a informação original seja preservada.

Um experimento simples permite que você compreenda esse conceito de informação e da preservação do significado de uma mensagem. Tome um texto qualquer impresso em papel, podendo ser colorido ou todo preto e branco. Leve esse papel a uma máquina de fotocópia e faça o seguinte: tire uma cópia do papel original e, em seguida, use-a para fazer outra cópia. Depois use a segunda cópia para fazer uma terceira, use a terceira para fazer uma quarta, e assim por diante. Como a máquina de fotocópia é um meio imperfeito de transmissão da mensagem (mensagem essa que é transmitida de um papel para outro), aos poucos vão sendo inseridos ruídos — imperfeições — nas cópias, os quais vão sendo ampliados de uma cópia para outra. Em pouco tempo os ruídos deixam de ser imperceptíveis e passam a ser bastante visíveis, porém, mesmo nesses casos, a mensagem é legível e compreensível. Ocorre que, se o processo é repetido muitas vezes, em algum momento a legibilidade da mensagem fica comprometida, e essa mensagem se perde.

A teoria da informação se preocupa não só com a quantificação da informação, como também com os aspectos inerentes à sua comunicação, a preservação de significado, o armazenamento e a possível compressão sem perda de significado (HOLLOS; HOLLOS, 2015).

Nos contam Hollos e Hollos (2015) que um sistema simples de comunicação (e aqui não estamos falando de um sistema de comunicação no sentido de um programa de computador que processa informações, mas sim de um sistema teórico em que ocorre/existe a informação em sua forma mais simples), quanto maior é a quantidade possível de mensagens, mais informação temos a respeito do sistema. Para ilustrar, tomemos uma situação hipotética: queremos atravessar uma área quadrada de 8 km x 8 km (64 km^2). Temos apenas

uma informação sobre essa área: em algum lugar ali, há um tigre selvagem. A Figura 1.7 a seguir representa esta situação:

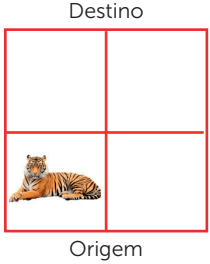
Figura 1.7 | Situação com apenas uma informação possível (uma mensagem)

Fonte: elaborada pelo autor.

Podemos afirmar que temos pouca informação sobre o caso, pois a informação é genérica demais: em uma área de 8 km x 8 km, a presença de um tigre é preocupante, pois corremos o risco de começar a andar e dar de cara com a fera.

Agora imaginemos que no mesmo ambiente há quatro estados possíveis: o tigre pode estar em um dos quatro quadrantes de 4 km x 4 km e sabemos que quadrante é esse. A Figura 1.8, a seguir, ilustra esse conceito:

Figura 1.8 | Situação com quatro informações possíveis (quatro possíveis mensagens)



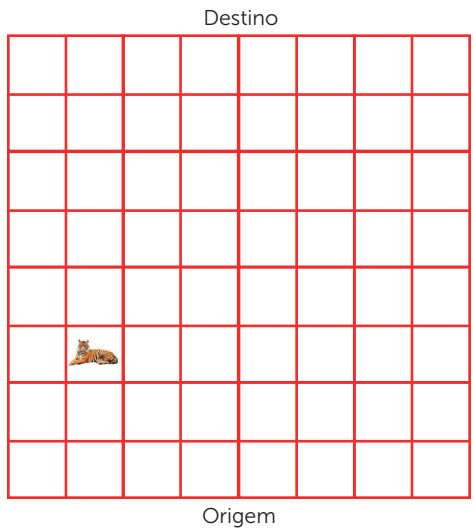
Fonte: elaborada pelo autor.

Nessa segunda situação, já temos algo de mais favorável para cruzarmos a região. Mesmo que o tigre esteja perto do meio, podemos realizar o trajeto bem próximos ao canto direito, onde teríamos uma chance. Ademais, o tigre pode estar bem próximo ao canto esquerdo, em cuja situação corremos menos risco ainda. O problema é que, se chega uma nova informação de que o tigre está no quadrante que

ocupamos, podemos ter um problemão: ele pode estar próximo e só descobrirmos isso quando for tarde demais. Com quatro estados possíveis, esse sistema nos dá mais informação, mas ainda assim pode não ser suficiente.

Um último caso: agora temos informação sobre cada quilômetro quadrado e sabemos em qual deles o tigre se encontra. A Figura 1.9 ilustra essa situação:

Figura 1.9 | Situação com quatro informações possíveis (quatro possíveis mensagens)



Fonte: elaborada pelo autor.

Aqui temos uma situação bem mais favorável, não é verdade? Sabemos onde o tigre se encontra com maior precisão. Como o sistema tem 64 informações possíveis, saber que o tigre se encontra mais à esquerda nos permite uma decisão bem mais segura, pois, seguindo pelo canto direito e monitorando a posição do tigre, podemos cruzar o terreno com mais segurança. Ademais, se vem outra informação de que o tigre mudou de quadrante, podemos saber em que direção ele está se movendo e assim ajustar nosso curso de acordo.

Em outras palavras: o exemplo acima nos mostra que o valor de uma informação é diretamente proporcional à quantidade possível de informações que um sistema pode nos dar (HOLLOS; HOLLOS, 2015).

Reflita

Hipoteticamente, se você estivesse diante de um pirata que escondeu um tesouro e pudesse fazer-lhe uma pergunta apenas, com a garantia de que lhe diria a verdade, você faria uma pergunta simples na expectativa de uma resposta sim/não ou faria uma pergunta mais elaborada na expectativa de uma resposta específica? Por quê?

Além desse aspecto básico, são características da informação:

- **Disponibilidade/acessibilidade** – facilidade de obtenção e acesso à informação.
- **Acurácia** – a informação deve ser acurada para o uso que dela se pretende fazer, ou seja, deve ser exata.
- **Objetividade** – o quanto uma informação é baseada em fatos, e não em elementos subjetivos, tais como opiniões.
- **Relevância** – o quanto uma informação está em linha com o assunto que está sendo discutido/processado.
- **Completude** – o quanto uma informação é, em si, completa, não tendo porções faltantes que sejam necessárias ao contexto a que se aplica.
- **Nível de detalhe/concisão** – o quanto uma informação é detalhada ou, opostamente, concisa; essas duas características são opostas e têm valor diferente (e igualmente oposto) dependendo da situação.
- **Timing** – função de utilidade da informação com base no momento em que está disponível; uma informação crucial a uma transação que está sendo realizada hoje mas que só estará disponível amanhã tem baixo *timing*, enquanto uma informação crucial para uma transação que será realizada amanhã mas que já está disponível hoje tem alto *timing*.
- **Custo** – quanto custa para uma fonte gerar uma informação.
- **Valor** – o quanto uma informação vale para um destinatário.

A tecnologia da informação (TI) é, segundo Planta e Murrell (2007), a aplicação de computadores no armazenamento, recuperação, processamento, transmissão, recepção e

manipulação de dados e/ou informações, o mais das vezes em um contexto profissional. É um subconjunto das TICs, ou tecnologias da informação e da comunicação.

Os autores nos informam que a TI é comumente confundida com computadores, redes e área profissional de informática de uma organização qualquer, e que esse uso (errôneo) vem sendo consagrado após décadas de uso.

É a TI a responsável pelos seguintes elementos acerca da informação dentro de uma organização:

- Aquisição da informação.
- Transporte da informação.
- Armazenamento e recuperação da informação (inclui a compressão dos dados para armazenamento otimizado).
- Segurança da informação.
- Ordenação e processamento da informação.

Exemplificando

O quesito completude é um dos mais importantes no que concerne à informação. Quando precisamos das informações pessoais de um indivíduo e temos apenas seu nome e sua identidade, temos o básico, mas a informação está longe de ser completa. Quando temos, além disso, seus dados naturais e fisiológicos (data de nascimento, peso, altura, nome dos pais, naturalidade, cor etc.), já temos mais informações que nos ajudam a avaliar o indivíduo. Contudo, ainda estão incompletas.

Se, indo mais à frente, adicionamos seus dados de residência, formação acadêmica e histórico profissional, estamos detalhando mais ainda.

É suficiente? Depende do propósito. Para uma ficha de empregos talvez seja, mas, para o Imposto de Renda, a informação estaria incompleta (faltam dados financeiros e de movimentação econômica do período).

O quanto uma informação está completa ou incompleta, em suma, depende do propósito da informação.

Infraestrutura da tecnologia da informação

A tecnologia da informação depende de uma infraestrutura própria para lidar com as informações de uma organização. Essa infraestrutura

é formada, basicamente, por três classes de elementos (PLANT; MURRELL, 2007):

- **Hardware** – equipamento tangível cujo principal propósito é o processamento de informações ou o apoio periférico a esse processamento. Exemplos: computadores, tablets, smartphones, servidores, desktops, laptops, notebooks, ultrabooks (todos dispositivos de processamento). Temos também, na subcategoria de periféricos: impressoras, mouses, teclados, monitores, scanners, *plotters*, leitores de código de barra, discos externos, pen drives, entre vários outros.
- **Softwares** – programas de computador, elementos intangíveis que se utilizam do hardware para realizar o processamento e a manipulação em geral dos dados. Fazem parte dessa subcategoria os sistemas operacionais (exemplos: Windows, MacOS, Linux), os *device drivers* (programas básicos e ocultos, usados para permitir que peças ou dispositivos de hardware conversem entre si e possam ser integrados), os programas de uso final.
- **Redes** – dispositivos tangíveis cujo propósito principal é a comunicação de dados. Incluem roteadores, *switches*, *hubs*, modems, cabeamento, *hot-spots* e antenas wi-fi, repetidores de sinal, entre outros.

A infraestrutura de TI deve ser administrada como qualquer outro recurso de uma organização (ou mesmo de um lar), sob pena de não ser tão eficiente quanto se espera e de não gerar os resultados de otimização que um ambiente de TI pode oferecer quando bem operado e administrado.

Diferenças e semelhanças de sistemas de informação e tecnologia de informação

Depois que você pôde entender os conceitos sobre informação e tecnologia da informação, vamos deixar bem claras as suas diferenças e semelhanças. Kroenke (2015) nos informa que um sistema de informação é um grupo de componentes de hardware, software e redes que interagem de forma a coletar e processar dados, transformando-os em informações e conhecimentos que sejam úteis a um indivíduo e/ou a uma organização para um propósito (ou conjunto de propósitos) específico.

Nesse sentido, o sistema de informação difere da tecnologia da informação nos seguintes aspectos:

- **Abrangência** – enquanto a TI é abrangente, englobando e se espalhando por toda uma organização, um sistema de informação é restrito, contido, limitado
- **Propósito** – a TI a visa atender a todos os aspectos de uma organização que necessitem de processamento de informações, de maneira genérica. Já os sistemas de informação têm propósito definido, sendo desenvolvidos e implantados para atingir um determinado propósito dentro da organização

Podemos afirmar, com base nesse contexto, que um sistema de informação é um subconjunto da infraestrutura de TI de uma organização. Trata-se de um subconjunto que tem por propósito resolver um problema bem definido dentro da organização.

Assimile

Um sistema de informação é um subconjunto da infraestrutura de TI da organização.

Sem medo de errar

A Prefeitura de Paraconé-Açu, em franco processo de informatização, aguarda o próximo passo de sua consultoria. Nesse momento, você vai inserir na cartilha os conceitos básicos de comunicação, informação e vai terminar com a caracterização de sistemas de informação.

A cartilha poderá ser assim estruturada:

PREFEITURA MUNICIPAL DE PARACONÉ-AÇU 2017
CARTILHA DE ASPECTOS BÁSICOS DA TECNOLOGIA DA INFORMAÇÃO
2ª PARTE
• Comunicação ◊ **Fonte** – (também chamado de remetente) elemento que produz a mensagem sendo comunicada.

- ◊ **Emissor** – (também chamado de transmissor) é o elemento que transforma a mensagem em um formato adequado (sinal) para que atravesse o canal de comunicação.
- ◊ **Sinal** – conjunto de códigos que traduzem a mensagem de forma que esta possa adequadamente trafegar pelo canal.
- ◊ **Canal** – meio utilizado para o tráfego do sinal que compõe a mensagem.
- ◊ **Receptor** – elemento que transforma o sinal de volta ao formato original, reconstruindo a mensagem.
- ◊ **Destino** – (também chamado de destinatário) elemento ao qual tem-se a intenção de que a mensagem chegue.
- ◊ **Mensagem** – conceito (ou informação) gerado pela fonte e que esta deseja ser do conhecimento do destino.
- ◊ **Ruído** – situação inerente ao canal que adiciona à mensagem elementos não intencionados pela fonte, os quais tendem a confundir-se com o sinal, deteriorando a qualidade deste.

- Informação
  - ◊ **Informação** – significado da mensagem.
    Tem mais valor a informação que faz parte de um conjunto maior de possibilidades de informações.
  - ◊ **Características**
  - ◊ **Disponibilidade/acessibilidade** – facilidade de obtenção e acesso à informação.
  - ◊ **Acurácia** – a informação deve ser acurada para o uso que dela se pretende fazer, ou seja, deve estar exata.
  - ◊ **Objetividade** – o quanto uma informação é baseada em fatos, e não em elementos subjetivos, como opiniões
  - ◊ **Relevância** – o quanto uma informação está em linha com o assunto sendo discutido/processado.
  - ◊ **Completude** – o quanto uma informação é, em si, completa, não tendo porções faltantes que sejam necessárias ao contexto a que se aplica.
  - ◊ **Nível de detalhe/concisão** – o quanto uma informação é detalhada ou, opostamente, concisa.
  - ◊ **Timing** – função de utilidade da informação com base no momento em que está disponível.

- ◊ **Custo** –quanto custa para uma fonte gerar uma informação.
- ◊ **Valor** – o quanto uma informação vale para um destinatário.

- **Tecnologia da informação**
- **Definição** – aplicação de computadores no armazenamento, recuperação, processamento, transmissão, recepção e manipulação de dados e/ou informações, o mais das vezes em um contexto profissional.
  É um subconjunto das TICs, ou tecnologias da informação e da comunicação.
  Responsável pelos seguintes elementos acerca da informação dentro de uma organização:
  - Aquisição da informação.
  - Transporte da informação.
  - Armazenamento e recuperação da informação (inclui a compressão dos dados para armazenamento otimizado).
  - Segurança da informação.
  - Ordenação e processamento da informação.
- ◊ Infraestrutura composta por:
  - Hardware.
  - Software.
  - Redes.

Avançando na prática

Informação de pouco valor

Descrição da situação-problema

A Rennaissance, uma empresa internacionalmente renomada de restauração, foi contratada pela Cúria Diocesana de Florença, na Itália, para a restauração do piso da Catedral Domo di Firenze, no centro da cidade. A Rennaissance pediu informações acerca da Igreja para poder planejar matérias-primas e cursos, tendo recebido o seguinte da Cúria:

- Localização: 43°46'23.1" de latitude norte, 11°15'22.4" de longitude leste;
- Ano de início das obras: 1296.
- Ano de inauguração/consagração: 1436.

- Estilo: gótico italiano e renascentista;
- Arquitetos: Arnolfo di Cambio, Filippo Brunelleschi, Emilio de Fabris.

Então, você considera que essas informações têm valor para o trabalho de Rennaissance? Se há alguma deficiência, qual das características inerentes à informação elas deixam de lado? Que outras informações seriam úteis ao trabalho da Rennaissance?

Resolução da situação-problema

As informações prestadas são de relativa utilidade ou, em alguns casos, de pouca utilidade para que a Rennaissance realize seu trabalho de restauração do piso da Catedral de Florença.

De todas as informações prestadas, apenas o estilo e talvez os nomes dos arquitetos tenham algum valor para o trabalho a ser feito. O estilo ajudaria na definição de tipos de materiais e técnicas de restauração, e o nome dos arquitetos ajudaria no estudo de obras semelhantes, com vistas a entender o direcionamento da obra.

As demais informações, porém, pecam no quesito ***relevância***. São precisas, pertinentes à obra em si e apresentam boa acurácia. Mas, no tocante à relevância, deixam muito a desejar.

Ocorre que, para o cálculo de materiais e para o planejamento do trabalho, seriam fundamentais as dimensões do piso da Catedral, a planta dessa obra (com vistas a planejar entrada de material e equipamentos, e a saída de resíduos e entulhos) e uma planta dos arredores do edifício, com vistas à logística da obra.

Quando prestamos informações a quem nos solicita, é fundamental considerarmos a relevância das informações prestadas, sob pena de cometermos o erro da Cúria Diocesana de Florença, nesse caso.

Faça valer a pena

1. Podemos definir comunicação como o ato de se transmitir significados intencionais de uma entidade ou grupo para outra entidade ou grupo, utilizando-se de sinais mutuamente compreendidos e regras para interpretação desses sinais.

Analise cuidadosamente as afirmações a seguir e depois assinale a alternativa

CORRETA:
I. O emissor é o elemento que produz a mensagem sendo comunicada.
II. O sinal é o meio utilizado para o tráfego.
III. O receptor é o elemento que transforma o sinal de volta ao formato original, reconstruindo a mensagem.
IV. A mensagem é o conceito (ou informação) gerado pela fonte e que esta deseja ser do conhecimento do destino.
São verdadeiras as afirmações:

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

2. Observe a definição a seguir, de um meio de comunicação:
"Bastante utilizado para a comunicação falada entre pessoas em um mesmo ambiente. Os equipamentos de transmissão e recepção sonoros são adequados para utilizar esse meio. Cordas vocais e alto-falantes são exemplos de elementos de transmissão; e ouvidos são exemplos de elementos de recensão".

O texto anterior se refere a qual meio pelo qual propagamos mensagens e, em essência, nos comunicamos?

a) Ar.
b) Vácuo.
c) Cabeamento metálico.
d) Cabeamento estruturado.
e) Fibra óptica.

3. Observe as asserções a seguir:
I. Quanto maior for o nível de detalhes inerentes a uma informação qualquer, menor será seu grau de concisão.
PORQUE
II. O nível de detalhe de uma informação é um conceito oposto ao nível de concisão desta mesma informação.

Analise as asserções anteriores e a relação entre elas e assinale a alternativa CORRETA:

a) I e II são verdadeiras, porém II não justifica I.
b) I e II são verdadeiras, e II justifica I.
c) I é verdadeira, e II é falsa.
d) I é falsa, e II é verdadeira.
e) I e II são falsas.

Referências

BOTELHO, A.; SCHWARCZ, L. M. **Cidadania, um projeto em construção**. São Paulo: Claro Enigma, 2013.

BRASIL. Câmara dos Deputados, **Constituição da República Federativa do Brasil de 1988**. Brasília: Planalto, 2016a. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 23 ago. 2017.

_____. Tribunal Superior Eleitoral, **Urna eletrônica:** 20 anos a favor da democracia. Brasília: Tribunal Superior Eleitoral, 2016b. Disponível em: <http://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/urna_eletronica/livreto-urna-programa-educativo_web.pdf>. Acesso em: 26 ago. 2017.

_____. Ministério da Ciência, Tecnologia e Inovação, **Inclusão digital**. Brasília: MCTI, 2016c. Disponível em: <https://www.governoeletronico.gov.br/eixos-de-atuacao/cidadao/inclusao-digital>. Acesso em: 28 ago. 2017.

CALLON, M.; LASCOUMES, P.; BARTHE, Y. **An essay on technical democracy**. Boston: MIT Press, 2001.

CHURCHILL, W. **Discurso na Câmara dos Comuns**. The Official Report, House of Commons (5th series, v. 444, p. 203-321), 11 nov. 1947. Disponível em: <http://hansard.millbanksystems.com/commons/1947/nov/11/parliament-bill#column_206>. Acesso em: 24 ago. 2017.

FOLHA DE S. PAULO. Número de smartphones em uso no Brasil chega a 168 milhões, diz estudo. **Folha de S. Paulo**, São Paulo, 15 abr. 2016, caderno Mercado, p. 1. Disponível em: <http://www1.folha.uol.com.br/mercado/2016/04/1761310-numero-de-smartphones-em-uso-no-brasil-chega-a-168-milhoes-diz-estudo.shtml>. Acesso em: 13 set. 2016.

FONSECA FILHO, C. **História da computação:** o caminho do pensamento e da tecnologia. Porto Alegre: EDIPUCRS, 2007.

GARRATT, G. R. M. **The early history of radio**. Londres: IET, 1994.

HOLLOS. S.; HOLLOS, J. R., **Information theory**. Denver: Abrazol Publishing, 2015.

KARASINSKI, L. O que é tecnologia? **Site Tecmundo**, publicado em 29 jul. 2013. Disponível em: <https://www.tecmundo.com.br/tecnologia/42523-o-que-e-tecnologia-.htm>. Acesso em: 11 set 2017.

KROENKE, D. **MIS Essentials**. 4. ed. Boston: Pearson, 2015.

NERI, M. et al. Lei de Moore e políticas de inclusão digital. **Revista Inteligência Empresarial**, Rio de Janeiro, n. 14, p. 4-9, 2003.

PLANT, R.; MURRELL, S. **An executive's guide to information technology**. Cambridge: Cambridge University Press, 2007.

ROSENFIELD, D. L. **O que é democracia**. 5. ed. São Paulo: Brasiliense, 2003.

ROOKSBY, E.; WECKERT, J. **Information technology and social justice**. Londres: Infosci, 2006.

SAMPAIO, J. R. O Maslow desconhecido: uma revisão de seus principais trabalhos sobre motivação. **Revista de Administração-RAUSP**, v. 44, n. 1, 2009.

SILVEIRA, S.A., Inclusão digital, software livre e globalização contra hegemônica. **Revista Software Livre e Inclusão Digital**, organizadores: Sergio Amadeu de Silveira e Joao Cassino, n. 7, p.11, 2003. Disponível em: <http://files.lnandrade.webnode.com/200000338-b6087b8f60/Inclusaodigital_1.pdf>. Acesso em: 13 set. 2017.

SHANNON, C. E. A Mathematical Theory of Communication. **The Bell System Technical Journal**, v. 27, p. 379–423 e 623–656, julho/outubro, 1948. Disponível em: <http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf>. Acesso em: 26 set. 2017.

Tecnologias de informação e comunicação nas redes e na internet

Convite ao estudo

Olá!

Vamos iniciar nossa segunda unidade de estudo, após termos visto o alicerce de conceitos cívicos que servirão de base para os conteúdos mais tecnológicos da disciplina de Tecnologias Aplicadas aos Sistemas de Segurança.

Você já deve ter percebido duas coisas com relação ao mundo que nos cerca: os computadores — de vários tipos, em vários formatos e capacidades — nos cercam por todos os lados; e esses computadores estão cada vez mais conectados, facilitando a comunicação deles próprios, uns com os outros, e de nós, seus usuários, com nossos amigos e conhecidos. Não é novidade para ninguém que esses pequenos (ou grandes) dispositivos são fundamentais em nossas vidas nos dias de hoje e que nos trazem o potencial de aumentar em ordens de grandeza nossa eficiência e produtividade. Distâncias se reduzem, tarefas complexas são realizadas com rapidez e precisão e, em termos de entretenimento, nunca pudemos experimentar imersão em universos tão criativos como nos dias de hoje.

Na base de todas essas possibilidades maravilhosas encontram-se dois elementos que são bastante simples em suas concepções: o computador e a rede.

Nesta unidade vamos entender os conceitos e mecanismos principais desses dois elementos fundamentais.

Visamos, aqui, a partir dos fundamentos da computação, entender as possibilidades e limitações da Tecnologia da Informação e Comunicação e do seu emprego, de uma forma geral, bem como na Segurança Pública e Privada. Como resultado, visamos criar uma cartilha com conceitos de TIC e Sistemas de Informação e Redes.

Vamos, então, ao nosso contexto de aprendizagem. A prefeitura de Nova Jubiabá acaba de adquirir um sistema de monitoração municipal composto de câmeras espalhadas por toda a cidade, mais servidores de armazenamento e processamento e um novíssimo software de apoio, baseado em inteligência artificial, que identifica situações de emergência tais como incêndios, acidentes, tumultos e assaltos, avisando de imediato o poder público.

Jubiabá, embora seja uma pequena cidade, é um município satélite de uma grande capital, exposta à onda de criminalidade comum em alguns centros urbanos. O prefeito percebeu que a implantação de um Centro de Operações de Polícia Militar (COPOM) auxiliaria muito no combate à criminalidade, o que permitiria ligar-se aos demais COPOM da capital vizinha e do estado, compartilhando informações criminais e imagens, possibilitando, dessa forma, uma intervenção mais rápida das unidades de policiamento militar e da Guarda Municipal. A Prefeitura fez, então, os contatos necessários e recebeu do Estado a autorização para implementar o centro de operações, onde participarão as forças estaduais e municipais de forma integrada.

Ocorre que os policiais e guardas municipais que integrarão o COPOM tem um conhecimento um tanto quanto superficial dos conceitos de Tecnologia de Informação, necessitando de treinamento. O prefeito decidiu, então, contratar você e sua empresa de consultoria para criar a ementa de um curso preparatório que leve os primeiros conceitos de TI para os futuros integrantes do COPOM. Esse é um desafio importante, pois tanto é uma excelente oportunidade de negócios para sua

empresa, quanto também é um assunto de suma importância para o combate efetivo à criminalidade de Nova Jubiabá.

Na primeira seção veremos os conceitos básicos sobre o computador, seus componentes e o modo como se interligam.

Na segunda seção veremos os conceitos da infraestrutura de TICs (Tecnologias da Informação e da Comunicação) que perfazem o alicerce da tecnologia digital que temos à nossa disposição, bem como os sistemas de alta disponibilidade, fundamentais para que não haja momentos em que necessitemos de um recurso e este não esteja disponível.

Na terceira seção entenderemos com mais detalhes o que é e como funciona a internet, a "rede das redes" que nos une a todos no cenário planetário, bem como sobre o software, esse conjunto de comandos que realiza nossas tarefas nos computadores do mundo todo.

Em frente!

Seção 2.1

Componentes básicos da TIC

Diálogo aberto

Quantos computadores existem na sua casa? Se você respondeu "nenhum" porque não tem um computador tipo desktop ou um *notebook*, olhe novamente, pois deixou de contar alguns que são bem importantes. Seu micro-ondas é um computador; o aparelho da TV a cabo é um computador, a televisão, hoje em dia, é um computador, e seu celular tipo *smartphone* é um computador. Os computadores nos cercam por todos os lados e são fundamentais para a condução de nossas atividades do dia a dia.

Nesta seção veremos o que são os computadores e como é a arquitetura deles, entendendo como funcionam.

Lembre-se de que a prefeitura de Nova Jubiabá está implantando uma solução digital de segurança pública, o Centro de Operações de Polícia Militar (COPOM), e para a operação deste sistema terá de desenvolver os integrantes deste centro. Esses policiais militares e guardas municipais deverão ser preparados em vários aspectos de tecnologia da informação.

Nessa primeira porção da ementa o curso básico de informática para os integrantes do COPOM da prefeitura de Nova Jubiabá, você deverá incluir os assuntos a serem abordados referentes à arquitetura básica de um computador (unidade de processamento, memória, barramento, entrada e saída), bem como as noções básicas de software e de sistema operacional. Como abordar os assuntos de forma que sejam compreendidos e abordados pelos novos integrantes? Como trazer estes assuntos para a realidade dos policiais? Como incentivá-los a continuar os estudos, dada a importância do funcionamento pleno do COPOM?

Todas as soluções a estes e outros questionamentos ficarão disponíveis em uma Cartilha com Conceitos de TIC e Sistemas de Informação e Redes, a qual os novos integrantes poderão consultar, em caso de dúvida, para o melhor desempenho de seus trabalhos. Essa cartilha será complementada ao longo das seções desta Unidade 2.

Nesta primeira seção vamos entender como funcionam os computadores, seus componentes principais e o software que nos auxilia em nossa miríade de atividades diárias.

Pronto para mais essa jornada?

Então vamos lá!

Não pode faltar

Na seção passada entendemos como evoluíram os computadores até os dias de hoje. Mas, como é um computador por dentro? Que partes compõem um computador e como estas se integram?

Por mais complexos ou simples que sejam, os computadores são formados por elementos bem conhecidos, organizados em uma arquitetura precisa, que extrai dos componentes o máximo em termos de eficiência, enquanto consome o mínimo possível de energia.

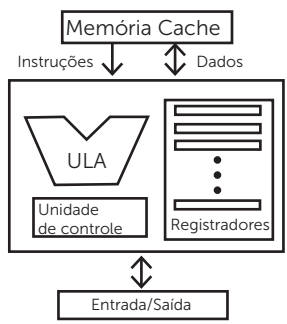
A partir de agora vamos observar mais de perto esses componentes.

Noções Básicas de Unidade de Processamento

Segundo Arruda (2007), a Unidade de Processamento Central de um computador, a CPU (do inglês Central Processing Unit), é o elemento responsável pela execução das instruções e dos cálculos matemáticos. É pela CPU do computador que todas as instruções passam e por ela são decodificadas e processadas. A CPU é o elemento central de todo computador, seu cérebro, por assim dizer.

A Figura 2.1, a seguir, representa os componentes lógicos de uma CPU:

Figura 2.1 | Elementos de uma CPU



Fonte: adaptada de Abd-El-Barr e El-Rewini (2005).

Abd-El-Barr e El-Rewini (2005) definem os elementos da CPU como:

- **Memória Cache** – pequena quantidade de memória dinâmica (memória rápida, a ser vista em mais detalhes um pouco mais à frente) para ser usada diretamente dentro do processador (CP), para dar velocidade ao acesso a dados e instruções.
- **Unidade Lógica e Aritmética (ULA)** – elemento responsável pela execução de operações de lógica booleana, que realiza operações cujos resultados podem ser zero, representando o falso, e um, representando o verdadeiro, bem como de operações aritméticas.
- **Unidade de Controle** – elemento que coordena o "tráfego" para dentro e para fora da CPU. Define para onde devem ser enviados os dados e de onde devem ser lidos os dados e as instruções, bem como a cadência de entrada e saída de dados e instruções.
- **Registradores** – posições especiais de memória interna ao processador, capazes de serem endereçados pela ULA. Os valores armazenados nos registradores são passíveis de participar das operações lógicas e aritméticas da ULA. Um dado armazenado em memória deve ser primeiramente transferido para um registrador antes de ser utilizado em um cálculo qualquer.
- **Entrada/Saída** – elemento de acesso da memória e/ou de outros componentes periféricos para o processador e do processador para esses componentes. Permite a entrada de dados para o processamento e para a saída de dados após o processamento.

Segundo Stallings (2010), desde o início da década de 1970, a CPU vem sendo implementada em um único chip, isto é, em uma única placa de silício. É importante que assim seja, isto é, que todas as funções da CPU estejam em uma mesma pastilha de silício, pois isso garante a velocidade de acesso aos dados e instruções, tornando mais ágil o processamento.

Assimile

Todas as operações aritméticas (somas, subtrações, multiplicações, divisões) e todas as operações lógicas (comparações) são feitas na Unidade Lógica e Aritmética (ULA). As operações são sempre feitas sobre números binários, isto é, compostos de "0" e "1", apenas.

Noções básicas de memória, barramento, entrada e saída

Tanto Hennessy e Patterson (2014) quanto Stallings (2010) definem memória como elementos onde são depositadas (temporária ou permanentemente) informações e de nos quais essas informações podem ser recuperadas. Uma analogia com o mundo real seria um caderno ou um livro. No caderno ou no livro, podemos armazenar informações que podem ser recuperadas. No caso do caderno, as informações podem ser armazenadas temporariamente, pois se as escrevemos com lápis, essas informações podem ser apagadas. No caso do livro, as informações ali armazenadas estão presentes permanentemente, após a impressão, não podendo ser reescritas.

Há várias maneiras de classificarmos as memórias presentes em um computador. Stallings (2010) oferece, entre outras, a classificação por *permanência* da informação. Por essa classificação, temos basicamente dois tipos de memória:

- **Memória ROM** – do inglês *read only memory,* ou memória apenas para leitura. Trata-se da memória permanente, isto é, uma vez gravada, não é apagada, a não ser em alguns casos especiais, e nunca pelo usuário durante a operação do computador. Não depende de o computador estar ligado para manter seus valores (depois de desligarmos e ligarmos o computador, as informações gravadas em ROM permanecerão sempre as mesmas). Pode ser dos seguintes subtipos:
    - ◊ **ROM Básica** – sua construção é em pastilha de silício, e os dados são "prensados" junto à pastilha em si. Uma vez escritas as instruções, não há como alterá-las nem em regime de manutenção.
    - ◊ **PROM (Programmable ROM)** – Refere-se a uma memória ROM um pouco mais maleável: é construída de forma genérica, permitindo que qualquer instrução ou dado seja gravado a *posteriori* em suas posições. Uma vez gravado

(programado) uma instrução ou dado, não há mais como ser alterado.

- ◊ **EPROM (Erasable PROM)** – além de poder ser programada, a EPROM pode ser apagada quando exposta a uma luz ultravioleta. Este tipo de memória é muito usada em laboratório, quando se testam novas configurações para algum componente do computador.
- ◊ **EEPROM (Electrically Erasable PROM)** – além de poder ser programada, pode ser apagada, mas sem a necessidade de uma luz ultravioleta. Este tipo de EPROM pode ser apagado com uso de uma corrente elétrica aplicada a um de seus terminais.

- **Memória RAM** – do inglês *random access memory* (memória de acesso aleatório). Trata-se da memória temporária, na qual as informações (bits "0" e "1") são armazenadas sob forma de sinais elétricos. Os dados armazenados podem ser apagados ou reescritos de acordo com a necessidade, e só estarão disponíveis enquanto o computador estiver ligado. São dos seguintes subtipos:
  - ◊ **RAM Estática** – cada bit é formado por um circuito chamado "flip-flop", composto por um conjunto de transistores. Uma vez armazenado, o bit fica presente sem a necessidade de outras ações para sua permanência, a não ser a alimentação do circuito. São rápidas, mas ao mesmo tempo mais caras, uma vez que para cada bit são necessários vários transistores. É usada no cache, isto é, na porção interna do processador que armazena dados e informações a serem usados mais imediatamente.
  - ◊ **RAM Dinâmica** – cada bit é formado por um capacitor. Uma vez armazenado, o bit precisa ser "refrescado" de tempos em tempos, uma vez que a carga do capacitor não é permanente, e tende a se deteriorar com o tempo. É mais lenta que a memória estática, mas muito mais barata, pois, ao invés de vários transistores, demanda apenas um capacitor para sua criação.

Há, ainda, as memórias secundárias, isto é, locais de armazenamento permanente, nos quais guardamos arquivos que não estão sendo manipulados pelo processador. Os HDs (*hard disks*, ou discos rígidos,

os *floppy disks* (ou discos maleáveis) são exemplos desse tipo de armazenamento. Veja na Figura 2.2 um exemplo de um HD.

Figura 2.2 | Unidade de Disco Rígido Aberta

Fonte: <https://goo.gl/rZZTW6>. Acesso em: 26 out. 2017.

Os barramentos são os circuitos que permitem a entrada e a saída de dados dos chips (processadores, memórias, periféricos etc.). São sempre de múltiplos de 8 bits e, atualmente, os barramentos mais comuns são de 84 bits, permitindo a transferência de 8 e 8 bytes (sendo que 1 byte tem 8 bits).

Reflita

Se a memória estática é mais rápida, por que não a utilizamos como toda a memória RAM do Computador? Em outras palavras, por que precisamos recorrer às memórias dinâmicas, mais lentas?

Noções básicas de hardware e software

Quando pensamos em hardware e software é importante entendermos do que se tratam esses dois conceitos. Velloso (2010) nos, afirma que quando falamos em hardware estamos nos referindo ao equipamento tangível, isto é, placas, consoles, carcaças, fios e tudo o que compõe o computador. O hardware é visível, tangível.

Velloso (2010) ainda nos, afirma que o software são os programas, códigos binários que compõem as instruções que passamos ao computador para serem realizadas as tarefas que queremos que sejam feitas pelo computador. O software é invisível, intangível.

O Quadro 2.1 faz um comparativo entre hardware e software:

Quadro 2.1 | Comparativo entre hardware e Software

Característica	Hardware	Software
Natureza	Física	Lógica
Composição	Átomos	Bits
Maleabilidade	Estático, inflexível (uma vez criado, será sempre daquela forma, com aquelas capacidades)	Dinâmico, flexível (pode ser modificado com facilidade
Escalabilidade	Custos pouco escaláveis: maior produção exige maior investimento	Custos bastante escaláveis: uma vez feito o investimento para a criação do software, sua reprodução não exige outros investimentos.
Investimento de criação	Alto, por exigir maquinário e localidades especializados	Baixo: pode ser produzido em computadores de baixo custo.

Fonte: adaptado de Velloso (2010).

Exemplificando

O forno de micro-ondas é um hardware, e o pequeno programa que ajusta tempo e intensidade dos raios de micro-ondas toda vez que usamos o forno é um software, no caso, armazenado em memória ROM dentro do circuito.

Noções básicas de sistema operacional

Entre todos os programas (software) passíveis de serem carregados e executados em um computador, nenhum ocupa uma posição tão importante e tão pouco apreciada quanto o sistema operacional. O sistema operacional é, segundo Velloso (2010), o programa cuja responsabilidade é o controle das operações do computador. É o sistema operacional que faz a "ponte" entre o hardware e aqueles programas que queremos executar.

Tomemos o navegador web, por exemplo, qualquer que seja a nossa preferência. O navegador web recebe uma URL via teclado ou via clique do mouse, acessa a rede, busca a página desejada e a exibe em tela. Se houver som, imagem ou vídeo, aciona o módulo correspondente para que o conteúdo seja exibido corretamente.

Nada disso ocorreria se não fosse o sistema operacional. Por quê?

É simples: o navegador (a exemplo de todos os outros pacotes de software) não tem acesso direto ao teclado, ao mouse, ao vídeo, às caixas de som, à placa de rede ou a qualquer outra parte do hardware. Quem tem acesso a tudo isso é o sistema operacional.

É o sistema operacional que faz o acesso ao hardware, e disponibiliza esse acesso aos demais programas. O sistema operacional fala a "língua" do hardware e disponibiliza funções que podem ser usadas pelos vários programas. Dessa maneira, por exemplo, o navegador cria o pedido de acesso a uma página na web, por exemplo, e passa esse pedido ao sistema operacional, que conversa com a placa de rede e envia o pedido para o *site* da Internet.

A Figura 2.3 representa essa relação do sistema operacional com os programas e com o hardware:

Figura 2.3 | Relação entre o Sistema Operacional e demais elementos

Fonte: elaborada pelo autor.

Pesquise mais

Uma das principais funções do sistema operacional é permitir a manipulação e o armazenamento de arquivos. Para tanto, o artigo de Andreza Leite explica como funcionam o sistema de arquivos dos sistemas operacionais, bem como sua utilidade.

LEITE, A. **Sistemas operacionais: sistemas de arquivos**. (Apresentação) Florianópolis: IF-SC. 2009. Disponível em: <http://docente.ifsc.edu.br/alex.forghieri/MaterialDidatico/Sistemas%20Operacionais/Material%20das%20aulas/06%20-%2024-06-2016/Sistema%20De%20Arquivos.pdf>. Acesso em: 11 out. 2017.

Sem medo de errar

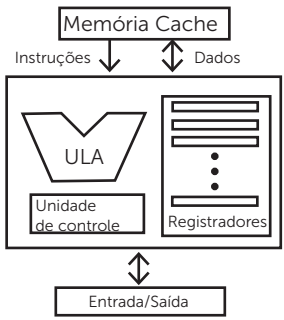
Com o objetivo de treinar os integrantes do COPOM que vão operar o novo sistema de segurança pública de Nova Jubiabá, você vai criar a ementa que os auxiliará a compreender um pouco mais acerca dos

conceitos básicos de hardware e software, ou seja, dos componentes de um sistema computacional completo e complexo.

Lembre-se de que, ao final desta unidade, você terá em mãos uma Cartilha com Conceitos de TIC e Sistemas de Informação e Redes, a qual você poderá iniciar com a apresentação do seguinte conteúdo para os alunos:

- CPU (Unidade Central de Processamento) representada logicamente pela Figura 2.1:

Figura 2.1 | Elementos de uma CPU



Fonte: adaptado de Abd-El-Barr e El-Rewini (2005).

- Os elementos representados são os seguintes:
  - ◊ Memória cache – pequena quantidade de memória dinâmica (memória rápida, a ser vista em mais detalhes um pouco mais à frente) para ser usada diretamente dentro do processador (CP), para dar velocidade ao acesso a dados e instruções.
  - ◊ Unidade lógica e aritmética (ULA) – elemento responsável pela execução de operações de lógica booleana, bem como de operações aritméticas.
  - ◊ Unidade de controle – elemento que coordena o "tráfego" para dentro e para fora da CPU. Define para onde devem ser enviados os dados e de onde devem ser lidos os dados e as instruções, bem como a cadência de entrada e saída de dados e instruções.
  - ◊ Registradores – posições especiais de memória interna ao processador, capazes de serem endereçados pela ULA.

Os valores armazenados nos registradores são passíveis de participar das operações lógicas e aritméticas da ULA. Um dado armazenado em memória deve ser primeiramente transferido para um registrador antes de ser utilizado em um cálculo qualquer.

- ◊ Entrada/saída – elemento de acesso da memória e/ou de outros componentes periféricos para o processador e do processador para estes componentes. Permite a entrada de dados para o processamento e a saída de dados após o processamento.

» Memórias

- Dois tipos:
  - ◊ ROM (apenas para leitura) com os seguintes subtipos:
    - ◊ PROM – ROM Programável (mas estática, após a programação, sem a possibilidade de ser modificada).
    - ◊ EPROM – PROM "apagável". Pode ser zerada e reprogramada, por meio de luz ultravioleta.
    - ◊ EEPROM – EPROM apagável por meio de uma corrente elétrica.
  - ◊ RAM (memória para escrita e leitura com os seguintes subtipos):
    - ◊ Estática – criada por circuitos complexos do tipo flip-flop, consumindo mais recursos, mas sendo bem mais rápidas. Usadas em cache, dentro do próprio microprocessador;
    - ◊ Dinâmica – criada por capacitores simples, consumindo mais energia e sendo mais lenta.

- Hardware e Software
  - ◊ Hardware
    - ◊ Equipamento tangível, isto é, placas, consoles, carcaças, fios e tudo o que compõe o computador.
  - ◊ Software
    - ◊ Programas, códigos binários que compõem as instruções que passamos ao computador para serem realizadas.

◊ O quadro a seguir compara ambos os elementos:

Quadro 2.1 | Comparativo entre hardware e Software

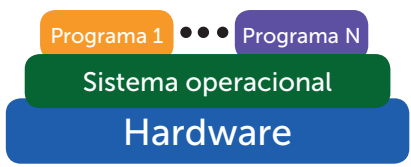
Característica	Hardware	Software
Natureza	Física	Lógica
Composição	Átomos	Bits
Maleabilidade	Estático, inflexível (uma vez criado, será sempre daquela forma, com aquelas capacidades)	Dinâmico, flexível (pode ser modificado com facilidade
Escalabilidade	Custos pouco escaláveis: maior produção exige maior investimento	Custos bastante escaláveis: uma vez feito o investimento para a criação do software, sua reprodução não exige outros investimentos.
Investimento de criação	Alto, por exigir maquinário e localidades especializados	Baixo: pode ser produzido em computadores de baixo custo.

Fonte: adaptado de Velloso (2010).

- Sistema operacional
  - ◊ Programa cuja responsabilidade é o controle das operações do computador.
  - ◊ Faz a "ponte" entre o hardware e os programas que queremos executar.

Imagem que representa a relação entre o hardware, o sistema operacional e os programas:

Figura 2.3 | Relação entre o Sistema Operacional e demais elementos



Fonte: elaborada pelo autor.

Avançando na prática

Classificando as memórias

Descrição da situação-problema

Turíbio saiu de sua aula sobre hardware e software animado com os conhecimentos que ali recebera. Mas, chegando em casa, encontrou alguns elementos e dispositivos que não soube classificar. Na aula seguinte, ciente da oportunidade de aprendizado que isso geraria para si e para os colegas de classe, Turíbio colocou esses elementos e dispositivos em uma caixa e os levou para a sala de aula.

Ao chegar à sala, pediu ao professor para classificá-los. O professor, por sua vez, enxergando ali uma oportunidade de que os alunos aprendessem a analisar e a debater sobre a classificação, optou por lançar o desafio de volta para a sala. Os dispositivos levados por Turíbio eram:

- Um pen drive de 8 GB;
- Um disquete de 3 e ½ polegadas;
- Um maço de cartões perfurados;
- Uma fita cassete;
- Um LP de *rock'n'roll*.

Como classificar os elementos citados de acordo com o que foi aprendido em sala de aula sobre as memórias?

Resolução da situação-problema

Podemos classificar os elementos apresentados por Turíbio da seguinte forma:

- Pen drive de 8 GB – dispositivo atual de armazenamento secundário baseado em memória *flash* que aceita múltiplas leituras e escritas.
- Disquete de 3 e ½ polegadas – dispositivo obsoleto de armazenamento secundário baseado em superfície magnética que aceita múltiplas leituras e escritas.
- Maço de cartões perfurados – dispositivo de armazenamento secundário baseado em papel, que aceita uma escrita e múltiplas leituras.

- Uma fita cassete – dispositivo obsoleto de armazenamento secundário baseado em superfície magnética que aceita múltiplas leituras e escritas.
- Um LP de *rock'n'roll* – dispositivo obsoleto de armazenamento de dados auditivos, que é equivalente à ROM: vem gravado de fábrica e não permite alteração.

Faça valer a pena

1. Observe o texto a seguir:
Elemento responsável pela execução das instruções e dos cálculos matemáticos. É por esse elemento que todas as instruções passam e são decodificadas e processadas. Esse é o elemento central de todo computador, seu cérebro, por assim dizer.

Assinale a alternativa que contém o elemento referido no texto acima:

a) ULA (unidade lógica e aritmética).
b) Memória RAM (memória de escrita aleatória).
c) Memória ROM (memória apenas para escrita).
d) CPU (unidade de processamento central).
e) Sistema operacional.

2. As ROMs (*read only memories*, ou, em português, memórias apenas para leitura) são fundamentais ao computador e aparecem em várias formas, disponíveis para serem usadas em computadores de tipos diferentes. ROM, PROM, EPROM e EEPROM são usadas em dispositivos da atualidade e têm sido assim desde o início do uso de *chips* (circuitos integrados).

No que concerne às ROMs, assinale a alternativa que pontua corretamente a diferença da PROM e da EPROM.

a) A PROM permite escrita aleatória, sendo usada em dispositivos móveis, enquanto a EPROM é mais indicada para dispositivos tradicionais de processamento, como os computadores pessoais.
b) A PROM é muito mais cara, uma vez que usa mecanismos da programação de computadores; já a EPROM é mais barata, pois não se utiliza desses tipos de elementos.
c) A PROM é programável, mas uma vez programada, não pode ser apagada; já a EPROM também é programável, mas pode ser apagada após sua programação.

d) A PROM é obsoleta, pois não se usa mais em computadores e dispositivos móveis; já a EPROM ainda está em uso pela indústria.
e) Não há diferença entre ambas.

3. Entre todos os programas (software) passíveis de serem carregados e executados em um computador, nenhum ocupa uma posição tão importante e tão pouco apreciada quanto o _____. Ele é o programa cuja responsabilidade é o _____ do computador. É ele quem faz a "ponte" entre o _____ e aqueles programas que queremos executar.

Assinale a alternativa que preenche corretamente as lacunas acima:

a) editor de texto, controle das operações, software.
b) navegador, controle das operações, hardware.
c) sistema operacional, fechamento de programas, software.
d) sistema operacional, controle das operações, hardware.
e) sistema operacional, controle das operações, software.

Seção 2.2

Redes e sistemas de alta disponibilidade

Diálogo aberto

Olá!

Você já percebeu como é frustrante tentar acessar um site ou um recurso qualquer na internet e esse recurso não estar disponível? Você tem pouco prazo para resolver um assunto de trabalho e precisa de uma informação que se encontra em um e-mail em sua caixa de entrada. Ao tentar acessar seu correio eletrônico, a surpresa: alguma coisa no caminho está fora do ar, e você fica sem conseguir o acesso desejado. É frustrante à beça, não?

Por outro lado, existem aqueles serviços que sempre estão lá quando você precisa deles e quando, por algum motivo, saem do ar, viram notícia internacional. Manchetes tais como "Máquina de busca X está fora do ar", ou "Rede social Y fica indisponível por 3 horas" chamam a atenção por sua raridade e pelo número de pessoas afetadas.

Em todos os casos que envolvem tecnologia da informação, 100% de disponibilidade é algo patentemente impossível, obviamente. Ainda assim, é possível maximizar a disponibilidade, tornando os momentos de falta de acesso uma fração desprezível do tempo e — preferencialmente — programada com antecedência.

Então é isso que você vai conhecer agora: depois de termos visto os conceitos básicos de um computador na seção anterior, agora vamos construir este conhecimento e entender como tornar as informações mais disponíveis para quem as quer acessar.

Vamos, então, retornar ao nosso contexto? Uma vez que o novo sistema de segurança pública municipal de Nova Jubiabá conectará elementos espalhados pela cidade toda, lembrando que o desafio maior será a implementação do Centro de Operações de Polícia Militar (COPOM) já autorizado pelo governo do estado, a ementa do curso de TI que você está ajudando a montar para os futuros integrantes do Centro, que operarão a referida solução, deverá conter conteúdos acerca da infraestrutura de telecomunicações que interligarão os vários

elementos da solução. Além disso, como o sistema é crítico e não pode parar, você deverá incluir conteúdos acerca de disponibilidade de sistemas, redundância e mecanismos de alta disponibilidade. Imagine o desafio: o COPOM estruturado, funcionando e, de repente, as informações sobre as ocorrências pararem de chegar? As viaturas das unidades policiais não serem acionadas? E, ainda, como trazer tantos assuntos deixando-os interessantes e palatáveis aos alunos que vão operar esse sistema tão crítico?

Nesta seção você vai conhecer os principais conceitos acerca de telecomunicação e redes; computação na nuvem, disponibilidade de sistemas, redundância e alta disponibilidade.

E aí? Vamos a mais esse desafio?

Não pode faltar

Você já percebeu como tem acesso a vários recursos da internet por seu computador e pelo seu *smartphone*, de maneira rápida e transparente, como se esses recursos fossem locais, no seu próprio aparelho? As telecomunicações, os serviços em nuvem e a alta disponibilidade de sistemas e serviços são os responsáveis por essas facilidades.

A partir de agora, vamos analisá-los com mais detalhes.

Telecomunicação e Redes

O termo "telecomunicação" significa comunicação a distância, e Carvalho e Badinhan (2011) a definem como a área de estudo e negócios que lida com a transmissão de informação entre pontos distantes, utilizando, para tanto, mecanismos eletrônicos através de meios físicos distintos.

Podemos, obviamente, entender os sinais de fumaça enviados pelos indígenas norte-americanos ou os faróis da antiguidade, sinalizando locais perigosos ou mesmo a ocorrência de emergências, como comunicação a distância. Porém, a era das telecomunicações começa, mesmo, apenas no século XIX.

Três eventos marcam o início da era das telecomunicações (CARVALHO, BADINHAM, 2011):

- **Telégrafo** – inventado por Samuel Morse, com a primeira transmissão feita em 1844 entre as cidades de Baltimore e Washington, nos EUA.
- **Telefone** – inventado por Alexandrer Graham Bell, em 1876.
- **Rádio** – inventado por Nikola Tesla, mas com atribuição a Guilermo Marconi, em 1895.

A partir do início do século XX as telecomunicações passaram a ter um papel fundamental no desenvolvimento de nossa sociedade, encurtando distâncias e permitindo que nos aproximássemos de entes queridos e de acontecimentos importantes em pontos distantes do planeta.

Assimile

O *boom* que ocorreu nas telecomunicações aconteceu a partir do início do século XX, quando passamos a ver a popularização do telégrafo, do telefone e do rádio.

Em 1927, tivemos a invenção da televisão, e o quadro se completou, na década de 1960, com o surgimento da internet. Essas são as principais tecnologias que temos à nossa disposição para telecomunicações. Você pode perceber facilmente que houve melhorias nessas tecnologias ao longo dos anos, com, por exemplo, a introdução da telefonia celular e da transmissão via satélite de sinais. Mas, em termos de grandes mecanismos de comunicação, estes são os principais e os que mais auxiliam na condução de nossas comunicações planetárias, profissionais e pessoais.

As telecomunicações ocorrem sobre meios físicos diferentes, e os dados devem "viajar "do ponto de transmissão ao ponto de recepção.

Os principais meios usados para as telecomunicações são:

- **Espaço (vácuo)** – no caso do espaço, a comunicação é feita por meio de ondas eletromagnéticas, tanto por mecanismos analógicos (modulação de amplitude e modulação de frequência) quanto por mecanismos digitais (0 e 1 codificados em ondas portadoras). O rádio, a televisão e as comunicações via satélite (rádio, TV, telefone, internet) usam este meio corriqueiramente.

- **Cabeamento metálico** – no caso dos cabos metálicos, a comunicação é feita por meio de pulsos elétricos, também analógicos e digitais. A telefonia é quem mais usa esse tipo de meio, mas os cabos metálicos também são usados para a televisão a cabo e para as comunicações transcontinentais, no caso dos cabos submarinos.
- **Cabeamento óptico** – no caso dos cabos de fibra óptica, a comunicação é feita por meio de sinais de luz e é puramente digital (o "0" é a ausência de um sinal luminoso, e o "1" é a presença de um sinal luminoso, com a diferença de frequência dos sinais servindo como separador de canais). A comunicação da internet é quem mais se utiliza do cabeamento óptico nos dias de hoje.

As telecomunicações são a infraestrutura sobre a qual se alicerçam todas as formas de comunicação da atualidade, e a Internet não é exceção.

Computação na Nuvem

Li, Li e Shih (2014) afirmam que a computação em nuvem, também denominada *cloud computing*, inicialmente visava apenas fornecer recursos computacionais (processamento e armazenamento) sob demanda por meio de compartilhamento de infraestruturas computacionais (hardware, software e redes). Contudo, apesar de essa situação inicial ter se concretizado por alguns anos, não demorou para que a computação em nuvem expandisse dramaticamente seu horizonte para serviços sob demanda em uma ampla gama de cenários flexíveis de compartilhamento de recursos em redes, servidores, armazenamento e aplicativos.

Em outras palavras, de um cenário em que o usuário limitava-se a utilizar recursos computacionais de processamento e armazenagem, a computação na nuvem evoluiu e passou a ser um serviço completo de compartilhamento. O usuário pode acessar aplicativos que não estão instalados em seu computador, armazenar arquivos remotamente e ter a sensação de que estão em seu próprio HD, além de utilizar serviços de rede rápidos e robustos como se os recursos utilizados fossem locais. Isso tudo sem um centavo sequer de investimento em infraestrutura: todos os recursos são oferecidos como serviços.

Reflita

Por que é mais vantajoso para o cliente contratar recursos como serviços do que investir e criar sua própria infraestrutura? Há desvantagens? Quais?

Seja como usuários, seja como profissionais, de nossas vidas certamente a computação em nuvem é parte e pode nos auxiliar sobremaneira no desempenho de nossas atividades:

- **E-mail** – nosso correio eletrônico é armazenado na nuvem e o aplicativo geralmente chega até a gente como um serviço, prestado o mais das vezes sem custo.
- ***Backup* de arquivos** – vários serviços estão disponíveis, inclusive gratuitamente, para armazenamento de arquivos e *backup* na nuvem.
- **Multimídia** – serviços de música sob demanda (Spotify, Apple Music, Deezer, entre outros) e vídeo sob demanda (Vimeo, YouTube, Netflix) estão disponíveis para armazenarmos e servirmos conteúdo próprio, ou para acessarmos conteúdo de terceiros. São serviços que utilizam a tecnologia *streaming*, aquela que transfere dados e informações multimídia por meio de conexões da internet.
- **Hospedagem de sites** – sites pessoais ou comerciais são armazenados não mais em servidores próprios, mas em serviços na nuvem com vantagens: disponibilidade, *backup* e velocidade garantidos pelos prestadores de serviços, com custos mais baixos que os que existiriam se fôssemos manter os servidores em instalações próprias.

Mas você pode perguntar: efetivamente o que é a nuvem? Roundtree e Castrillo (2013) atestam que, nos dias de hoje, a nuvem é uma infraestrutura robusta de hardware, software e redes localizada na internet fora das instalações de seus clientes, mas acessível por todos eles, em que se oferecem recursos (também de software, hardware e redes) como serviço, aliviando esses clientes de investimentos em infraestrutura.

As principais características dos serviços oferecidos na nuvem são (ROUNDTREE, CASTRILLO, 2013):

- **Serviço sob demanda** – o cliente pode requerer acesso a mais ou menos serviços (mais espaço de armazenamento, por exemplo), no momento em que deseje, sem necessidade de intervenção de pessoal de suporte ou de configurações que precisem ser planejadas e executadas com antecedência. A instantaneidade do atendimento da demanda é fundamental na nuvem.
- **Acesso amplo, robusto e rápido aos recursos** – o cliente só precisa de uma conexão simples à rede (internet) e já terá acesso aos recursos demandados. O provedor de serviços na nuvem, por sua vez, garante velocidade, robustez da conexão e banda suficiente para quantos clientes queiram utilizar os serviços.
- **Otimização de recursos** – os recursos sendo utilizados pelo cliente só estarão disponíveis durante a utilização, sendo reorganizados, redistribuídos e otimizados para outros clientes quando não forem mais necessários.
- **Flexibilidade com agilidade** – os recursos devem ser expansíveis ou comprimíveis, isto é, devem ser elásticos com a agilidade demandada pelo cliente, de maneira transparente, sem atrasos. Picos de uso, por exemplo, não devem gerar atrasos ou lentidões.
- **Mensuração de serviços** – o cliente deve ser cobrado exclusivamente pelos recursos que utiliza, quando os utiliza. Isso implica mensurar com precisão a utilização desses recursos, bem como a contabilização transparente para o cliente e o acordo prévio de como serão feitas as cobranças sobre as mensurações aferidas.

São basicamente três os modelos de negócio sob os quais os serviços na nuvem são oferecidos aos clientes, crescendo em complexidade e especialização (ROUNDTREE, CASTRILLO, 2013):

1. **IaaS (*Infrastructure as a Service*, ou Infraestrutura como Serviço)** – o provedor da nuvem oferece máquinas físicas (servidores) ou máquinas virtuais, bem como rede e armazenamento para que seus clientes utilizem como melhor lhes aprouver. O provedor garante a disponibilidade dos recursos contratados, bem como a expansibilidade de acordo com a necessidade do cliente.

2. PaaS (*Platform as a Service*, ou Plataforma como Serviço) – o provedor da nuvem oferece, por exemplo, a plataforma de banco de dados ou a plataforma de desenvolvimento de software para que o usuário construa seu ambiente sobre elas.
3. SaaS (*Software as a Service*, Software como Serviço) – o provedor disponibiliza toda a infraestrutura: servidores, rede, armazenamento, plataforma de bancos de dados, sistema operacional e outros aplicativos básicos, bem como a aplicação principal (software) usada pelo cliente.

A nuvem "veio para ficar", como diz o dito popular, uma vez que oferece recursos com conveniência e em modelos compatíveis com a necessidade atual do mercado.

Disponibilidade de sistemas

Segundo Schmidt (2006), disponibilidade é a medida do tempo durante o qual um serviço ou um determinado recurso está disponível para uso. A interrupção na disponibilidade de um componente altera a disponibilidade do serviço se esse componente for necessário para fornecer o serviço. Como exemplo, o autor diz que a interrupção da disponibilidade da única placa de rede efetivamente determina a indisponibilidade de comunicação, porém não determina a indisponibilidade do sistema local do computador para o usuário que está ao teclado.

O autor afirma, ainda, que o termo "disponibilidade" também se refere a recursos que ajudam o sistema a permanecer operacional mesmo quando da ocorrência de falhas. Exemplo disso é o espelhamento de discos, que melhora a disponibilidade das informações.

O cálculo da disponibilidade é dado pela seguinte fórmula:

$$\text{Disponibilidade} = \frac{\text{tempo disponível}}{\text{tempo total}}$$

Nesse caso, "tempo total" é dado pela soma do tempo disponível com o tempo indisponível.

Outra medida de disponibilidade — com maior utilidade prática que a disponibilidade — é o tempo médio entre falhas, ou MTBF (*Mean Time Between Failures*). No caso da disponibilidade, esta é medida

em percentual (e deve ser sempre 99,999% do tempo para o sistema ser considerado confiável. No caso do MTBF, é medido em horas (SCHMIDT, 2006).

Um dos objetivos do *design*, da engenharia e dos processos produtivos é aumentar a disponibilidade de dispositivos e serviços. Nos dias de hoje, quando passamos praticamente o tempo todo conectados, a indisponibilidade de um serviço qualquer vai ser percebida por milhões de pessoas, afetadas pela falha.

Um exemplo de sistemas em que a disponibilidade é fator preponderante são os sistemas críticos, isto é, os sistemas em que a indisponibilidade torna-se um problema institucional, que põe em risco a sociedade e/ou a própria organização. O sistema de registro de transações de uma operadora de cartões de crédito, por exemplo, é um sistema crítico, uma vez que, se parar, toda a operação da empresa fica inoperante, colocando em risco a existência da própria instituição. Outro exemplo de sistema crítico é o próprio COPOM (Centro de Operações da Polícia Militar), que atende emergências via telefone 190. Se por algum acidente o COPOM que atende uma região parasse, isso implicaria uma ruptura na segurança pública daquele local, colocando em risco a comunidade que ali reside.

Exemplificando

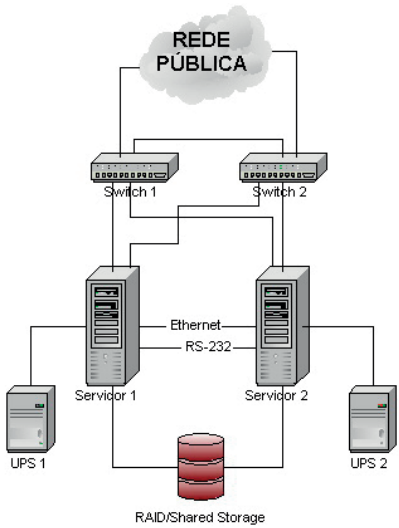
No que concerne aos equipamentos de computação pessoal, a impressora é o dispositivo com menor MTBF, entre 3.000 e 12.000 horas. Por sua vez, o mouse é um dos dispositivos com maior MTBF, entre 50.000 e 200.000 horas.

Fonte: <https://src.alionscience.com/pdf/TypicalEquipmentMTBFValues.pdf>.

Então, caro aluno, uma vez que lhe apresentamos a questão da disponibilidade dos sistemas e que estes podem vir a não funcionar, vamos falar um pouco sobre algumas soluções, como a alta disponibilidade. A alta disponibilidade é definida como o conjunto de ações tomadas para garantir que, quando um elemento falhar, o sistema continuará funcionando, provendo seus serviços. Isso ocorre quando um sistema não tem pontos únicos de falha, ou seja: é composto de elementos que estão prontos para substituirem uns aos outros em caso de falha de um deles (SCHMIDT, 2006).

A Figura 2.4 mostra um exemplo de um sistema de computação de alta disponibilidade.

Figura 2.4 | Exemplo de Sistema de Alta Disponibilidade



Fonte: <https://goo.gl/Ytp3YF>. Acesso em: 19 out. 2017.

Na Figura 2.4 podemos ver que a alta disponibilidade é atingida por meio de:

- **Redundância de rede** – há dois *switches* criando a rede. Caso um deles esteja indisponível, o outro garante a conectividade dos dispositivos. Além disso, ambos os switches acessam a rede pública (por meio de dois roteadores separados, obviamente) por canais diferentes. O ideal é que cada canal venha de um provedor diferente, para haver alta disponibilidade também no nível das comunicações remotas.
- **Redundância de servidores** – há dois servidores, com os dados sendo guardados em um sistema comum de armazenamento de alta disponibilidade (sistema RAID). Caso um dos servidores venha a falhar, os dados continuarão disponíveis e sendo processados pelo outro servidor.
- **Redundância de alimentação** – em que pese o fato de que todos os servidores estejam sendo alimentados pela mesma rede elétrica, há dois *nobreaks* (UPS), um para cada lado da

rede. Caso haja falha na rede elétrica, os *nobreaks* passam a funcionar, e, como há dois deles, adicionamos mais um nível de alta disponibilidade.

Outros mecanismos de alta disponibilidade a serem considerados são os sistemas de *backup*, que podem ser de dois tipos:

- ***Backup* local** – por meio de fitas magnéticas, CDs/DVDs ou HDs externos. Útil nos *backups* do dia a dia e para armazenamento remoto de *backups*, evita que os *backups* sejam comprometidos em caso de incêndio ou inundação, por exemplo).
- ***Backup* remoto** – por meio de armazenamento na nuvem. Tende a ser mais caro e a não gerar *backups* físicos, mas tem disponibilidade garantida, o que nem sempre é verdade para *backups* locais, que podem se deteriorar e se perder.

Pesquise mais

A alta disponibilidade é parte de um assunto mais amplo chamado "Tolerância a falhas". A pesquisadora Taisy Silva Weber, professora do programa de pós-graduação da UFRGS discute o assunto em um artigo bastante didático. Vale a pena conferir, em especial as seções 2 e 3.

WEBER, T. S. **Tolerância a falhas:** conceitos e exemplos, Programa de Pós-Graduação em Computação, Instituto de Informática, UFRGS, 2003. Disponível em: <http://www.inf.ufrgs.br/~taisy/disciplinas/textos/ConceitosDependabilidade.PDF>. Acesso em: 19 out. 2017.

Sem medo de errar

O COPOM, o novo sistema, será empregado por operadores em processo de treinamento pela prefeitura de Nova Jubiabá, processo para o qual eles precisarão conhecer um pouco mais da teoria que envolve telecomunicações, nuvem e alta disponibilidade.

Lembre-se de que nosso produto será a Cartilha com Conceitos de TIC e Sistemas de Informação e Redes. Para tanto, você poderá criar uma ementa com os seguintes tópicos, que muito auxiliarão os operadores do COPOM quando lhe ocorrerem as dúvidas mais básicas:

- Telecomunicações
  - ◊ Comunicação a distância
    - O que é – a capacidade de dois ou mais indivíduos ou organizações comunicarem-se mesmo estando separados por grandes distâncias.
    - Como começou – abordar o início das telecomunicações, como estudado nesta seção.
    - Por que é importante para a sociedade a capacidade de se comunicar a distância – apontar pelo menos 3 grandes problemas resolvidos com as telecomunicações, e/ou 3 grandes vantagens de se ter a possibilidade de comunicação a distância.
  - ◊ Comunicação por meios eletrônicos
    - Exemplos de comunicação por meios eletrônicos – explorar os meios mais conhecidos e usados: rádio, televisão, telefone, Internet
  - ◊ Histórico das telecomunicações – para cada um dos itens seguintes, descrever em um ou dois parágrafos histórico, funcionamento e evolução.
    - Telégrafo.
    - Telefone.
    - Rádio.
    - Televisão.
    - Internet.
  - ◊ Meios de transmissão – para cada um dos meios seguintes, estabelecer as características principais, limitações e principais utilizações nos dias de hoje.
    - Éter (espaço).
    - Cabeamento metálico.
    - Cabeamento óptico.
  - ◊ Implicação das telecomunicações para a sociedade contemporânea – em que nossa sociedade nos dias de hoje é diferente da sociedade de 150 anos atrás, na qual não havia telecomunicações?

- Computação na nuvem
  - ◊ Definição – o que é?
  - ◊ Exemplos – onde são utilizados? Buscar exemplos complementares aos discutidos nesta seção.
  - ◊ Características – quais são as características da computação na nuvem? Quais elementos compõem esse modelo computacional: o que está envolvido em termos de software, hardware e redes? Explanar em parágrafos curtos e objetivos.
  - ◊ Modelos de negócio – explicar funcionamento, opções e limitações de cada um dos 3 modelos de negócio aqui discutidos.
- Alta disponibilidade
  - ◊ O que é disponibilidade - é a medida do tempo durante o qual um serviço ou um determinado recurso está disponível para uso. Explanar com mais detalhes a implicação dessa definição.
  - ◊ Cálculo de disponibilidade – mostrar o cálculo discutido nesta seção, explicando cada termo e sua relação com a disponibilidade.
  - ◊ Mecanismos de alta disponibilidade – o que são e como podem ser caracterizados.
  - ◊ Exemplo explicativo de alta disponibilidade.
  - ◊ Exemplo de sistemas críticos – buscar exemplos de sistemas semelhantes aos dois que são descritos nesta seção.

Dessa maneira, com essa ementa, os operadores do COPOM terão visto os principais assuntos que formarão o alicerce do conhecimento acerca do sistema que operarão para a prefeitura de Nova Jubiabá.

É importante estabelecer que esses assuntos serão úteis porque o sistema será altamente dependente da infraestrutura de telecomunicação da cidade, podendo-se utilizar recursos da nuvem — como o *backup* de informações e relatórios —, e necessitará de alta disponibilidade, uma vez que será um sistema crítico para a administração municipal e, principalmente, para a segurança pública da cidade, pois sua indisponibilidade provocaria transtornos tanto para a população quanto para a prefeitura.

Avançando na prática

Escolhendo o serviço da nuvem para o *site* da empresa

Descrição da situação-problema

O senhor Juvenâncio Rallatesta é diretor de TI da Total Security Segurança Patrimonial, uma empresa de segurança privada de grande porte da capital. A Total Security está interessada em criar uma presença na internet por meio de um *website*. O sr. Rallatesta procurou sua empresa de consultoria para entender como funcionam os modelos de negócio de computação na nuvem e como seria a implantação do site da Total Security em cada um dos modelos. Este *website*, além do marketing para a empresa, auxiliaria, também, nas atividades administrativas nas diversas empresas em que a Security presta os serviços de segurança patrimonial, como o registro das ocorrências de segurança, o que poderia ser feito *on-line*.

Como ajudar o sr. Rallatesta? Como lhe apresentar as informações de maneira que sejam didáticas e compreensíveis, permitindo uma decisão sensata por parte da diretoria da Total Security?

Resolução da situação-problema

Para resolver o problema proposto pelo sr. Juvenâncio Rallatesta, é importante observar os três modelos de negócio da computação na nuvem, e para cada um deles projetar como seria a implantação do *site* da Total Security.

Analisando os modelos de negócio, temos o seguinte:

- **IaaS (Infraestrutura como Serviço)** – neste caso a Total Security contrataria um servidor (virtual, pois um servidor físico teria recursos demais para um website apenas) e ficaria responsável pela implantação do Sistema Operacional, da infraestrutura de servidor *web*, do desenvolvimento de *site* e de sua manutenção periódica (diária, se os conteúdos vierem diariamente). A vantagem aqui é o baixo custo aliado à alta disponibilidade, mas boa parte do trabalho fica por conta da Total Security, que pode não ter o pessoal disponível para desenvolver e manter o *site*.
- **PaaS (Plataforma como serviço)** – neste caso, a Total Security contrataria serviços que incluem o hardware e mais a plataforma de software, no caso o sistema operacional e mais o banco de dados, mais o software básico para a implantação do software.

Tudo isso é oferecido como serviço, e a cargo da Total Security fica o desenvolvimento e a manutenção do *site*.

- **SaaS (Software como serviço)** – neste caso a Total Security especifica o que quer em seu *site* e aprova o *design*. O provedor de serviços implanta e dá a manutenção, e a Total Security, por sua vez, apenas fornece o conteúdo, que será implantado no site pelo prestador, sempre que chegar às suas mãos.

Pronto: você auxiliou a Total Security que, por ser uma empresa de advocacia, deve optar ou pelo PaaS ou pelo SaaS, de forma a minimizar seu trabalho.

Faça valer a pena

1. Observe a seguir a descrição da invenção de três meios de telecomunicação:

1. Inventado por Samuel Morse, com a primeira transmissão feita em 1844, entre as cidades de Baltimore e Washington, nos EUA
2. Inventado por Alexandrer Graham Bell, em 1876
3. Inventado por Nikola Tesla, mas com atribuição a Guilermo Marconi, em 1895.

Os três itens acima se referem, respectivamente, a:

a) 1. Rádio, 2. Telefone, 3. Telégrafo.
b) 1. Internet, 2. Televisão, 3. Satélite.
c) 1. Televisão, 2. Rádio, 3. Internet.
d) 1. Telégrafo, 2. Telefone, 3. Rádio.
e) 1. Rádio, 2. Telégrafo, 3. Televisão.

2. Observe os elementos a seguir acerca dos serviços de computação na nuvem:

I. Acesso amplo, robusto e rápido aos recursos.
II. Otimização de serviços.
III. Investimentos em hardware.
IV. Flexibilidade com Agilidade.

Todos os elementos acima são candidatos a características de serviços de computação na nuvem, mas será que todos o são?

Assinale a alternativa que contém características dos serviços de computação na nuvem:

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

3. A alta disponibilidade é definida como o conjunto de ações tomadas para garantir que, se um elemento falhar, o sistema continuará funcionando, provendo seus serviços. Isso ocorre quando um sistema não tem pontos únicos de falha, ou seja: é composto de elementos que estão prontos para substituirem-se uns aos outros em caso de falha de um deles.

A Empresa X contratou um canal de comunicação terrestre da Empresa A e um canal de comunicação via satélite, também da Empresa A. Ambos os canais são concentrados na sede da Empresa A, na capital do estado. A Empresa X conseguiu eliminar, por essas duas contratações, o ponto único de falha em redes? Por quê?

a) Sim, porque contratou serviços de duas tecnologias diferentes, uma vez que, se o canal de terra falhar, o canal de satélite continuará funcionando, e vice-versa.
b) Não, porque os canais via satélite são extremamente instáveis.
c) Sim, porque as duas tecnologias contratadas são extremamente confiáveis.
d) Não, porque, apesar de serem duas tecnologias diferentes, ambas são concentradas em um mesmo prédio, que é um ponto único de falha.
e) Não, porque um canal de Terra não difere em nada de um canal via satélite.

Seção 2.3

Internet e programas

Diálogo aberto

Você já reparou que vivemos em uma época em que estamos instantaneamente conectados ao que acontece em praticamente todo o planeta? Queremos falar com algum conhecido em um país distante? Não há problema: um aplicativo em nosso celular permite o envio instantâneo de mensagens de texto, de mensagens de voz, e — se a conexão for de boa qualidade – mesmo da fala em tempo real, como numa ligação telefônica. E tudo isso sem pagar nada além do que já pagamos mensalmente na conta do celular. Outro exemplo: longe se vão os tempos em que precisávamos ir até a videolocadora para buscar o filme que estávamos com vontade de assistir. Hoje, esse filme está instantaneamente à nossa disposição, sem o perigo de "todas as cópias estarem alugadas", como no tempo das locadoras.

Ambos os exemplos — e inúmeros outros — são possíveis, por conta de uma ferramenta que temos à nossa disposição: a internet.

Sim, agora que vimos nas seções anteriores como funciona um computador, suas características e capacidades, vamos ver como o computador conecta-se conecta a outros computadores, bem como as consequências dessas conexões.

Vamos retomar nosso contexto de aprendizagem? Após os integrantes do COPOM da prefeitura de Nova Jubiabá terem tido contato com o conteúdo de arquitetura básica de computadores, a infraestrutura de telecomunicações e os mecanismos de alta disponibilidade, é hora de conhecerem um pouco mais acerca das redes de computadores e como a implementação do Centro de Operações de Polícia Militar – COPOM, já autorizado pelo Governo do Estado e a cargo da Prefeitura, funcionará e conectará em uma única e coesa solução.

Seu trabalho agora é incluir na ementa o conteúdo acerca de redes de computadores, protocolos e elementos de funcionamento. Como mostrar aos futuros integrantes do COPOM a importância das redes não apenas para o projeto da prefeitura de Nova Jubiabá, mas também

para sua vida pessoal e profissional como um todo? E como fica a questão das informações, muitas vezes criminais, que serão veiculadas por aquele centro? Será que essas informações e os sistemas lá empregados são todos seguros?

Como temos o produto previsto, você deverá preencher a Cartilha com Conceitos de TIC e Sistemas de Informação e Redes com a solução para essas problemáticas apresentadas. Então, não se esqueça desse aspecto!

Nesta seção veremos as redes de computadores e seus protocolos; em seguida estudaremos a internet, seu histórico e suas características; depois, entenderemos o que é segurança da informação; e finalizaremos com uma pincelada sobre segurança de sistemas, que será o assunto principal nas próximas unidades.

E então? Vamos partir para mais essa jornada?

Não pode faltar

Você já percebeu o quanto dependemos da troca de dados entre sistemas computacionais? Experimente *deslogar* seu celular por algumas horas: certamente você vai perceber o quanto a falta dessa troca de dados será sentida.

Pois é, vem sendo assim há muito tempo. A necessidade de comunicação a distância, como vimos na seção anterior, é bem mais antiga que os computadores, e não é de espantar que, quando os primeiros computadores comerciais foram instalados, seus operadores passaram a desejar que se comunicassem. A troca de dados entre computadores é, de fato, um dos alicerces da sociedade moderna.

A partir de agora, você vai conhecer um pouco mais de perto as características das redes de computadores e da internet, a mais importante dessas redes.

Redes de Computadores, Protocolos

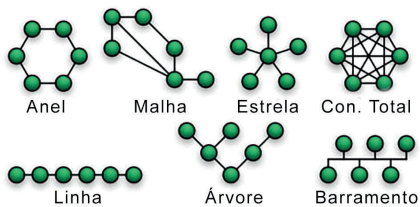
Tanenbaum (2011) define redes de computadores como um conjunto de dois ou mais computadores autônomos, isto é, que podem operar independentemente um do outro, que são interconectados por uma tecnologia qualquer que lhes permite trocar dados.

As tecnologias são variadas para a interconexão de computadores e espelham os meios que vêm sendo usados em telecomunicações:

- Cabeamento metálico.
- Cabeamento de fibra óptica.
- Éter (espaço, atmosfera ou vácuo).

A conexão dos computadores pode ser realizada de várias formas, chamadas "topologias". As topologias mais comuns em redes de computadores são representadas na Figura 2.5:

Figura 2.5 | Principais topologias de redes de computadores



Fonte: adaptada de Paulino (2010).

As características de cada uma das topologias apresentadas na Figura 2.4 são as seguintes (PAULINO, 2010):

- **Anel** – os dados passam de computador a computador até chegar ao seu destino. Um pacote de dados especial chamado *token* é constantemente transportado no ciclo do anel (passando por todos os computadores), e, quando o token está no estado **livre**, qualquer computador pode tomá-lo, marcando-o como **em uso** e a ele anexar um conjunto de dados para um computador de destino. As redes baseadas nessa topologia são chamadas de redes *token ring*.
- **Malha** – alguns computadores têm conexão direta com outros, mas não com todos. Nesta topologia, cada computador tem uma árvore de roteamento, isto é, um mapa dizendo que computador está conectado com quais outros computadores. Dessa forma, quando o computador A quer enviar dados para o computador B, passa esses dados, junto com o endereço de destino, para o computador mais próximo ao destino com o qual tenha conexão.
- **Estrela** – todos os computadores estão conectados a um computador central, que faz o roteamento dos pacotes da origem para o destino.

- **Linha** – funciona como o anel, porém sem completar o ciclo.
- **Árvore** – um computador recebe conexão de apenas um outro, mas pode se conectar com mais de um no caminho "para cima". O resultado é um sistema de ramificação que se assemelha a uma árvore.
- **Barramento** – topologia mais comum em redes de pequeno porte (redes locais). Todos os computadores estão conectados entre si por meio de um barramento (um cabo), com um mecanismo de ocupação do barramento permitindo que este seja utilizado sem que haja confusão nas comunicações.

As tecnologias de rede englobam, ainda, os protocolos utilizados para que ocorra a troca dos dados. Tanenbaum (2011) compara os protocolos de redes de computadores com as línguas que nós, seres humanos, utilizamos para nos comunicar. Usamos palavras e expressões diferentes, e mesmo caracteres diferentes, em muitos casos, quando nos comunicamos em uma ou em outra língua; contudo, conseguimos passar as mesmas mensagens, os mesmos significados.

Os protocolos digitais de comunicação entre computadores estabelecem como as mensagens devem ser codificadas de maneira que sejam compreendidas por todos os computadores que por meio deles se comunicam.

Historicamente há vários protocolos que, ao longo das várias décadas, vêm conectando computadores, muitos dos quais já estão em desuso, ou rapidamente sendo substituídos por protocolos mais amplamente adotados. Dois exemplos de protocolos em desuso evidenciam a necessidade de padrões abertos em comunicação de dados. Os padrões abertos são, é importante frisar, aqueles cujas especificações estão disponíveis para implementação sem custo para as empresas. Diferentemente dos padrões proprietários ou dos padrões disponibilizados por seus criadores por meio do pagamento de *royalties* (taxas cobradas periodicamente para uso de propriedade intelectual protegida), os padrões abertos têm suas especificações publicadas e podem ser utilizados por qualquer empresa que os queira utilizar. Observemos dois protocolos que não são considerados abertos (TANENBAUM, 2011):

- **SNA (Systems Network Architecture)** – criado pela IBM em 1975, o SNA é, até os dias de hoje, o protocolo utilizado para integrar os *mainframes* da IBM. Trata-se de um protocolo proprietário cuja especificação é de conhecimento público, mas que sempre foi estritamente controlado pela IBM.
- **IPX/SPX (*internetwork packet exchange / secure packet exchange*)** – criado pela Novell em 1986 e batizado comercialmente de Netware, o IPX/SPX foi responsável pela proliferação de redes locais em uma época em que a interconexão de computadores em um escritório ainda era pouco divulgada. Com a proliferação do modelo Ethernet e o consequente barateamento dos equipamentos de rede local (em especial dos *hubs e switches*), o Netware caiu em desuso e a empresa passou a atuar em outras áreas de TI.

Com a proliferação de protocolos proprietários, a ISO (*International Organization for Standardization*, ou Organização Internacional para a Padronização), criou, em 1978, o modelo OSI (*Open Systems Interconnection*, ou Interconexão Aberta de Sistemas). O modelo OSI surgiu para padronizar a comunicação entre computadores conectados em uma rede. Tanenbaum (2011) mostra-nos que o modelo divide a comunicação entre computadores em sete camadas de protocolos, dando origem às "7 camadas OSI", demonstradas na Figura 2.6:

Figura 2.6 | As 7 Camadas da OSI

Fonte: adaptada de Tanenbaum (2011).

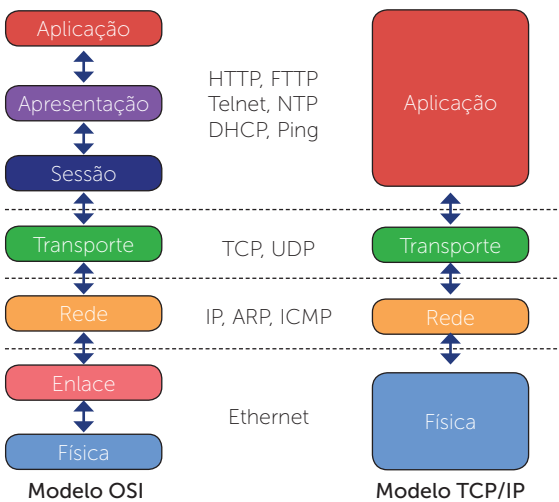
A ideia da pilha de protocolos proposta pela OSI é a de que cada camada converse, dentro do mesmo computador, apenas com as camadas superior e inferior, adicionando complexidade e mais informações quanto mais para cima caminhamos. Entre os computadores, apenas camadas de mesmo nível se "conversam". As 7 camadas do modelo OSI servem apenas para referência didática, uma vez que nunca foram implementadas na prática.

Assimile

Um protocolo digital de comunicação estabelece o formato da comunicação entre dois dispositivos computacionais.

Na prática, o modelo que prevalece é o modelo TCP/IP, no qual as camadas *física e enlace* são agrupadas, bem como também são agrupadas as camadas de *sessão, apresentação e aplicação*. A Figura 2.7, a seguir, mostra a correspondência entre as pilhas OSI e TCP/IP, bem como os protocolos de cada camada, atualmente em uso:

Figura 2.7 | Correspondência entre os Modelo OSI (teórico) e TCP/IP (implementado na Prática)



Fonte: adaptada de Tanenbaum (2011).

São os protocolos que fazem as comunicações entre computadores, dispositivos móveis e todos os aparelhos conectados em rede. São eles as línguas com que os computadores falam entre si quando se comunicam.

Internet: história e características

Segundo Ryan (2010), o período pós-Segunda Guerra Mundial foi um tempo de escalada armamentista em que vimos o surgimento da Guerra Fria: uma série de medidas por parte dos EUA e da União Soviética no sentido de estabelecer hegemonia sobre o planeta todo. Como ambos os países rapidamente desenvolveram um arsenal nuclear capaz de destruir o planeta várias vezes, essas medidas tomavam o lugar de uma guerra aberta, na qual a destruição mútua estava assegurada.

Com a possibilidade de bombas nucleares explodirem e causarem rupturas na infraestrutura do país, as Forças Armadas americanas buscavam soluções que lhes permitissem continuar funcionando mesmo diante de tais explosões. Ocorre que os sistemas de comunicação da época eram centralizados, com elementos interdependentes, geralmente resultando em uma comunicação que dependia de um único ponto, muitas vezes de um único prédio. Isso significa que seria fácil interromper as telecomunicações do país: algumas poucas explosões em locais estratégicos deixariam o país sem a possibilidade de se coordenar por meio das telecomunicações. Essas preocupações foram externadas pela RAND, um centro de pesquisa sem fins lucrativos mantido pelo governo norte-americano. Paul Baran, um dos membros da RAND, foi quem postulou o problema e obteve autorização para buscar soluções (RYAN, 2010).

Nesse contexto, continua Ryan (2010), surgiu a ideia de um modelo de comunicações não centralizado, também postulado por Baran, no qual a comunicação entre partes não afetadas por rupturas (leia-se: bombas nucleares) pudesse continuar mesmo que boa parte da rede estivesse indisponível. As forças armadas comissionaram estudos em universidades com o objetivo de desenvolver esse modelo de comunicação descentralizada.

Em 1961, Leonard Kleinrock, então doutorando no Instituto de Tecnologia de Massachusetts (MIT), desenvolveu o conceito de rede de comutação de pacotes, e, em 1965, essse conceito foi implementado na prática em dois laboratórios independentes, ao mesmo tempo:

- Na Inglaterra, por Donald Davie, no Laboratório Nacional de Física;
- Nos EUA, por Lawrence Roberts e Tomas Mil, no Laboratório Lincoln, em Boston.

A organização RAND continuou à frente dos esforços para obter um modelo funcional, até que as Forças Armadas atribuíram essa função à DARPA (Defense Advanced Research Project Agency, ou Agência do Projeto de Pesquisa de Defesa Avançada), criando o Projeto ARPANET, a futura rede descentralizada a serviço das Forças Armadas (RYAN, 2010).

O projeto daria frutos em 1973, quando Robert E. Kahn e Vint Cerf desenolveram a arquitetura de comunicações que seria rebatizada como TCP/IP. Essa pilha de protocolos tinha a vantagem de ser rápida e de simples implementação, o que permitiu sua adoção por parte de várias universidades norte-americanas e europeias, no momento em que o projeto foi desmilitarizado (RYAN, 2010).

Nascia, nesse momento, a internet.

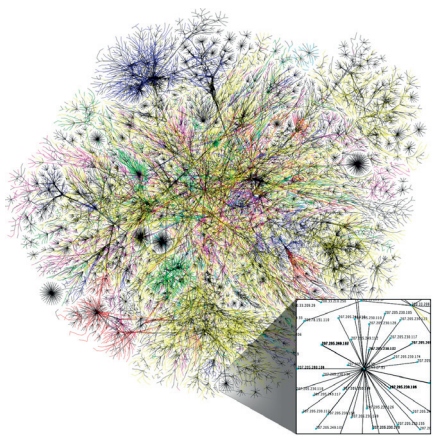
A internet é, segundo Ryan (2010), o sistema global e interconectado de redes de computadores que utilizam o protocolo TCP/IP para suas comunicações. Engloba governos, instituições de ensino, empresas privadas e mesmo boa parte dos cidadãos privados do planeta.

É interessante e importante observar que a internet — que, podemos argumentar, é a mais importante ferramenta de comunicação a serviço da humanidade desde a invenção da escrita, 7.000 anos atrás — só foi possível por causa do protocolo TCP/IP. Em um momento em que a área da computação era dominada por poucas (e gigantescas) empresas, com modelos proprietários de processamento e comunicação e computadores enormes caros, o protocolo TCP/IP foi disponibilizado e prioritariamente ignorado por essas empresas. Os computadores conectados pelo protocolo TCP/IP, no início, pertenciam a instituições (universidades e centros de pesquisa) que não tinham recursos para adquirir os grandes e poderosos computadores da IBM, da Burroughs, da Honeywell, nem para os conectar por meio de protocolos proprietários. O protocolo TCP/IP era o meio de comunicação "dos pobres", mas com uma vantagem: estava ao alcance de todos. Aos poucos, universidades, pequenas empresas, centros de pesquisa e mesmo cidadãos comuns passaram a utilizá-lo, e duas décadas depois — no fim dos anos 1980, antes da explosão — a internet já era a maior rede de comunicação do planeta (RYAN, 2010).

Em 1990, outro (talvez o maior) passo foi dado nessa revolução das comunicações digitais. O pesquisador Tim Berners-Lee, radicado no CERN (Centro Europeu de Pesquisas Nucleares) criou, testou e publicou o protocolo HTTP (hypertext transport protocol, ou protocolo de transporte de hipertexto). Mais uma vez, um protocolo de comunicação entre computadores era criado de maneira aberta, sem que ninguém precisasse pagar nada por sua utilização. Ocorre que o protocolo HTTP é a base da World Wide Web, ou simplesmente "web", como a conhecemos, desde que surgiu em nossos computadores. Graças à interface gráfica, à ampla disponibilização de informações e à enorme facilidade de uso e acesso, a web vem revolucionando as comunicações mundiais. Com o advento dos dispositivos móveis, a partir de meados da década de 2000, o contingente populacional com acesso à internet é o maior de toda a história, e tende a englobar toda a população em apenas mais alguns anos. Segundo o site Internet World Stats (2017), dos 7,5 bilhões de habitantes de nosso planeta, 3,9 bilhões têm acesso à internet hoje em dia. Em outras palavras, a internet é acessada por 51,7% da população.

Nos dias de hoje a internet é uma rede tão ampla e tão complexa, que é difícil representá-la graficamente. A *Opte.org*, uma organização que visa representar a internet de maneira significativa, publica vários gráficos tentando mostrar o que é a internet, e a Figura 2.8 é uma dessas representações. No destaque, um dos nós finais de roteamento com os endereços IP por ele servidos:

Figura 2.8 | Representação gráfica dos caminhos de roteamento da internet



Fonte: <https://goo.gl/UHzpbg>. Acesso em: 11 nov. 2017.

Reflita

A internet seria tão grande e tão popular se os protocolos TCP/IP e HTTP fossem privados (de proprietários) em vez de públicos e gratuitos? Quais seriam as consequências?

Noções básicas de segurança da informação

Sêmola (2014) define *segurança da informação* como o conjunto de ações tomadas para proteger um conjunto de informações, preservando seu valor para o indivíduo ou organização que detém sua propriedade. O autor nos informa que administrar a segurança da informação de uma organização é uma tarefa que pertence à Gestão de Riscos, isto é, as ações tomadas para se proteger dependem de uma análise de risco, pesando fatores como:

- O valor intrínseco da informação.
- O custo da proteção à informação.
- O custo dos impactos de uma possível violação à segurança.

A análise de risco não difere das análises realizadas, por exemplo, pelas seguradoras ao definir o preço de um seguro, ou das análises conduzidas por empresas quanto aos investimentos que devem fazer com determinados recursos financeiros.

Os três aspectos principais a cargo da Segurança da Informação são (SÊMOLA, 2014):

- **Confidencialidade** – propriedade da informação que estipula que a informação só deve estar disponível para indivíduos autorizados por quem lhe detém a propriedade. Indivíduos e/ou organizações não autorizados não devem a ela ter acesso.
- **Integridade** – propriedade da informação que estipula que a informação não deve sofrer modificações não autorizadas após sua emissão, por parte do proprietário, até chegar ao destinatário. Em todo o seu ciclo de vida a informação deve manter sua integridade, e todas as modificações pela qual venha a passar devem ser de conhecimento e devem ter autorização do proprietário.
- **Disponibilidade** – propriedade da informação que estipula que a informação deve estar disponível para utilização sempre que os indivíduos ou organizações autorizadas desejarem a ela ter acesso.

Pesquise mais

Os pesquisadores X e Y discutem os principais aspectos da gestão de segurança da informação em pequenas e médias empresas, iniciando pelas características a serem mantidas pela SI: confidencialidade, integridade e disponibilidade. Vale a pena a leitura de Netto e Silveira (2007), disponível em: <http://www.scielo.br/pdf/jistm/v4n3/07.pdf> (acesso em: 14 nov. 2017).

A segurança da informação preocupa-se com a manutenção da confidencialidade, da integridade e da disponibilidade da informação e se utiliza de algumas ferramentas para tanto:

- **Processos** – em que pese o fato de as ferramentas de proteção serem importantes na manutenção da segurança, nenhuma ferramenta funciona apropriadamente sem que seja utilizada adequadamente. Quem garante esta utilização adequada são os processos, isto é, as instruções e os modos de utilização formalizados por meio de instruções.
- **Treinamento** – outra forma de proteger a informação que não é baseada em ferramentas de proteção. O indivíduo que lida com a informação deve ser treinado a fazê-lo com o cuidado necessário, de forma a não ser ele o ponto fraco da segurança.
- **Criptografia** – a criptografia permite que a informação seja cifrada em seu ponto de origem, trafegada por meios não seguros de comunicação e decifrada apenas por indivíduos e/ou organizações autorizadas. A criptografia colabora com a manutenção tanto da confidencialidade quanto da integridade da informação.
- **Alta disponibilidade** – os mecanismos de alta disponibilidade são úteis à segurança da informação, uma vez que preservam a informação, atuando sobre a disponibilidade desta.

Noções básicas de segurança de sistemas

Os sistemas de informação são, segundo Prado e Souza (2014), conjuntos inter-relacionados de partes formadas por hardware, software, dados, pessoas e processos cujo objetivo é a coleta, o processamento, o armazenamento e a distribuição de informações com o objetivo de apoiar a tomada de decisões.

Os sistemas de informação, dado seu papel crítico dentro da instituição, devem ser protegidos, e a segurança de sistemas é a porção da área de segurança da informação que se preocupa com sua complexidade e com seus aspectos únicos.

Aqui, os conceitos de *confidencialidade, integridade* e *disponibilidade* devem ser aplicados não apenas às informações em si, mas também ao hardware e ao software que compõem os sistemas, bem como às pessoas que os operam.

Nas próximas duas unidades trabalharemos exclusivamente com a segurança sob o ponto de vista dos sistemas.

Não perca!

Exemplificando

Um aspecto que exemplifica a complexidade da segurança de sistemas é a segurança dos sistemas de bancos de dados, os quais inevitavelmente fazem parte de qualquer sistema de informações.

No caso dos bancos de dados, é preciso cuidar da segurança sob os seguintes aspectos:

- Processo de uso dos bancos de dados – o uso e a administração devem ser regulados por processos formais.
- Treinamento dos analistas e operadores do sistema de banco de dados.
- Hardware – recai sobre a equipe de TI esta responsabilidade, mas sempre sob supervisão dos administradores do sistema de banco de dados.
- Software – recai sobre a equipe de TI essa responsabilidade, mas sempre sob supervisão dos administradores do sistema de banco de dados.
- Dados – responsabilidade da administração de banco de dados
- Integração com outros sistemas – responsabilidade conjunta dos administradores do sistema de banco de dados, dos administradores dos demais sistemas com os quais se estabelece a integração, e da equipe de TI que cuida da integração (e da segurança) sob o aspecto de infraestrutura.

Sem medo de errar

Com o intuito de auxiliar os integrantes do COPOM da prefeitura de Nova Jubiabá a se prepararem para operar a nova solução de segurança adotada no município, você deverá incluir os tópicos de redes, internet e segurança (da informação e de sistemas) no programa de treinamento, lembrando que esses tópicos também farão parte da Cartilha com Conceitos de TIC e Sistemas de Informação e Redes, o seu produto.

Uma ementa possível de ser desenvolvida é a seguinte:

- Redes de Computadores
  - ◊ As principais topologias e a forma como funcionam – as várias maneiras de se conectarem computadores, de forma centralizada ou não.
  - ◊ O que são protocolos de comunicação e por que há protocolos diferentes – protocolos são, efetivamente, maneiras usadas para que dois dispositivos troquem informações.
  - ◊ A pilha OSI de protocolos de comunicação – estabelecer as 7 camadas do modelo OSI: física, enlace, rede, transporte, seção, apresentação, aplicação.
  - ◊ A pilha TCP/IP de protocolos de comunicação – estabelecer as 4 camadas do modelo TCP/IP: física, rede, transporte, aplicação.
- A internet
  - ◊ Histórico da internet
    - ◊ Necessidade de comunicação diante da possibilidade de ataques nucleares.
    - ◊ A DARPANET e o projeto militar de comunicação.
    - ◊ O protocolo TCP/IP como resultado.
    - ◊ A desmilitarização do projeto e a adoção por parte de universidades e centros de pesquisa.
    - ◊ O surgimento da eeb por meio da criação do protocolo HTTP.
  - ◊ Abrangência da internet nos dias de hoje.

- ◊ Como representar a internet, uma rede gigantesca.

- Segurança da Informação
  - ◊ Definição de Segurança da Informação - o conjunto de ações tomadas para proteger um conjunto de informações, preservando seu valor para o indivíduo ou organização que detém sua propriedade.
  - ◊ Os pontos a serem protegidos pela SI:
    - ◊ Confidencialidade – apenas os indivíduos autorizados têm acesso à informação.
    - ◊ Integridade – a informação emitida pelo seu criador não sofre alterações não autorizadas.
    - ◊ Disponibilidade – a informação está disponível onde e quando for solicitada pelas partes autorizadas.
  - ◊ Mecanismos de proteção utilizados pela SI:
    - ◊ Processos – formas de atuação pelos operadores autorizados.
    - ◊ Treinamento – capacitação formal.
    - ◊ Criptografia – embaralhamento da informação de forma que apenas as partes autorizadas a ela tenham acesso.
    - ◊ Alta-Disponibilidade – garantia de que a informação ou recurso estarão disponíveis mesmo diante de falhas no ambiente.

- Segurança de sistemas
  - ◊ Definição de sistemas - conjuntos inter-relacionados de partes formadas por hardware, software, dados, pessoas e processos cujos objetivos são a coleta, o processamento, o armazenamento e a distribuição de informações com o intuito de apoiar a tomada de decisões.
  - ◊ Definição de segurança de sistemas e sua importância – garantia de *confidencialidade, integridade e disponibilidade* em sistemas de segurança, uma vez que essa segurança é fundamental para que os sistemas possam ser operados adequadamente e ofereçam resultados corretos e úteis para seus proprietários.

Dessa maneira, os futuros operadores do COPOM estarão a par de todos os conteúdos e estarão, também, ambientados a desenvolver suas tarefas conhecendo os alicerces tanto das redes quanto da segurança.

Avançando na prática

A mensagem foi burlada

Descrição da situação-problema

Clarência é funcionária dos Correios da pequena cidade de Fuxicópolis. Ela tem o hábito de abrir as cartas que considera importantes e ler o conteúdo, antes de dar prosseguimento ao seu envio e entrega. Clarência é secretamente apaixonada por Genélio, um caixeiro viajante que mora na cidade vizinha e que está se correspondendo com Junália, uma jovem residente de Fuxicópolis. Ao ler uma carta de Genélio para Junália, Clarência descobre que o caixeiro está apaixonado pela moça. Dias depois, chega à sua agência a resposta de Junália para Genélio. A jovem está declarando que também está apaixonada por ele e sugere que se casem imediatamente. Sem conseguir se segurar, Clarência decide alterar a carta de Junália, acrescentando o seguinte trecho:

"É importante que nos casemos logo, meu querido Genélio, pois ontem matei meu antigo namorado, o Rubelindo, que teimava em querer me reconquistar. Escondi o corpo, mas temo que a polícia logo vá encontrá-lo. Quando descobrirem, quero estar longe daqui, em teus braços, morando em uma cidade bem distante para podermos começar em paz nossa história de amor".

Alguns dias após enviar a carta de Junália, chega às mãos de Clarência uma resposta de Genélio, desfazendo qualquer compromisso entre ambos. Como essa carta poderia trazer dúvidas a Junália, que não entenderia o motivo da brusca quebra de compromisso, Clarência decide simplesmente jogar a carta fora.

Nessa situação ocorreram várias violações às características da segurança da informação. Explique quais quesitos foram violados em quais momentos.

Resolução da situação-problema

As características de segurança violadas foram:

- **Confidencialidade** – foi violada quando Clarência abriu e leu cartas que não eram destinadas a ela, tanto de Genélio para Junália, quanto de Junália para Genélio.
- **Integridade** – foi violada por Clarência no momento em que adicionou um trecho — patentemente falso — na carta de Junália, dando a impressão de que a moça, sendo desequilibrada, cometera um assassinato e buscara o amor do caixeiro viajante como forma de escapar das consequências de seu ato.
- **Disponibilidade** – foi violada por Clarência quando decidiu simplesmente suprimir a última carta de Genélio desfazendo os compromissos.

Faça valer a pena

1. As redes de computadores podem ser definidas como um conjunto de dois ou mais computadores autônomos, isto é, que podem operar independentemente um do outro, que são interconectados por uma tecnologia qualquer que lhes permite trocar dados.

A fim de poderem trocar informações, os computadores precisam de uma linguagem comum, que determine como as informações serão codificadas e enviadas. A esta linguagem comum damos o nome de:

a) Topologia de Rede.
b) Internet.
c) Protocolo de comunicação.
d) TCP/IP.
e) Pilha OSI.

2. O período pós-Segunda Guerra Mundial foi um tempo de escalada armamentista no qual vimos o surgimento da Guerra Fria: uma série de medidas por parte dos EUA e da União Soviética no sentido de estabelecer hegemonia sobre o planeta todo. Como ambos os países rapidamente desenvolveram um arsenal nuclear capaz de destruir o planeta várias vezes, essas medidas tomavam o lugar de uma guerra aberta, na qual a destruição mútua estava assegurada.

Assinale a única alternativa correta que indica por que os sistemas de comunicação da época do início da Guerra Fria não eram considerados adequados.

a) Porque eram muito caras e de difícil implantação por conta dos altos custos financeiros envolvidos na criação de redes de comunicação que englobassem um país inteiro.
b) Porque eram muito passíveis de ruídos, o que impossibilitava a troca confiável de mensagens, uma vez que os ruídos impediam a comunicação de conteúdo sensível aos ruídos.
c) Porque eram muito inseguras, com constantes ameaças a confidencialidade, integridade e disponibilidade das informações.
d) Porque as redes de comunicação eram centralizadas, e a ruptura no nó central (por um ataque nuclear, por exemplo) destruiria a rede como um todo, deixando as partes sem comunicação.
e) A pergunta induz ao erro, uma vez que a infraestrutura de comunicação da época era plenamente adequada e capaz de suportar rupturas causadas por ataques nucleares.

3. Na brincadeira infantil chamada "telefone sem fio", uma fila de crianças é formada. A primeira criança fala uma mensagem no ouvido da segunda. A segunda criança tenta repetir a mensagem no ouvido da terceira, e assim por diante, até chegar à última criança. Essa última criança, então deve repetir a mensagem. A graça da brincadeira baseia-se em uma característica da segurança da informação.

Assinale a única alternativa correta que indica qual é característica da informação e a forma como ela explica a graça da brincadeira de "telefone sem fio".

a) Confidencialidade, que é burlada porque a mensagem é passada de um para outro.
b) Disponibilidade, porque a mensagem se perde totalmente, não chegando nada do outro lado.
c) Confidencialidade, que é mantida, uma vez que apenas o emissor e o receptor sabem qual é.
d) Cooperação, porque todas as crianças participam da brincadeira.
e) Integridade, que é burlada com a mensagem sendo modificada no meio do caminho.

Referências

ABD-EL-BARR, M., EL-REWINI, H., **Fundamentals of computer organization and architecture**. Nova York: Wiley, 2005.

ARRUDA, F. A História dos Processadores. **Site Tecmundo**, publicado em 17 ago. 2007. Disponível em: <https://www.tecmundo.com.br/historia/2157-a-historia-dos-processadores.htm>. Acesso em: 5 out. 2017INTERNET WORLD STATS. Internet users in the world. 30 jun. 2017. Disponível em: <http://www.internetworldstats.com/stats.htm>. Acesso em: 28 out. 2017.

CARVALHO, A. G.; BADINHAN, L. F. C. **Eletrônica:** Telecomunicações, São Paulo: Fundação Padre Anchieta, 2011.

HENNESSY, J. L., PATTERSON, D. A. **Arquitetura de computadores:** uma abordagem quantitativa. 5. ed. Rio de Janeiro: Elsevier, 2014.

LEITE, A. **Sistemas operacionais:** sistemas de arquivos. (Apresentação) Florianópolis: IF-SC. 2009. Disponível em: <http://docente.ifsc.edu.br/alex.forghieri/MaterialDidatico/Sistemas%20Operacionais/Material%20das%20aulas/06%20-%2024-06-2016/Sistema%20De%20Arquivos.pdf>. Acesso em 11 out. 2017.

LI, K.; LI, Q.; SHIH, T. K. **Cloud Computing and Digital Media:** Fundamentals, Techniques, and Applications. Nova York: CRC Press, 2014.

NETTO, A. S, SILVEIRA, M. A. P. Gestão de segurança da informação: fatores que influenciam em sua adoção em pequenas e médias empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação**, v. 4, n. 3, 2007, p. 375-397.

PAULINO, D. Topologia de Redes. **Oficina da Net**, 15 jan. 2010. Disponível em: <https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens>. Acesso em: 26 out. 2017.

PRADO, E., SOUZA, C. A. **Fundamentos de sistemas de informação**. Rio de Janeiro: Elsevier, 2014.

ROUNDTREE, D.; CASTRILLO, I. **The Basics of Cloud Computing.** Boston: Elsevier, 2013.

RYAN, J. **A History of the Internet and the Digital Future.** Londres: Reaktion Books, 2010.

SÊMOLA, M. **Gestão de segurança da informação:** uma visão executiva. Rio de Janeiro: Elsevier, 2014.

SCHMIDT, K. **High Availability and Disaster Recovery**. Berlin: Springer-Verlag, 2006.

STALLINGS, W. **Arquitetura e organização de computadores.** 8. ed. São Paulo: Pearson Pratice Hall, 2010.

TANENBAUM, A. **Redes de Computadores.** 5. ed. Rio de Janeiro: Campus, 2011.

VELLOSO, F. **Informática:** conceitos básicos. 9. ed. Rio de Janeiro: Elsevier, 2014.

Tecnologias aplicadas na segurança pública

Convite ao estudo

Olá! Vamos iniciar mais uma unidade e, nesta, você vai mergulhar de cabeça em questões importantes de tecnologia a serviço da segurança pública.

Em primeiro lugar, será que a tecnologia é importante para a segurança pública?

Um exemplo mostra que sim, a tecnologia pode ajudar, e muito. É o caso do boxeador norte-americano Rubin Carter, condenado por um triplo-homicídio que, nos dias de hoje, está claro que ele não o cometeu. Infelizmente, Carter passou vinte anos preso por conta desses homicídios, até ter sua pena cancelada. Mais uma vez: câmeras nas ruas da pequena cidade de Patterson, Nova Jérsei, onde se encontrava, e mesmo no restaurante onde os crimes ocorreram, teriam evitado que Carter tivesse passado duas décadas na cadeia sem ter cometido o crime.

Nesta unidade você vai entender os conceitos de Tecnologia da Informação e Comunicação (TIC), tornando-se apto a implementar um pequeno projeto na segurança pública.

Vamos então ao nosso contexto de aprendizagem. "Com sete casos por dia, latrocínio sobe 58% no país em sete anos", foi a notícia que Frederico das Neves leu em um jornal de grande circulação, quando entrou em seu gabinete para trabalhar naquela sexta-feira. Frederico era Secretário de Segurança Pública em um dos estados do Norte do País. Ele assumira recentemente o seu cargo, com a incumbência de reduzir os altos índices de criminalidade em seu Estado, um

daqueles em que mais aumentou a delinquência nos últimos dois anos. Frederico sabia que a tecnologia de informação, por si só, não resolveria os problemas da criminalidade, mas que seria um grande aliado no seu combate. Na análise da situação das unidades policiais, o Secretário novato tinha ciência de que seu governador acabara de investir fortemente em novos sistemas e novas tecnologias de informação. "Mas será que estes investimentos tão elevados poderão dar o retorno necessário para que a criminalidade seja mitigada?", pensou Frederico. Ele sabia que seriam enormes os desafios, como escolher os tipos de tecnologias, os sistemas mais adequados e as pessoas que iriam operá-los, e tinha algumas ideias para estruturar alguns projetos mais simples, mas que retornassem de forma mais efetiva em termos de redução da criminalidade.

Sobre nossa nova unidade, na primeira seção vamos entender os laudos e boletins virtuais, bem como a identificação biométrica. Na segunda seção, entenderemos como funcionam os Centros de Operações da Polícia Militar, suas tecnologias de TIC e sua integração com outros sistemas que podem apoiar as operações. Na terceira seção, entenderemos como o software auxilia na Inteligência Policial, como é feito o monitoramento ambiental e o que são (e como funcionam as conexões ultra-seguras.

Os desafios são grandes e muito interessantes.

Prepare-se, pois já vamos começar.

Seção 3.1

TIC nos processos criminais e na identificação dos infratores

Diálogo aberto

Se você usa bancos ou celulares há mais de 5 anos, já percebeu uma tendência: a forma que utilizamos para nos identificar para o caixa eletrônico ou para o nosso aparelho celular está mudando. Anteriormente, nos identificávamos por meio de senhas, mas recentemente temos nos deparado com a alternativa de utilizarmos alguma parte de nosso corpo: nossas digitais, as palmas de nossas mãos, as íris de nossos olhos, nossa face, etc. É uma tendência conveniente, porque se podemos esquecer nossa senha, não vamos esquecer nosso polegar ou nossos olhos em algum lugar. Esses mecanismos são chamados de "biometria", e são muito úteis em no dia-a-dia, além de apresentarem uma camada mais robusta de segurança do que as senhas.

Frederico da Neves, o nosso Secretário de Segurança Pública de um dos Estados do Norte do País, em visita a uma das maiores delegacias da capital, percebeu que esta repartição pública, com os investimentos recentes, apresentava uma boa infraestrutura de rede, com um link de Internet e banda larga bem adequados. A unidade, por ser a maior da capital, tinha um fluxo muito alto de registros de ocorrências e os Boletins de Ocorrência já vinham sendo realizados por meio digital. O Secretário sabia que, se agilizasse o processo de identificação dos infratores, este aspecto poderia refletir no acompanhamento dos índices de criminalidade. Saber quem cometeu o delito, o local que aconteceu o ilícito, se o infrator era reincidente eram dados imprescindíveis, e Frederico desconfiava que ter acesso a estes seria fundamental para alcançar os seus objetivos maiores: o de reduzir os índices de criminalidade no Estado. Mas quais seriam as tecnologias necessárias para atingir estes objetivos? Elas poderiam ser usadas também para melhorar a segurança interna da Secretaria de Segurança Pública? Como criar um projeto de TICs, ainda que simplificado, para auxiliar Frederico?

Estes são alguns desafios que você, na posição do nosso

Secretário de Segurança Pública, terá de enfrentar. Vamos, então, auxiliar Frederico?

A partir de agora você vai entender melhor como funcionam os laudos e boletins de ocorrência digital, além de entender o que é e como funciona identificação biométrica.

E então? Vamos lá?

Não pode faltar

Você já deve ter feito isso algumas vezes ao longo de sua vida: entrar em um cartório para reconhecer firma em algum documento.

Este processo, que é antigo e confiável, atribui o poder de identificação a uma entidade confiável, no caso o cartório, na figura de seu tabelião. O cartório guarda cópias das assinaturas de várias pessoas, e o tabelião tem a capacidade de comparar a cópia verdadeira (feita de próprio punho pela pessoa em questão) com a cópia apresentada, atestando (ou negando) sua veracidade.

Em que pese esse processo funcionar adequadamente, será que a tecnologia digital tão difundida nos dias de hoje, não teria uma maneira mais moderna, simples, barata e segura para identificarmos pessoas e organizações? Será que não temos como eliminar a figura do cartório desse processo de identificação?

A resposta é "sim", e a maneira de fazermos isso é por meio da certificação digital. A partir de agora você vai entender como isso funciona. Afinal de contas, essa identificação digital é fundamental para que os laudos digitais sejam confiáveis.

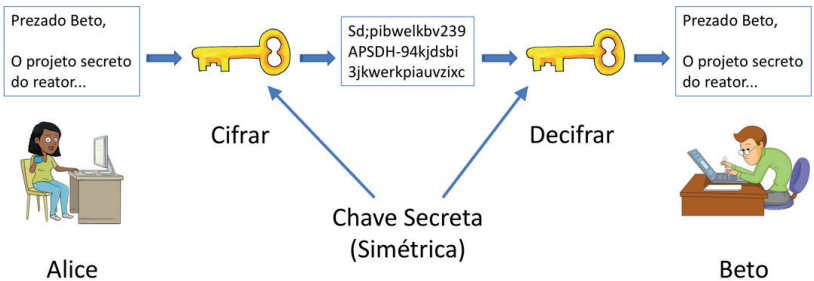
Laudo Digital

Para entendermos a certificação digital, devemos primeiramente entender como funciona a criptografia. A criptografia, como nos mostra Singh (2002), é o mecanismo de cifrar uma mensagem de maneira que apenas o destinatário possa compreendê-la. Ciframos uma mensagem antes de enviá-la, e apenas o destinatário – que tem a chave para decifrar a mensagem – conseguirá lê-la.

Esse mecanismo é bastante antigo, e em sua forma mais tradicional se baseia em uma chave secreta (ou simétrica) de cifragem

e decifragem, como nos mostram Buchman, Karatsiolis e Wiesmaier (2013). Esta chave, usada tanto para cifrar quanto para decifrar a mensagem (daí ser chamada de "simétrica"), é compartilhada entre as duas partes antes do início do processo de comunicação. A Figura 3.1, a seguir, ilustra esse conceito:

Figura 3.1 | Mecanismo de criptografia de chave secreta (ou simétrica)



Fonte: adaptada de Buchman, Karatsiolis e Wiesmaier (2013)

Em que pese a criptografia de chave secreta ter sido bastante utilizada ao longo da História, com inúmeros segredos de Estado tendo sido por ela protegidos, esse mecanismo apresenta algumas falhas que reduzem seu valor nos dias de hoje. As duas principais falhas são:

- Como a mesma chave é usada para cifrar e decifrar a mensagem, se esta chave for comprometida, toda a comunicação terá sido comprometida
- Este processo não permite autenticar o emissor da mensagem. A princípio, a identidade do emissor é garantida pela chave secreta, mas se esta chave for descoberta por outra pessoa, esta outra pessoa pode se fazer passar pelo emissor.

Exemplificando

Um dos códigos baseados em chave secreta mais utilizados no início do século XX era o código baseado em livros. A mensagem era baseada em ternas de números, como por exemplo:

(13,3,157) (7,20,34) (85,12,22) (133,4200) (31,13,1)

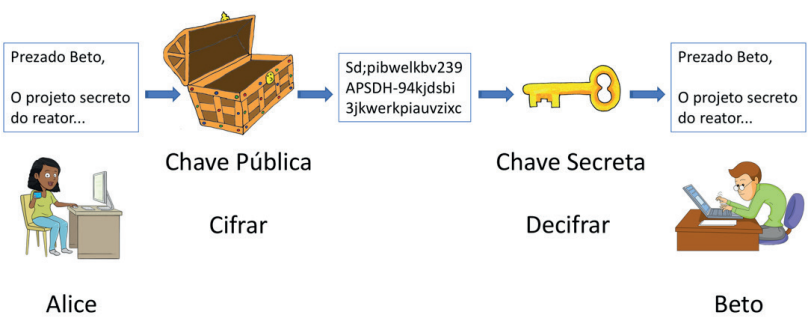
O primeiro número indica a página do livro, o segundo número indica a linha, e o terceiro número indica a palavra. A chave secreta é o nome e a edição do livro em questão. Sem saber qual o nome e a edição do livro, é virtualmente impossível decifrar o código.

Estas falhas foram resolvidas com o surgimento de um novo mecanismo de criptografia, chamado "criptografia de chave pública". Buchman, Karatsiolis e Wiesmaier (2013) descrevem o processo de criação de chaves públicas da seguinte forma:

- Uma pessoa ou organização cria, por meio de um software, um par de chaves: uma chave pública e uma chave privada.
- A chave pública poderá ser acessada por quem queira se comunicar seguramente com a pessoa ou organização que a gerou, e é disponibilizada, e será usada para cifrar a mensagem. Esta chave pública não tem utilidade nenhuma para decifrar a mensagem.
- A chave privada é secreta e fica sob custódia da pessoa ou organização que a gerou, e serve para decifrar a mensagem.

Quando alguém cria um par de chaves pública/privada é como se estivesse criando uma caixa segura (chave pública) que pode ser aberta apenas por uma única chave (secreta). Uma vez fechada, a caixa se tranca automaticamente, e quem está de posse não pode fazer mais nada. Essa caixa é, então, reproduzida e distribuída para quem quiser mandar mensagens para quem a criou. A Figura 3.2, a seguir mostra este funcionamento:

Figura 3.2 | Mecanismo de criptografia de chave secreta (ou simétrica)



Fonte: adaptada de Buchman, Karatsiolis e Wiesmaier (2013).

A chave privada de uma pessoa ou organização serve, ainda, para "assinar" a mensagem, e esta assinatura pode ser checada com a chave pública, que estará em poder do destinatário. O processo completo de uma comunicação entre Alice e Beto deve ocorrer assim:

- Alice gera um par de chaves privada e pública
- Beto gera um par de chaves privada e pública
- Alice envia sua chave pública a Beto
- Beto envia sua chave pública a Alice
- Alice cria uma mensagem cifrada com a chave pública de Beto
- Alice usa sua chave secreta para "assinar" a mensagem
- Alice envia a mensagem cifrada e assinada para Beto
- Ao receber a mensagem, Beto usa a chave pública de Alice para checar se a assinatura é válida
- Após checar a assinatura, Beto usa sua chave privada para decifrar a mensagem

Para que esse mecanismo fique robusto, falta apenas resolver uma pequena vulnerabilidade: quem me garante que quando recebo uma chave pública da pessoa ou organização "X", foi realmente essa pessoa ou organização que gerou a tal chave? Em outras palavras, como é possível garantir a autenticidade da pessoa ou organização cuja chave pública tenho em mãos?

Surge aí a figura da entidade responsável pela autenticação. Esta entidade (uma pessoa ou uma organização confiável) recebe minha chave pública diretamente de minhas mãos, e quem quiser minha chave pública pode ir retirá-la com essa entidade. Essa entidade tem a responsabilidade de certificar as identidades das pessoas, e leva o nome de **Entidade Certificadora**. No Brasil, os Correios, por exemplo, têm essa responsabilidade. Outras entidades também podem emitir esses certificados digitais, como no caso da Receita Federal. Qualquer cidadão pode ter um certificado digital, que é usado para garantir sua identidade, além de garantir a segurança de suas mensagens. Toda essa infraestrutura leva o nome de ICP-Brasil, ou Infraestrutura de Chaves Públicas do Brasil.

Então, voltando aos laudos digitais, estes são emitidos e gerenciados usando este conceito. As polícias de vários Estados da Federação já adotam corriqueiramente este tipo de procedimento,

por meio desta tecnologia. Em São Paulo, por exemplo, a coleta de evidências periciais e os dados de processos investigativos são armazenados digitalmente, disponibilizados para a emissão de laudos, cuja emissão é garantida pela certificação digital administrada pela ICP-Brasil (SPTC-SP, 2015).

O processo de certificação digital utilizado na emissão e administração de laudos digitais traz várias vantagens aos processos em que são utilizados, atuando sobre dois dos principais elementos da segurança da informação e mais sobre um terceiro elemento, a autenticidade:

- **Confidencialidade** – Em casos de processos sigilosos, os laudos podem ser criptografados de maneira a estarem acessíveis apenas a quem de direito, impermeáveis a partes não autorizadas.
- **Integridade** – Os laudos são assinados digitalmente e qualquer alteração em seu conteúdo invalida a assinatura digital, o que é facilmente percebido pelo software de certificação.
- **Autenticidade** – Os laudos podem ser utilizados em processos judiciais uma vez que podemos certificar sua procedência oficial.

Boletim Digital

A Internet agiliza o acesso às informações de inúmeras maneiras, e o Poder Público também se aproveita dessas vantagens. As polícias estaduais, por exemplo, disponibilizam os serviços de boletim de ocorrência digital, permitindo que o cidadão registre ocorrências e acompanhe seu desenvolvimento sem precisar ir à delegacia, com informações precisas e instantâneas ao seu dispor.

Como a administração policial é de alçada do Estado, cada uma das unidades da Federação tem autonomia para implantar este serviço, e todos, mais o Distrito Federal, os oferecem à população por meio das Delegacias Online (CORRÊA, 2015).

No Estado de São Paulo, por exemplo, os boletins que podem ser registrados online são (SSP-SP, 2017):

- Roubo/furto de veículo
- Roubo/furto/perda de objeto ou documento
- Injúria/calúnia/difamação

- Acidente de trânsito sem vítima
- Desaparecimento de pessoa
- Encontro de pessoa

Os dados registrados entram na fila de investigação, e o cidadão pode acompanhar seu desenvolvimento pelo próprio site. Os registros podem ser consultados e o cidadão pode, inclusive, ter acesso a cópias registradas e certificadas digitalmente, para fins de seguro e outros usos oficiais do documento. É mais um exemplo de documento que tem sua autenticidade chancelada pelos certificados digitais, dando ao cidadão a segurança de que os fatos relatados serão adequadamente mantidos pelo Poder Público.

Uma vantagem enorme dos boletins de ocorrência digitais é que permitem a formação de um quadro de estatísticas criminais mais preciso, com indicadores de criminalidade atualizados mensalmente.

Assimile

Os boletins de ocorrência digitais são integrados com bancos de dados, tendo suas informações indexadas, o que permite a busca de seus elementos com o uso de palavras-chave, o cálculo estatístico e a geração de relatórios executivos que ajudam na tomada de decisão por parte do Poder Público.

Biometria na Identificação de Infratores

Martins (2009) define biometria como o estudo das características físicas do indivíduo por meio de medições biológicas com o intuito de extrair características únicas, que permitam a identificação do indivíduo sendo mensurado.

As características biométricas podem ser usadas como vantagens para a segurança, e para entender o motivo, é importante compreender os três níveis de autenticação possíveis:

- **Nível 1** – Aquilo que você e apenas você sabe. Estamos falando aqui das senhas, que dependem de conhecimento. Como vantagem, conhecimento é intangível, e barrando-se a coerção física (tortura), é inatingível por outras pessoas. Como desvantagem, conhecimento pode ser perdido (como o esquecimento da senha) ou compartilhado (como

escrever a senha em um caderno e alguém ler).

- **Nível 2** – Aquilo que você e apenas você tem. Estamos falando aqui de objetos, tais como chaves, cartões magnéticos ou mesmo controles remotos (de portões, por exemplo). A vantagem é que não é preciso depender da memória, e os dispositivos são copiáveis com mais dificuldade do que as senhas. Como desvantagem há a necessidade de sempre tê-los à mão, a possibilidade de perda, os custos de reposição, e o fato de que o portador é identificado pelo dispositivo, seja ele quem for (o que abre espaço para falsidade ideológica)
- **Nível 3** – Aquilo que você e apenas você é. Estamos falando aqui dos elementos biométricos. Suas digitais, por exemplo, são únicas e as chances de alguém ter uma digital que se confunda com a sua são de menos de 1 em 1 milhão. As vantagens são a unicidade dos elementos que nos definem e a facilidade de uso, uma vez que não precisamos lembrar nada nem carregar nenhum dispositivo. Os problemas ocorrem com a falsificação, que no caso das digitais e do reconhecimento facial já têm casos reais.

O reconhecimento biométrico é uma ciência antiga: desde o início do século XX, as perícias criminais vêm desenvolvendo técnicas para identificar impressões digitais, bem como utilizando estes elementos para a identificação de indivíduos (na maioria dos casos, suspeitos em investigações criminais). Surgiu a profissão de perito papiloscopista justamente pela necessidade de identificar os padrões e as nuances das digitais (MANTONI, MAIO, JAIN, PROBHAKAR, 2009).

Reflita

Muitos bancos estão usando uma combinação do nível 1 (senha) com o nível 2 (*token*). Por que essa combinação é útil? De que forma ela melhora a segurança do sistema sendo acessado?

Figura 3.3 | As 9 categorias de impressões digitais

Fonte: Mantoni, Maio, Jain, Probhakar, (2009, p. 33).

Os 9 tipos básicos de digitais, são, conforme a imagem acima:

- 1 Arco Leve
- 2 Arco Agudo
- 3 Presilha Externa
- 4 Presilha Interna
- 5 Verticilo em Bolso Central
- 6 Verticilo Plano
- 7 Verticilo Polegar
- 8 Verticilo em Bolso Polegar
- 9 Presilha Dupla

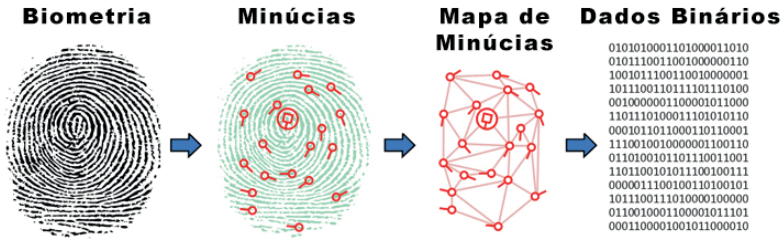
Mais recentemente a TI entrou em cena, mapeando dois tipos de elementos encontrados nas digitais: as terminações e as bifurcações. A Figura 3.4, a seguir, aponta estes elementos:

Figura 3.4 | Terminações e Bifurcações em uma impressão digital

Fonte: adaptada de Mantoni, Maio, Jain, Probhakar, (2009, p. 33).

Os elementos extraídos da leitura biométrica são chamados de minúcias e, além de seu tipo, o ângulo que formam com a horizontal é anotado. Destas minúcias e ângulos, são criados os mapas de minúcias que armazenam também as distâncias entre elas. Este mapa é, então, transformado em um conjunto de dados binários que identifica a digital. Toda vez que uma digital é colhida, seu mapa binário é gerado e comparado ao mapa binário armazenado na base de dados de digitais. Assim é possível identificar o indivíduo. Este método torna obsoleta a função de papiloscopista, com as vantagens de ser imensamente mais preciso, rápido e barato (MANTONI, MAIO, JAIN, PROBHAKAR, 2009). A Figura 3.5, a seguir, ilustra o processo de extração dos dados binários a partir da digital:

Figura 3.5 | Fluxo de extração de dados binários a partir de uma digital:



Fonte: adaptada de IdenityOne, (s/d)

Mecanismos semelhantes à digital são usados para outros elementos passíveis de leitura biométrica, como por exemplo:

- Íris ocular – Utilizado para identificação em celulares de última geração
- Veias da palma da mão – Utilizado em bancos e caixas eletrônicos
- Timbre de voz – Utilizado em softwares especializados de reconhecimento
- Formato facial – Utilizado em celulares de última geração

Reconhecimento Facial na Segurança Pública

O reconhecimento facial é feito de forma semelhante ao mapeamento biométrico de impressões digitais. As minúcias são os elementos da face, tais como olhos, sobrancelhas, boca, nariz. Essas são mapeadas, e sua distância e ângulo de uma para com as outras são registradas, permitindo a criação de um mapa binário representativo.

Em que pese a tecnologia já estar disponível em smartphones de última geração (como no caso do Samsung Glaxo Note 8 e o Apple iPhone X), é nos sistemas de vigilância em grandes espaços públicos que esta tecnologia está, de fato, provando seu valor.

Os sistemas de reconhecimento facial, integrados com grandes bases de dados de pessoas de interesse do mundo todo – criminosos procurados, suspeitos de terrorismo, traficantes internacionais, e por aí vai – são implantados, por exemplo, em aeroportos internacionais, permitindo que o Poder Público identifique a entrada de suspeitos em suas fronteiras.

Estes sistemas também são utilizados em espaços públicos, em especial em eventos, tais como shows e eventos esportivos. Indivíduos que não se comportam adequadamente, por exemplo em partidas de futebol, são identificados e registrados no sistema, podendo ser acompanhados em eventos futuros, ou mesmo impedidos de entrar nas dependências do estádio, em caso de reincidência.

Pesquise mais

A jornalista Elaine Martins, do site TecMundo, escreveu um excelente artigo introdutórios obre Biometria e seus vários aspectos. Vale a pena conferir em: https://www.tecmundo.com.br/o-que-e/3121-o-que-e-biometria-.htm. Acesso em 12 dez. 2017.

Sem medo de errar

A fim de auxiliar na criação de um projeto de TICs para a segurança pública de maneira a auxiliar o Secretário Frederico das Neves, vamos começar pela implantação de um projeto que utilize a biometria para identificar suspeitos em crimes ocorridos na região sob sua jurisdição.

O Projeto de TICs pode começar pela adoção de certificados digitais para a emissão de laudos e Boletins de Ocorrência, garantindo sua autenticidade e integridade para o cidadão, bem como para os demais órgãos. Vamos ver como ficaria a primeira parte do projeto, de acordo com o Quadro 3.1 que se segue.

Quadro 3.1 | Projeto de Tecnologia de Informação e Comunicações 1ª Parte

PROJETO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÕES – 1º PARTE (Apenas os Principais Aspectos)
OBJETIVO ESTRATÉGICO GERAL DO PROJETO: • Reduzir os índices de criminalidade, implementando ações de TICs.
CERTIFICADOS DIGITAIS

ONDE: Em todas as unidades subordinadas à Secretaria de Segurança Pública do Estado (Delegacias, Estabelecimentos Prisionais, COPOM, etc.).

RESPONSÁVEIS: Secretaria de Segurança Pública

AÇÕES A REALIZAR:

- Adoção de Certificados Digitais
- Emissão de Certificados Digitais para os funcionários a cargo da composição de laudos;
- Emissão de Certificados Digitais para os funcionários a cargo da emissão de boletins de ocorrência.

QUANDO: implantados até o ano de 2018.

FINALIDADE: A apresentação dos certificados digitais em conjunto com os documentos emitidos para que o cidadão e/ou os órgãos competentes tenham a certeza de que os documentos emitidos são, de fato autênticos e têm sua integridade preservada.

BIOMETRIA

ONDE: Em todas as unidades subordinadas à Secretaria de Segurança Pública do Estado (Delegacias, Estabelecimentos Prisionais, COPOM, etc.).

RESPONSÁVEIS: Secretaria de Segurança Pública.

AÇÕES A REALIZAR:

A biometria pode ser utilizada, nesse caso, de várias formas, e para o projeto de TICs deve ser empregada da seguinte maneira:

- Identificação de digital para entrar nas dependências da secretaria, substituindo crachás;
- Identificação de íris para entrar em áreas reservadas, como o COPOM;

• Identificação de digital combinada com senha para acessar os computadores da secretaria; • Identificação de íris para controle dos detentos.
FINALIDADE: Garantir a identidade da pessoas.
IDENTIFICAÇÃO DIGITAL
ONDE: Delegacias e Presídios
RESPONSÁVEIS: Delegados e Diretores de Unidades Prisionais
AÇÕES A REALIZAR: • Detentos e suspeitos • Identificação de digital para todas as evidências coletadas em cenas de crimes • Identificação de digital coletada no indiciamento, combinada com apresentação de identidade • Identificação de face para conferência junto a base de dados mantida pela Secretaria da Segurança Pública.
FINALIDADE: Agilizar os processos criminais.

Fonte: elaborado pelo autor.

Avançando na prática

Decifrando o código

Descrição da situação-problema

A polícia da fronteira acaba de prender um traficante em uma agência dos Correios. Esse traficante estava enviando uma carta para um conhecido receptador da capital. Dentro do envelope havia um pequeno pedaço de papel, onde estava escrito o seguinte:

nf qebtnf purtnenb qrcbvf qr nznaun zrvn abvgr an qbpn ivagr qb cbegb

A polícia da capital, após ser informada do ocorrido, foi até o endereço e prendeu o receptador. Após vasculhar o local, encontraram um envelope vindo da fronteira contendo apenas o seguinte:

Rotaciona 13

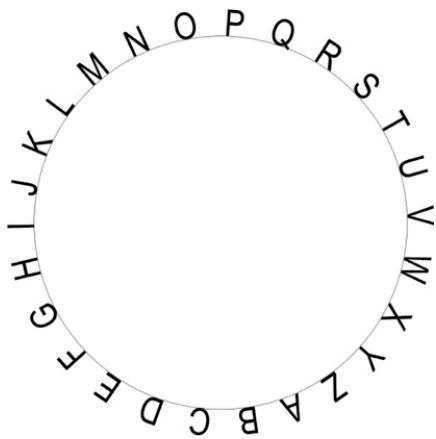
Depois de muito pensar sobre o assunto, a polícia conseguiu apreender um carregamento de cocaína. Onde e quando as drogas foram apreendidas?

Resolução da situação-problema

Depois de pensar muito sobre o que a primeira mensagem apreendida significava, os policiais chegaram à conclusão de que se tratava de uma mensagem secreta, que deveria ser decifrada. Chegaram, também, à conclusão de que "Rotaciona 13" seria a chave para decifrar a primeira mensagem.

Partindo do princípio que "Rotaciona" se refere a alguma coisa circular, pensaram em possibilidades de coisas circulares, até que um deles teve uma ideia: "e se colocássemos o alfabeto em torno de um círculo? Dessa forma poderíamos rotacionar as letras." A Figura 3.6, a seguir, ilustra esse conceito:

Figura 3.6 | O alfabeto em formato circular



Fonte: elaborada pelo autor.

Dessa forma, quando se encontra na mensagem secreta a letra "A", a mesma será substituída rotacionando o alfabeto em 13 posições, resultando na letra "N". De maneira análoga, "B" gera "O", "C" gera ""P", e assim por diante.

Aplicando a chave à mensagem apreendida, a polícia chega à seguinte mensagem:

as drogas chegarao depois de amanha meia noite na doca vinte do porto

Bingo! Assim a polícia soube exatamente onde e quando realizar a prisão dos traficantes, prendendo todos em flagrante delito no momento em que recebiam a carga ilegal no porto, dois dias depois.

Faça valer a pena

1. A criptografia é o mecanismo de cifrar uma mensagem de maneira que apenas o destinatário possa compreendê-la. Nós ciframos uma mensagem antes de enviá-la, e apenas o destinatário – que tem a chave para decifrar a mensagem – conseguirá lê-la.

Em um mecanismo de criptografia de chave secreta, a chave também é chamada de "simétrica". Assinale a alternativa que explica adequadamente o porquê desse nome:

a) A chave é chamada "simétrica" porque existe simetria na mensagem cifrada que sempre começa e termina pelos mesmos caracteres
b) A chave é chamada "simétrica" porque existe simetria na chave de decifragem, que sempre começa e termina pelos mesmos caracteres
c) A chave é chamada "simétrica" porque é sempre igual à mensagem que se quer decifrar
d) A chave é chamada "simétrica porque a mesma chave usada para cifrar a mensagem é usada para decifrá-la
e) A chave secreta não é chamada de simétrica, pois esse é o nome dado à chave pública

2. Quando alguém cria um par de chaves pública/privada, é como se estivesse criando uma caixa segura (chave pública) que pode ser aberta

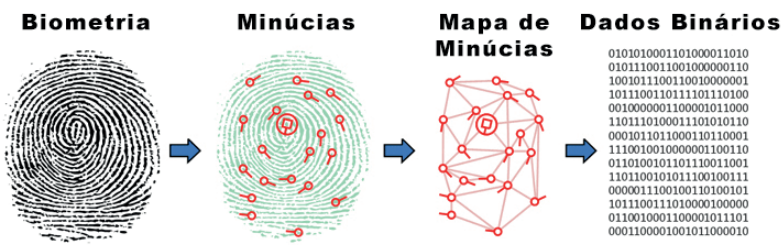
apenas por uma única chave (chave secreta). Uma vez fechada, a caixa se tranca automaticamente, e quem está de posse não pode fazer mais nada. Essa caixa é, então, reproduzida e distribuída para quem quiser mandar mensagens para quem a criou.

Uma das vantagens do mecanismo de chave pública sobre o mecanismo de chave privada é:

a) No mecanismo de chave pública ambas as chaves são publicadas, facilitando-se, assim, o acesso a elas
b) No mecanismo de chave pública a mensagem pode ser assinada, autenticando-se, assim, o emissor
c) No mecanismo de chave pública as mensagens são publicadas, facilitando-se, assim, o acesso a elas
d) No mecanismo de chave pública a mesma chave usada para criptografar a mensagem é usada para descriptografá-la
e) Não há vantagens do mecanismo de chave pública quando comparada ao mecanismo de chave privada

3. Os elementos extraídos da leitura biométrica são chamados de minúcias, e além de seu tipo, o ângulo que formam com a horizontal é anotado. Destas minúcias e ângulos, são criados os mapas de minúcias, que armazenam, também as distâncias entre minúcias. Este mapa é, então, transformado em um conjunto de dados binários que identifica a digital. Toda vez que uma digital é colhida, seu mapa binário é gerado e comparado ao mapa binário armazenado na base de dados de digitais. Assim é possível identificar o indivíduo. A Figura 3.4, a seguir, ilustra o processo de extração dos dados binários a partir da digital:

Figura 3.4 | Fluxo de extração de dados binários a partir de uma digital:



Fonte: adaptada de IdentyOne.

Uma das consequências da adoção de mecanismos de identificação biométrica foi a seguinte:

a) O processo de identificação de suspeitos ficou mais caro do que com o uso de papiloscopista
b) O processo de identificação de suspeitos ficou mais lento do que com o uso de papiloscopista
c) O processo de identificação de suspeitos ficou menos preciso do que com o uso de papiloscopista
d) O processo de identificação de suspeitos ficou menos judicialmente robusto do que com o uso de papiloscopista
e) A profissão de papiloscopista tornou-se obsoleta na identificação de suspeitos de crimes

Seção 3.2

TIC no policiamento

Diálogo aberto

Você já percebeu como as tecnologias de informação e comunicação (TICs) facilitam a nossa vida?

Elas fazem isso de muitas formas, e uma delas, certamente, é facilitando o trabalho dos responsáveis pela segurança pública. Um exemplo claro e clássico são os rádios de comunicação que há tantas décadas auxiliam no policiamento, levando informações aos policiais em campo e permitindo que comuniquem fatos importantes acerca das situações que enfrentam. Mas é claro que os benefícios não terminam por aí. As TICs, recentemente, têm sido adotadas com maior intensidade e velocidade, adicionando eficiência ao poder policial, e auxiliando na manutenção da ordem pública e da paz entre os cidadãos. De fato, como qualquer noticiário será rápido em demonstrar, muito ainda há de ser feito e muito ainda teremos que caminhar para vivermos em uma sociedade decente e menos violenta. Ainda assim, é visível como a capacidade de processar dados de maneira mais rápida e precisa, de integrar sistemas de informação diferentes e complementares, tudo isso aliado à capacidade de comunicação instantânea e confiável, traz inúmeras vantagens ao poder de policiamento e garantia da segurança pública ao estado.

Retomando o nosso contexto de aprendizagem, o Secretário de Segurança pública de um dos Estados do Norte do País, Frederico das Neves, na sua busca pela redução dos índices de criminalidade, entende que as TICs auxiliam sobremaneira nesta tarefa. Depois de iniciar o projeto de implementação de soluções de TIC na segurança, com a adoção de Certificados Digitais e o uso da biometria para identificação dos detentos, dentre outras medidas, percebeu que nem todas as cidades de seu Estado tinham em operação um Centro de Operações da Polícia Militar (COPOM), e ainda, os municípios em que estes funcionavam não tinham por completa a integração entre os sistemas das viaturas e os sistemas do COPOM. Mas quais seriam

as ações a serem desenvolvidas no projeto de implementação da TIC na segurança para integrar todos os sistemas de segurança das viaturas e do COPOM, a ser implantado em cada cidade. Quais são os desafios envolvidos nesta integração (tecnológicos, processuais e legais)? Há vantagens nesta integração? Quais? Ainda, Frederico tinha ouvido falar que os usuários com seus smartphones, caso atuassem de forma estruturada, poderiam contribuir para a melhoria do policiamento comunitário. Como incluir no projeto de Frederico medidas que possibilitassem estruturar, em cada cidade, medidas que, com o uso das redes sociais, aperfeiçoassem o policiamento, permitindo reduzir os índices de criminalidade?

Nessa seção veremos o uso de dispositivos móveis e outras tecnologias aplicados à segurança pública, o uso de TICs nas viaturas e no COPOM, e as redes sociais e sua relação com o policiamento comunitário.

Vamos em frente!

Não pode faltar

Houve um tempo em que inúmeras emergências resultavam em tragédias simplesmente porque os responsáveis pela segurança não tinham como saber do ocorrido. Em outras tantas situações, crimes ficavam sem solução justamente pela falta de tecnologia dos tempos em que ocorreram. De certa forma, os métodos e processos investigativos puderam ser desenvolvidos como forma de compensar recursos mais precisos de detecção, mas ainda assim, o trabalho policial e as ações de segurança pública, em tempos de desastres, são imensamente facilitados com a presença de tecnologias de informação e comunicação.

Vamos analisar alguns dos usos dessas tecnologias como apoio à segurança pública, a partir de agora.

Dispositivos Móveis e Outras Tecnologias Aplicados à Segurança Pública

Segundo Ferrús e Sallent (2015), até recentemente, as forças policiais do mundo todo (inclusive no Brasil) dependiam das malhas de comunicação via PMR (Public Mobile Radio, ou rádio móvel público), especificamente alicerçadas nas tecnologias

- **TETRA** – Terrestrial Trunked Radio (ou, em português, Entroncamento Terrestre de Rádio), uma tecnologia para comunicação criptografada via rádio, com transmissão analógica. Desenvolvido e utilizado principalmente nos estados europeus.
- **TETRAPOL** – Evolução do padrão TETRA, já com transmissão em modo digital
- **Project 25** – Padrão digital para dispositivos móveis, também criptografado, e em uso principalmente na América do Norte
- Estas malhas de comunicação, em que pese serem amplamente utilizadas e altamente confiáveis, não deixam de ter suas limitações, em especial:
- A criptografia usada em qualquer uma delas já foi quebrada e há equipamentos à venda que permitem ouvir todas as faixas. Estes equipamentos, mesmo ilegais em vários países, continuam em uso, e permitem que, desde equipes de filmagem de produções sensacionalistas, até o crime organizado monitorem canais exclusivos da polícia, dos bombeiros e de outras organizações que agem durante emergências.
- O modelo PMR permite majoritariamente a transmissão de voz, com apenas algumas poucas informações podendo ser passadas em texto, em virtude dos protocolos e equipamentos utilizados. Informações em multimídia, por exemplo, não são passíveis de fazer parte das comunicações

Apesar da popularidade e em face às limitações do modelo PMR, Ferrús e Sallent (2015) nos mostram que o cenário está mudando. Entra em cena a tecnologia LTE (Long Term Evolution, ou evolução de longa duração), uma tecnologia digital cujo primeiro resultado prático foram as redes 4G, em 2012. A transmissão em LTE 4G já atinge, nos dias de hoje, 50Mbps (megabits por segundo), o que permite a transmissão de quaisquer conteúdos multimídia, inclusive vídeo e áudio em tempo real. Ainda segundo os autores, em todo mundo as agências de PPDR (Public Protection and Disaster Relief, ou defesa pública e apoio em caso de desastres) estão ativamente buscando a adoção desta tecnologia.

Exemplo de uso dessa tecnologia é dado por Bayley e Stenning

(2016), que referenciam o uso de câmeras corporais por policiais em rotinas de policiamento como forma de melhorar a qualidade dos serviços prestados pela polícia. As câmeras corporais auxiliam em três níveis complementares:

- Permitem aos centros de operações uma avaliação mais precisa das situações em que os policiais se envolvem, com dados audiovisuais em tempo real sendo transmitidos. Estes dados em tempo real são fundamentais no apoio às decisões do centro de operações, que pode dimensionar com maior precisão os recursos policiais e/ou emergenciais a serem destinados a cada ocorrência;
- Permitem ao poder público avaliar as ações dos policiais, agindo como elemento coibidor de abusos do poder policial durante ocorrências;
- Também servem como elemento de defesa dos próprios policiais, uma vez que fornecem dados mais precisos acerca das ocorrências, diferentemente de material audiovisual colhidos pelo público (em smartphones e câmeras pessoais), que podem apresentar quadros fora do contexto total da ocorrência.

A Figura 3.7, a seguir, mostra um protótipo adaptado em um óculos, em uso pela polícia da cidade de Greenville, na Carolina do Sul, nos E.U.A. (GREENVILLE, 2017):

Figura 3.7 | Exemplo de câmera corporal usada por policiais em campo

Fonte: Greenville (2017).

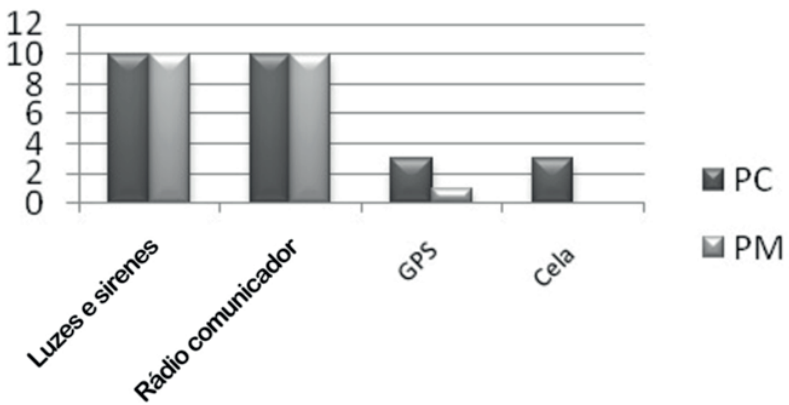
Assimile

A tecnologia LTE 4G já permite comunicação de dados na taxa de 50Mbps (megabits por segundo), o que permite ao poder público se comunicar em multimídia com oficiais em campo, e não apenas mais apenas via voz.

TIC nas Viaturas Policiais

Bock, Pozzebon e Frigo (2016) afirmam que no Brasil, tanto as polícias civis, quanto as polícias militares estão cientes das deficiências de suas viaturas no tocante à tecnologia disponível. O Gráfico 3.1, a seguir, ilustra uma das respostas à pesquisa realizada pelos autores junto a policiais civis e militares, questionando a presença de equipamentos em viaturas usadas pelas corporações, em especial: sirene, rádio, GPS e cela. A pesquisa foi feita com 10 policiais militares (PM) e 10 policiais civis (PC) do Rio Grande do Sul, em uma cidade considerada típica em termos de população e orçamento: a cidade costeira de Torres.

Gráfico 3.1 – Questionamento a Policiais (civis e militares quanto aos equipamentos disponíveis em viaturas



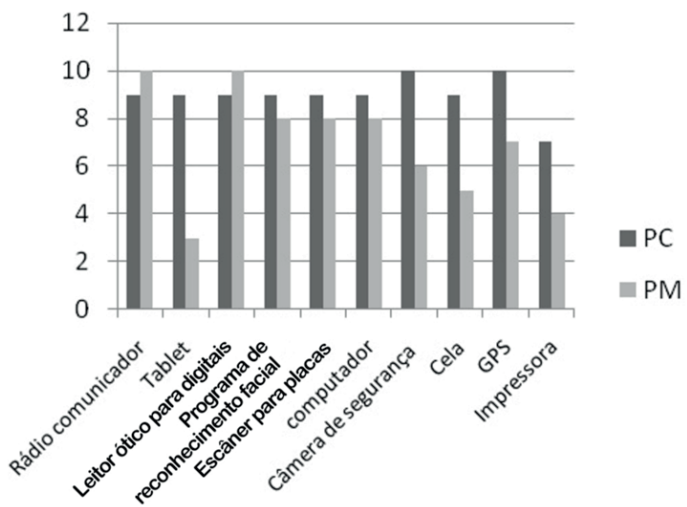
Fonte: Bock, Pozzebon e Frigo (2016)

O gráfico mostra que, apesar de todas as viaturas estarem hoje em dia equipadas com sirene e rádio, apenas 3 policiais civis e 1 militar atestam a presença de GPS em suas viaturas. No caso de cela (segregação segura dentro da viatura - uma cela física, um reforço

em aço no bólido da viatura, na parte de trás, onde vão os suspeitos, com grades e trancas, garantindo que eles não escaparão da custódia dos policiais), apenas 3 policiais civis contam com as mesmas. A pesquisa dos autores mostra que, em termos de TICs, estamos ainda muito longe do ideal. Os mesmos policiais, quando questionados acerca do que pensam ser necessário para suas viaturas para que o policiamento seja mais efetivo, deram respostas dentro do esperado no que concerne as TICs. O gráfico 3.2 mostra as opiniões dos mesmos 10 policiais no tocante às seguintes tecnologias:

- Rádio
- Tablet
- Leitor óptico para digitais
- Programa de Reconhecimento Facial
- Scanner para placas
- Computador
- Câmera de Segurança
- Cela
- GPS
- Impressora

Gráfico 3.2 – Expectativa dos policiais quanto às tecnologias em suas viaturas – PM (Polícia Militar) e PC (Polícia Civil)



Fonte: Bock, Pozzebon e Frigo (2016)

É importante observar que de todas as tecnologias mencionadas pelos policiais civis e militares, com exceção da cela, são dependentes ou podem se beneficiar das TICs. A única que não depende, mas pode de fato se beneficiar é o rádio comunicador que, como discutido nessa mesma seção, tem soluções analógicas atualmente em uso. Ainda assim, o rádio pode se beneficiar das TICs, uma vez que as comunicações via LTE são confiáveis e resilientes, como os provedores de serviço de celular vêm demonstrando ao longo dos últimos anos. Já as demais tecnologias – tablete, leitor óptico para digitais, programa de reconhecimento facial, scanner para placas, computador, câmera de segurança, GPS e impressora – dependem diretamente de TICs para seu funcionamento e integração com os sistemas policiais existentes.

Exemplificando

Um exemplo do uso da TIC na cela, a segregação segura dos presos e os integrantes das polícias em viaturas específicas, pode ser visto no vídeo "Ministério da Justiça entrega 215 carros-cela para transporte de presos". Disponível em: <https://www.youtube.com/watch?v=3ku2FTAy48Q>. Acesso em 04 dez. 2017.

Reflita

Que vantagens poderiam ser derivadas da presença de sistemas de reconhecimento facial em viaturas policiais? Em caso de queda na rede de comunicação (Internet via celular), estes sistemas teriam alguma utilidade para o policiamento e, por consequência, de alguma forma a redução da criminalidade? Por quê?

TIC nos Centros de Operações de Polícias Militares – COPOM

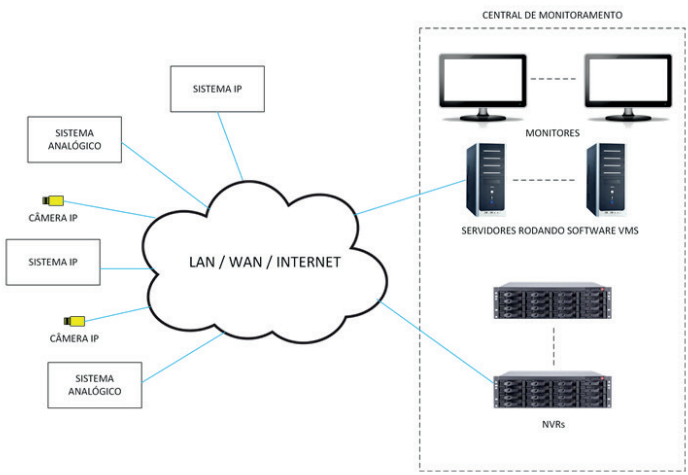
COPOM é a sigla dos Centros de Operação da Polícia Militar. Estes centros de operação são localizados em cada cidade com presença da Polícia Militar, e podem ser desde bem modestos: uma linha telefônica recebendo chamados da população, operada por um policial ou escrivão com acesso a rádio para coordenar ações com outros policiais, delegados e delegacias de cidades vizinhas; até centros dedicados de atendimento e coordenação de ações policiais, com centenas de policiais operando equipamentos de última geração

de comunicação e processamento, e coordenando ações em terra e ar (helicópteros da polícia). O COPOM é, segundo Lima (2004), um portal de acesso ao balcão de serviços da Polícia Militar, serviços esses que são requisitados pelo estado e ao mesmo tempo são dever do Estado ao cidadão.

O COPOM depende de informações para habilitar seus administradores a tomarem decisões durante ocorrências de segurança (crimes em andamento ou recém-ocorridos, acidentes no âmbito de ação da polícia, desastres naturais e que tais). Esta necessidade de informações, aliada à necessidade de comunicação plena com os policiais de campo, torna fundamental a disponibilização de uma infraestrutura de TIC que atenda as demandas de uma sociedade que clama por mais segurança.

Almeida (2014) estabelece uma arquitetura otimizada para centros de monitoração, arquitetura esta adotada pelo COPOM da Polícia Militar do Estado de São Paulo. A Figura 3.8, a seguir, estabelece esta arquitetura:

Figura 3.8 | Arquitetura de um centro de Monitoração



Fonte: <http://institutocftv.com.br/images/estudo%20ellan%20-%20central%20de%20monitoramento%20(small).png>. Acesso em 20 nov. 2017.

De acordo com a arquitetura estabelecida na Figura 3.8, temos:

- **Central de Monitoramento**
  - Servidores rodando VMS (Virtual Machine System, ou Sistema de Maquina Virtual), criando máquinas virtuais em

cada cliente (ou seja, em cada computador sendo operado para o atendimento de emergências)

- NVRs (Network Video Recorders, ou gravadores de vídeo em rede), sistemas de gravação do feed de vídeos enviado pelos policiais, viaturas e helicópteros em campo
- Monitores – instalados nas mesas dos operadores e em um painel de controle do tipo video wall

- **Campo (conectado à central de monitoramento por meio de redes locais, redes de longa distância ou pela Internet)**
  - Sistema analógico de comunicação
  - Sistema IP de vídeo
  - Sistema IP de comunicação
  - Sistema IP de mensagens escritas

Um exemplo de como esta arquitetura de TICs pode ser implantada pode ser visto no COPOM da Polícia Militar do Estado de Sã Paulo, como nos mostra novamente Almeida (2014), na Figura 3.9, a seguir:

Figura 3.9 | Instalação de monitoração do COPOM, PMESP

Fonte: <http://institutocftv.com.br/images/61806%20(small).jog.>. Acesso em 20 nov. 2017.

Pesquise mais

Assista a esse excelente vídeo de demonstração feito pelo COPOM da PMESP, mostrando como funcionam as operações ali monitoradas e deflagradas. Disponível em: https://www.youtube.com/watch?v=-wUHM0RGR3k . Acesso em 18 dez. 2017.

As redes sociais são cada vez mais utilizadas pelas corporações para apoio a ações de segurança pública. Rosa (2015) nos mostra que os custos inexistentes de acesso e publicação em redes sociais – em especial no WhatsApp, no Facebook e no Twitter –, aliados à facilidade de acesso, tornam as redes sociais fermentas úteis na provisão de serviços de segurança pública.

O autor exemplifica que o 15o Batalhão da Polícia Militar de Canoas (RS) aumentou o numero de apreensões de foragidos com a ajuda do WhatsApp, capturando 27 foragidos nos três primeiros meses do ano de 2015 e mais 15 só no mês de abril.

Algumas maneiras úteis de se utilizar as redes sociais na segurança pública são:

- Perfil no Twitter, WhatsApp e Facebook para facilitar a comunicação com a população, divulgação de informações sobre ocorrências e emergências, diálogo com cidadãos
- Hashtags (termos de busca) específicos usados pela população para alertar sobre ocorrências, em constante monitoração pela polícia

Exemplificando

A Polícia Militar do Estado de São Paulo (PMESP) criou a *hashtag* #pmesp para se comunicar com o público usuário do Twitter, como complementação do telefone 190 e do disque-denúncia 181. Outras *hashtags* também são úteis nessa comunicação bilateral: #rocam, #baep, #rota, entre outras.

Sem medo de errar

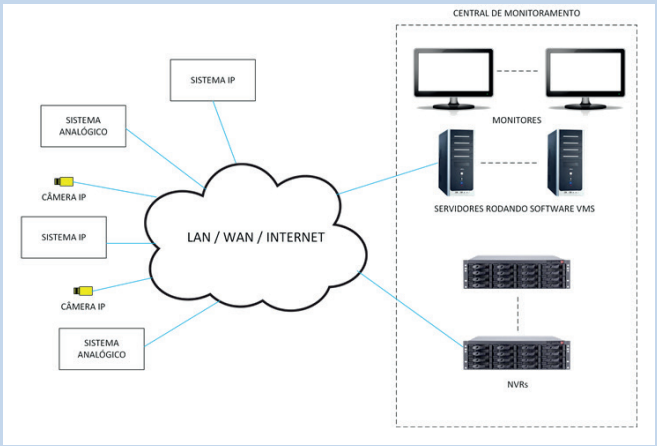
Vamos dar continuidade ao nosso Projeto Simples de TIC na Segurança Pública, o nosso produto. A fim de implementar Centros de Operações da Polícia Militar (COPOM) nas cidades do Estado, e integrá-las com as viaturas, como solicitado pelo secretário Frederico das Neves, podemos ter os seguintes pontos abordados no Quadro 3.2 que se segue.

Quadro 3.2 | Projeto de Tecnologia de Informação e Comunicações 2ª Parte

PROJETO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÕES – 2º PARTE (Apenas os Principais Aspectos)
OBJETIVO ESTRATÉGICO GERAL DO PROJETO: • Reduzir os índices de criminalidade, implementando ações de TICs.
Estabelecimento do COPOM
ONDE: Capital e cidades satélites
RESPONSÁVEIS: Sr. Frederico das Neves
AÇÕES A REALIZAR: • Infraestrutura dos COPOMs • Cidades pequenas (até 10.000 habitantes) • Criar tronco telefônico dedicado com número gratuito de 3 dígitos para acesso da população (o tronco deve concentrar três linhas telefônicas, garantindo que até 3 ocorrências possam ser informadas ao mesmo tempo). • Divulgar nos meios de comunicação a existência da linha telefônica de acesso para emergências. • Criar posição na delegacia da cidade, com acesso telefônico para recebimento das chamadas. • Implantar sistema de computador com solução de registro de ocorrências conectada à Secretaria de Segurança Pública, por meio da qual a delegacia da cidade pequena poderá registrar ocorrências diretamente no banco de dados central do Estado, podendo ser catalogada e estatisticamente integrada nos números de criminalidade e atendimento do Estado. • Implantar infraestrutura de comunicação via Internet que permita a integração deste terminal com a infraestrutura estadual.

- Cidades Médias (entre 10.000 e 100.000 habitantes)
  - Criar tronco telefônico dedicado com número gratuito de 3 dígitos para acesso da população (o tronco deve concentrar vinte linhas telefônicas, garantindo que até 20 ocorrências possam ser informadas ao mesmo tempo).
  - Divulgar nos meios de comunicação a existência da linha telefônica de acesso para emergências.
  - Criar cinco posições na delegacia da cidade, com acesso telefônico para recebimento das chamadas, com policiais treinados para atender as chamadas e categorizá-las adequadamente.
  - Implantar sistema de computador com solução de registro de ocorrências local, com base de dados local para registro de ocorrências.
  - Conectar solução local à Secretaria de Segurança Pública, por meio da qual os registros locais possam ser compartilhados com banco de dados central do Estado, podendo ser catalogada e estatisticamente integrada nos números de criminalidade e atendimento do Estado.
  - Implantar infraestrutura de comunicação via Internet que permita a integração deste terminal com a infraestrutura estadual.
  - A infraestrutura do COPOM de cidades médias pode seguir o modelo da Figura 3.8, a seguir:

Figura 3.8 | Arquitetura de um centro de Monitoração



Fonte: <https://goo.gl/LFidYt>. Acesso em 20 nov. 2017.

- Cidades Grandes
  - Os COPOMs das cidades grandes devem ser atualizados para conter painel central tipo ***dashboard***, onde casos em andamento e mapas pertinentes sejam expostos o tempo todo, para ação e decisão do comando da polícia
  - O sistema deve comportar a integração com os sistemas de cidades satélites, para integração de ocorrências, permitindo ações coordenadas
- Viaturas
  - As viaturas devem ser modernizadas, contendo os seguintes equipamentos, para o uso dos quais os policiais devem ser treinados:
    - Rádio (se já não houver)
    - GPS
    - Leitor de digitais
    - Scanner para placas
    - Câmera de Segurança
    - Câmeras corporais nos policiais
    - Cela
    - Sistema de GPS e tela com sistema integrado ao COPOM, para envio e recebimento de informações de ocorrências em andamento
- Mídias Sociais
  - Uma aplicação do tipo "Cidadão colabora com a segurança" deve ser criada para que a população possa se comunicar com a polícia
  - A PM deve divulgar os **hashtags** da Polícia Militar, o grupo de WhatsApp e a página do Facebook da PM, de forma que os cidadão munidos de smartphones possam relatar ocorrências durante o dia-a-dia.

QUANDO: implantados até o ano de 2018.
FINALIDADE: Estabelecer o COPOM e integrá-lo às cidades do Estado, colaborando para a melhoria da segurança.
RESPONSÁVEIS: Sr. Frederico das Neves

Fonte: elaborado pelo autor.

Perceba, caro aluno, que os desafios envolvidos na integração tecnologia, processos podem ser superados com o projeto sobredito, havendo várias vantagens nesta integração, como a

melhoria no policiamento efetivo e a consequente redução dos índices de criminalidade.

Desta forma, Frederico, que tinha ouvido falar que os usuários com seus smartphones, caso atuassem de forma estruturada, poderiam contribuir para a melhoria do policiamento comunitário, poderá implementar medidas que possibilitem estruturar, em cada cidade, o uso das redes sociais. Outra boa e simples medida que pode contribuir para uma segurança mais efetiva.

Avançando na prática

Procurando alternativas para as câmeras corporais

Descrição da situação-problema

O pequeno município de Jijoquara do Norte tem um problema: alguns cidadãos estão reclamando que alguns dos policiais militares (são 20, no total), agem com muita violência durante as rondas noturnas que fazem na cidade. O Cel. Ivo Noleretti, comandante da PM para o município gostaria de implantar câmeras corporais nos policiais, de maneira a garantir que suas ações sejam sempre de acordo com a lei e com o treinamento que recebem. Infelizmente, o custo dos equipamentos ainda é proibitivo para o orçamento exíguo da corporação de Jijoquara do Norte.

Contudo, o Cel. Moderati fez uma perquirição aos fundos da corporação, e percebeu que teria orçamento para investir cerca de R$300,00 por policial (R$6.000,00 no total). Decidiu, então buscar em sites de compras pela Internet soluções, que se não permitem a transmissão em tempo real das ocorrências, pelo menos conseguem filmá-las para uso posterior.

Consultando sites de vendas e discutindo um processo de uso de equipamentos de filmagem, você consegue chegar a uma solução para que a PM de Jijoquara tenha ciência das ações dos policiais?

Resolução da situação-problema

Uma busca em sites de compra revela que há equipamentos de filmagem tipo minicâmara esportiva na faixa de R$40,00 a R$150,00, com a capacidade de filmar e armazenar as imagens em cartões do tipo micro-SSD (que custam entre R$20,00 e R$100,00, dependendo da capacidade).

As câmeras variam em sua capacidade, resolução dos filmes, duração de bateria e capacidade de comunicação (algumas delas, você vai perceber) podem inclusive se comunicar via sinal de Wi-Fi).

Uma boa configuração teria que ter a capacidade de filmar em HD (1280x720), com bateria de duração de pelo menos 4h, e capacidade para SSDs de 64GB.

Tão importante quanto o equipamento é o processo:

- Os policiais deverão manter as câmeras na lapela o tempo todo. As câmeras deverão estar ligadas sempre que os policiais estiverem fora da viatura (a menos que estejam fora de serviço ou em intervalo de alimentação).
- Os policiais deverão submeter os cartões SSD todo dia ao final do expediente.
- A ausência de filmagens de ocorrências registradas ou relatadas pelo público gera sanções disciplinares contra os policiais (para garantir que todas as ocorrências serão registradas).

Assim, os policiais estarão monitorados, com suas ações gravadas, ainda que a revisão ocorra posteriormente. O processo de responsabilização garante que as gravações não deixarão de ser feitas, e o público – ciente de que as câmeras deverão esta ligadas, atuará também na fiscalização.

Além do efeito fiscalizatório, as gravações, ainda que analisadas depois, poderão fornecer elementos valiosos para a análise da efetividade do policiamento, permitindo que a corporação aja no sentido de fornecer elementos faltantes a título de treinamento, aferidos nas ações dos policiais.

Faça valer a pena

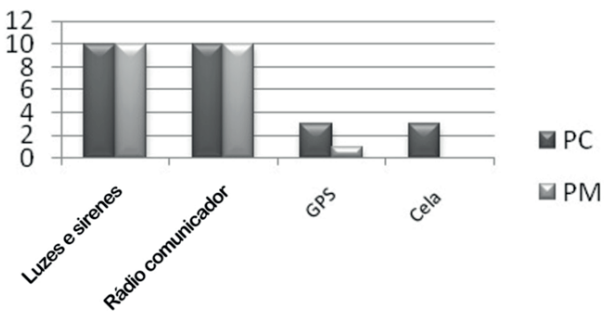
1. Em qualquer lugar do mundo – mesmo no Brasil – é possível adquirir um rádio capaz de captar comunicações policiais, dos bombeiros, e de serviços emergenciais. No geral, tais rádios nem custam tão caro, estando certamente ao alcance do cidadão mais interessado, apesar de não ser legal a operação desses dispositivos em faixas e protocolos reservados para o poder público.

Em teoria, um rádio sem autorização não poderia permitir que se ouça comunicações da polícia, bombeiros e outras agências de defesa pública. Qual das alternativas a seguir justifica o funcionamento desses rádios produzidos e comercializados clandestinamente?

a) Não há fabricantes não-autorizados, pois o governo não permite sua existência.
b) Os fabricantes clandestinos só estão na clandestinidade porque as licenças de produção estão expiradas, mas voltam à legalidade quando acertam sua situação.
c) O governo estimula o uso de rádios clandestinos, pois assim a população fica ciente do que está acontecendo
d) A criptografia foi quebrada, e já não é mais um segredo para os fabricantes de dispositivos originais.
e) O governo autoriza a produção desses rádios clandestinos pois se beneficia dos impostos coletados com suas vendas.

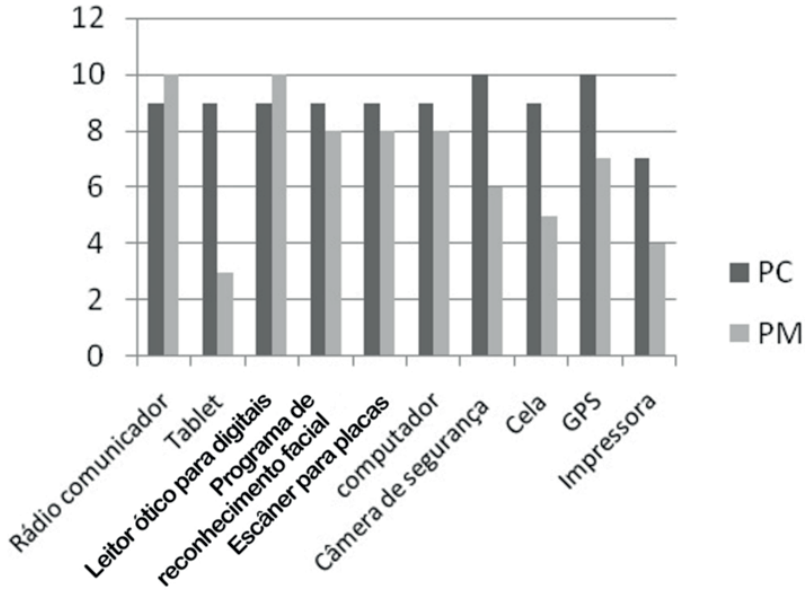
2. O gráfico 3.1, a seguir mostra os equipamentos presentes em viaturas policiais, enquanto o gráfico 3.2 mostra os equipamentos julgados úteis pelos policiais.

Gráfico 3.1 – Questionamento a Policiais (civis e militares quanto aos equipamentos disponíveis em viaturas)



Fonte: Bock, Pozzebon e Frigo (2016)

Gráfico 3.2 – Expectativa dos policiais quanto às tecnologias em suas viaturas



Fonte: Bock, Pozzebon e Frigo (2016)

Assinale a única alternativa a seguir que apresenta uma conclusão correta que se pode tirar acerca da comparação entre os dois gráficos.

a) A polícia nem sempre investe de maneira constante no aparelhamento das viaturas.
b) A maioria dos equipamentos solicitados pelos policiais são dependentes de TICs
c) Os equipamentos solicitados pelos policiais são obsoletos e não auxiliam no processo de policiamento
d) Os equipamentos solicitados pelos policiais são baratos e estão à disposição das forças policiais
e) De todos os equipamentos solicitados, apenas as impressoras são, de fato, úteis ao policiamento.

3. COPOM é a sigla dos Centros de Operação da Polícia Militar. Estes centros de operação são localizados em cada cidade com presença da Polícia Militar, e podem ser desde bem modestos: uma linha telefônica recebendo chamados da população, operada por um policial ou escrivão com acesso a rádio para coordenar ações com outros policiais, delegados e delegacias

de cidades vizinhas; até centros dedicados de atendimento e coordenação de ações policiais, com centenas de policiais operando equipamentos de última geração de comunicação e processamento, e coordenando ações em terra e ar (helicópteros da polícia).

Sobre o uso de TICs no COPOM, assinale a alternativa correta:

a) As TICs não têm utilidade para o COPOM, que já consegue o máximo de eficiência apenas com linhas telefônicas para atender as emergências
b) O COPOM só utiliza TICS autorizadas pelo Ministério da Educação, uma vez que é este órgão que determina o que pode ser usado para treinar os policiais
c) O COPOM utiliza TICs de acordo com seu porte e orçamento, podendo ser desde uma linha telefônica apenas, para uso do 190, até um centro completo de operações conectado via TICs
d) O COPOM não utiliza TICs nos dias de hoje devido à falta de padronização nas tecnologias existentes, que ainda não passaram por um processo de sedimentação adequado
e) O COPOM é obrigado por lei a adotar todas as TICs disponíveis comercialmente

Seção 3.3

TIC na inteligência e monitoramento

Diálogo aberto

Na seção anterior vimos como as TICs podem auxiliar, de maneira genérica, as atividades da segurança pública. Agora, é hora de nos concentrarmos em dois aspectos específicos dessa utilidade das TICs: os processos de inteligência policial e os processos de monitoração. Em ambos, as TICs têm um papel preponderante.

Você já percebeu que estamos sendo efetivamente "inundados" por uma quantidade gigantesca de dados gerados todos os dias? Cada transação comercial é registrada; a posição geográfica é conhecida pelos sistemas de GPS; as mensagens de WhatsApp são armazenadas; os hábitos de audiência do Netflix são armazenados (e usados para gerar novos filmes e séries pela empresa); os posts nas redes sociais são guardados para sempre. Esta absurda quantidade de dados pode ser vista como caótica, desconexa, intratável. Ainda assim, há sistemas de inteligência que conseguem identificar padrões e extrair desse caos todo muito conhecimento útil. A segurança pública já consegue se beneficiar desse processo de análise e correlação em grandes bases de dados, identificando suspeitos e situações potencialmente perigosas para o público. Exemplo disso é o programa HART, utilizado pela polícia inglesa para analisar a ficha corrida de um detento com o intuito de prever se, diante da possibilidade de sua soltura, ele é mais ou menos passível de reincidir em comportamento violento. O programa é um sucesso, conseguindo altas taxas de precisão na previsão do comportamento de ex-detentos ingleses. Nesse caso (como em tantos outros), o uso de tecnologias cibernéticas é mandatório, uma vez que a quantidade de dados a serem analisados e correlacionados é várias ordens de grandeza superior ao que o ser humano é capaz de lidar.

Outra preocupação proeminente é com a segurança e o sigilo das informações de segurança coletadas, processadas e trafegadas por várias redes. Trata-se de informações muito sensíveis, e que devem ser protegidas o tempo todo, sem exceção.

Retornando o nosso contexto de aprendizagem, nesta fase do projeto de segurança pública do novo Secretário, Frederico das Neves deverá endereçar uma preocupação da segurança das comunicações para o novo projeto de TICs: como garantir que as conexões do sistema sejam seguras, isto é, que as informações de segurança só sejam acessíveis por pessoas autorizadas? Nesse sentido, deverão ser usadas conexões seguras de comunicação, e você deverá auxiliar a Secretaria de Segurança Pública a escolher a melhor opção para tanto, incluindo esta solução no projeto de TICs sendo composto no momento.

Para auxiliar nessa tarefa, na presente seção você vai entender como funcionam os programas que auxiliam a inteligência policial, vai conhecer o papel das TICs nas conexões ultra-seguras, vai conhecer o papel das TICs na monitoração ambiental e, por fim, vai entender como se dá o monitoramento por satélite, conhecendo o sistema SISFRON.

Não pode faltar

A partir de agora vamos mergulhar em algumas aplicações de TICs em segurança pública. Veremos o papel preponderante que as mesmas estão assumindo cada vez mais na proteção a pessoas, patrimônio e recursos da nação.

Softwares e Modelos de Inteligência Policial

Junior e Dantas (2006) mostram que a atividade de segurança pública – em especial a atividade policial – vem sendo beneficiada pelos avanços da Tecnologia da Informação. Os autores citam a mineração de dados em grandes bases de dados como grande exemplo desses avanços. Mineração esta que permite a identificação de comportamentos delitivos, o que antes da utilização de computadores e softwares específicos era impossível, dado o volume intratável de dados a serem analisados (sob o ponto de vista da capacidade humana).

Este novo campo de estudos é chamado Análise de Vínculos, cujo objetivo é encontrar padrões de comportamento em documentação disponível publicamente sobre um indivíduo ou organização, determinando, entre estes padrões, os vínculos que, potencialmente, levarão este indivíduo ou organização a um comportamento delitivo, em futuro próximo.

Este tipo de análise se alicerça sobre a Inteligência Artificial, ramo da Ciência da Computação que se preocupa com o desenvolvimento de técnicas e métodos pelos quais os computadores possam exibir qualidades cognitivas que se assemelhem à inteligência humana (JUNIOR & DANTAS, 2006).

Os autores apontam cinco áreas de desenvolvimento da Inteligência Artificial:

- **Jogos por computador** – em que o sistema exiba características de aprendizado, ganhando experiência a cada partida (Xadrez, Damas, Go, entre outros).
- **Sistemas especialistas** – em que os sistemas são programados para tomar decisões com base em informações prévias (sistemas de diagnóstico médico, sistemas de análise financeira em mercado de capitais, entre outros).
- **Linguagens naturais** – sistemas que permitem a interação entre o ser humano e o computador em sua língua nativa, sem a necessidade de que o humano aprenda linguagens de programação ou se expresse de maneira mecânica para ser compreendido (assistentes virtuais como SIRI e Alexa, entre outros).
- **Robótica** – desenvolvimento de capacidade de interação dos sistemas cibernéticos com o mundo real por meio de visão, audição e tato artificiais (novamente os assistentes artificiais, como SIRI e Alexa, entre outros)
- **Redes neurais** – sistemas que simulam a inteligência humana por meio de elementos, que por sua vez simulam os neurônios e as conexões entre eles no cérebro humano. Estas redes enfraquecem ou fortalecem as conexões (ou vínculos) entre os neurônios artificiais em resposta a estímulos. Este enfraquecimento ou fortalecimento, quando estendido a toda uma rede neural, efetivamente permite que esta rede aprenda com o processo.

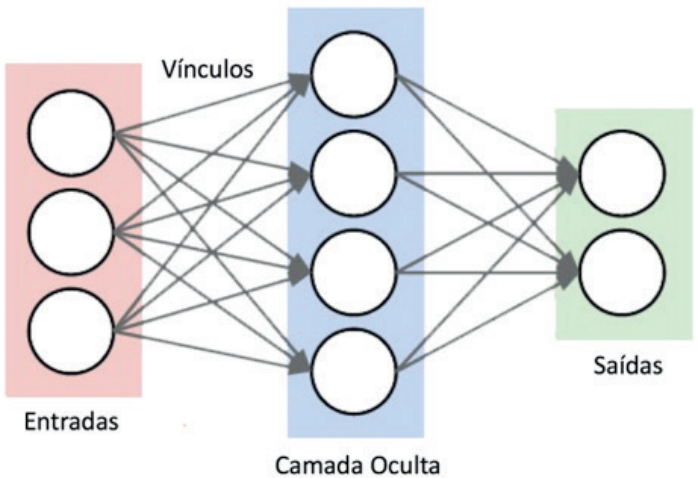
Assimile

Nos estudos de segurança pública, em especial de Criminalística, Análise de Vínculos diz respeito à capacidade de se encontrar padrões de comportamento em documentação disponível publicamente sobre

um indivíduo ou organização, determinando entre estes padrões os vínculos que potencialmente levarão estes a um comportamento delitivo, em futuro próximo.

A metodologia da Análise de Vínculos permite que uma rede neural seja alimentada por informações de comportamento de um indivíduo ou organização cujo comportamento futuro tenha (ou não) sido delitivo. Esta última informação não é alimentada no sistema. Os programadores da rede então perguntam se aquele conjunto prévio de comportamentos levará a algum comportamento delitivo. Após o sistema responder "sim" ou "não", a resposta correta é inserida, o que permite que o sistema ajuste os pesos de suas conexões internas, aumentando a força daquelas que colaborariam para a resposta correta, e enfraquecendo aquelas que colaborariam para a resposta errada. A Figura 3.10, a seguir, ilustra uma rede neural hipotética:

Figura 3.10 | Uma rede neural hipotética



Fonte: elaborada pelo autor.

A Figura 3.10 representa uma rede neural hipotética com as seguintes características:

- **Camada de Entrada** – nesse caso formada por três nós. Cada nó da camada de entrada recebe um dado qualquer

que pode, por exemplo, ser a resposta a uma pergunta afirmativa/negativa. Um exemplo: "o indivíduo em questão sofreu violência física na infância?"

- **Camada Oculta** – uma rede neural pode ter mais de uma camada oculta, é bom frisar. Esses nós ocultos representam a rede neural, simulando a interconexão de neurônios. Estes contêm o peso dos vínculos de entrada e saída, e são "treinados" para aumentar ou diminuir o peso desses vínculos.
- **Vínculos** – caminhos que ligam os nós da rede neural. Em seu conjunto, vão facilitar ou dificultar que uma resposta na camada de saída seja dada.
- **Camada de Saída** – conjunto de respostas fornecidas pela rede neural. A comparação das respostas obtidas pela rede com a resposta real gera um processo de feedback, que enfraquece os vínculos que gerariam a resposta errada e fortalece os vínculos que gerariam a resposta certa ao longo de toda a rede neural (isto é, envolvendo todos os vínculos).

Após vários milhares de cenários de teste, por meio dos quais o sistema é treinado, o que ocorre é que as respostas corretas vão se tornando a praxe. Quando estas respostas corretas ultrapassam algum limite determinado pelos administradores do sistema – em geral superior a 90% dos casos – o sistema é considerado adequado para uso preditivo.

Exemplificando

Um exemplo em que este tipo de ferramenta de inteligência policial já está sendo usado é fornecido pela British Telecom (2017). A polícia da cidade de Durham, no Reino Unido, está utilizando uma rede neural de Análise de Vínculos para decidir se atribui ou não liberdade condicional a detentos sob sua custódia. O sistema funciona com base na análise de um conjunto de informações sobre o detento em questão, informações essas coletadas pelo próprio sistema judiciário de Durham (excluindo crimes e ocorrências de fora de Durham, os autores fazem questão de frisar para que tenham controle total sobre a qualidade das informações). Com base nessas informações o sistema prevê se o detento em questão é passível de cometer outros atos

delitivos mediante uma potencial liberdade condicional. O sistema é conservador, isto é, quando a probabilidade de saída é dúbia, decide por negar a condicional, uma vez que é uma questão de segurança pública. Apenas quando é claro para o sistema que o detento em questão não trará perigo para a sociedade, o detento é solto. O sistema tem taxas de acerto altas:

- Está correto em 98% dos casos em que aponta que um detento apresenta baixo risco para a sociedade;
- Está correto em 88% dos casos em que aponta que um detento apresenta alto risco para a sociedade

TIC nas Conexões Ultra Seguras

Singh (2002) aponta para um fato interessante ocorrido durante a Segunda Guerra Mundial. Tanto os Aliados quanto o Eixo tinham equipes cuja missão única era encontrar cabos de comunicação do inimigo e inutilizar esses cabos. O motivo era simples: a comunicação por meio de cabos – naquela época, no início da década de 1940 – era considerada segura e confiável. Sem os cabos, afirma o autor, as comunicações deveriam ocorrer por meio de ondas de rádio, o que as tornava menos confiáveis (mais ruídos, menos alcance, etc.) e, principalmente, acessíveis por quem quer que tivesse um aparelho de rádio, ou seja: qualquer um poderia escutar as comunicações do inimigo.

Este quadro, afirma Singh (2002), impulsionou o desenvolvimento de mecanismos que impedissem que qualquer um tivesse acesso a comunicações, tornando-as privadas mesmo que o meio de acesso (a atmosfera) fosse público, permitindo o acesso de quem quer que fosse.

Exemplificando

Diante da impossibilidade de evitar que o inimigo compreendesse as comunicações no campo de batalha no Pacífico, durante a Segunda Guerra Mundial, os EUA desenvolveram uma estratégia engenhosa de "criptografia": treinaram nativos da tribo Navajo, nativa do estado do Novo México, para se comunicarem usando sua língua nativa. A língua Navajo era impermeável à tradução, e garantia sigilo nas comunicações. Este mecanismo nunca foi quebrado pelas forças inimigas durante todo o período em que foi utilizado na Segunda Guerra Mundial (SINGH, 2002).

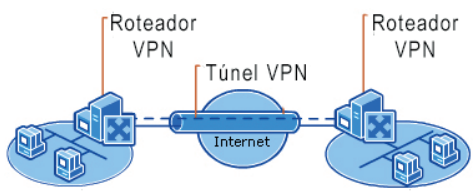
As primeiras barreiras tecnológicas utilizadas para proteger as TICs foram a frequência de comunicação, apesar de bastante ineficientes. Quem quisesse escutar a conversa de duas partes precisaria saber em que frequência ela ocorre. A dificuldade para burlar esse tipo de barreira desapareceu quando foi inventado o dial. Nada diferente dos botões giratórios dos rádios de hoje em dia, estes dispositivos permitem a varredura de todo o espectro de transmissão, e encontrar a frequência correta é uma questão de tempo e paciência.

Em seguida, os chamados scramblers foram inventados e passaram a ser usados em telecomunicações sigilosas. Os scramblers funcionam por meio da transposição e inversão de frequências e amplitudes, utilizando uma lógica restrita aos aparelhos que transmitem e são autorizados a receber as mensagens. O mecanismo funciona como a criptografia de chave privada – que vimos na seção 1 desta unidade 3–, uma vez que a forma e sequência de inversões e transposições funciona como uma chave secreta, de conhecimento apenas das partes autorizadas.

Este mecanismo, tal como é o caso de todos os mecanismos baseados em chaves privadas, sofre de problemas graves, como já discutido: não é possível autenticar o emissor da mensagem e, uma vez comprometida a chave, qualquer um que tenha um scrambler e o configure da maneira correta pode ouvir a conversa.

Esta questão crucial do sigilo das telecomunicações só foi resolvida com o advento dos mecanismos de chave pública, que permitiu o surgimento de uma das mais úteis e confiáveis tecnologias de comunicação segura: as VPN, (Virtual Private Networks), ou redes virtuais privadas. Hoje em dia, os roteadores que permitem a comunicação entre redes são dotados da capacidade de estabelecer e manter VPN, o que tira da esfera de responsabilidade do usuário a decisão sobre como e quando criptografar suas comunicações. A Figura 3.11, a seguir, ilustra como se dá o tunelamento VPN:

Figura 3.11 | Duas redes se comunicando via tunelamento VPN



Fonte: elaborada pelo autor.

Uma VPN é estabelecida entre duas entidades comunicantes quando as mesmas (sejam elas rádio, telefones ou computadores) realizam os seguintes passos:

1. As entidades comunicantes iniciam o protocolo de comunicação trocando certificados digitais atestando sua autenticidade;
2. Uma vez identificadas, as duas partes trocam chaves públicas de criptografia.
3. De posse das chaves públicas mútuas (que são seguras, porém lentas), ambas as partes entram em acordo sobre uma chave privada a ser usada (que permite comunicação bem mais rápida), protegidas pela criptografia de chave pública.
4. Decidida a chave privada, as chaves públicas podem ser descartadas, e a comunicação efetiva tem início. A chave pública é usada apenas para a seção corrente, pois mesmo que seja decifrada (o que demora, no mínimo vários meses ou mesmo anos), já não terá validade alguma para comunicações correntes.

Reflita

Seria útil ter dois locais ultras seguros se comunicando por um meio inseguro sem garantia de sigilo entre as comunicações? Comparando essa situação hipotética com o que costumam dizer os especialistas em segurança: a corrente sempre quebra no elo mais fraco, você consegue estabelecer um paralelo? Qual o elo fraco, nesse caso? Como pode ser fortalecido?

TIC e Fiscalização Ambiental

As TICs são neutras quanto à sua aplicação, obviamente. Uma vez desenvolvidas, podem ser aplicadas para resolver uma miríade de problemas. É interessante notar que, por exemplo no caso dos computadores pessoais, a tecnologia para auxiliar o usuário – aplicativos de produtividade – é apenas alguns poucos mais antiga que a tecnologia desenvolvida apenas para gerar o caos – vírus, vermes e malware em geral.

Da mesma maneira, no que concerne o meio ambiente, as TICs podem ser usadas também em benefício do cidadão e do país.

As Polícias Militares Estaduais, por exemplo, mantêm

departamentos internos dedicados às ocorrências que dizem respeito ao Meio Ambiente. Como informa o Sistema Ambiental Paulista [s.d.], por exemplo, as ocorrências ambientais serão atendidas pela unidade de Polícia Militar Ambiental, integrante do SISNAMA (Sistema Nacional do Meio Ambiente), órgão federal pertencente ao Ministério do Meio Ambiente.

Entre as TICs utilizadas para auxílio na fiscalização ambiental, devemos começar, claro, pela própria Internet, amplamente utilizada tanto para a dispersão de informações, quanto para facilitar a interação do cidadão com os órgãos governamentais de fiscalização. O site da Polícia Militar Ambiental da PMESP (Polícia Militar do Estado de São Paulo), por exemplo, oferece vários serviços, como pode ser visto na Figura 3.12, a seguir:

Figura 3.12 | Serviços oferecidos no site da Polícia Militar Ambiental da PMESP:

Fonte: <http://www3.policiamilitar.sp.gov.br/unidades/cpamb/>. Acesso em 26 nov. 2017.

Os serviços de TICs oferecidos pela Polícia Ambiental de São Paulo (e pelas polícias ambientais de vários outros estados, também, obviamente) compreende:

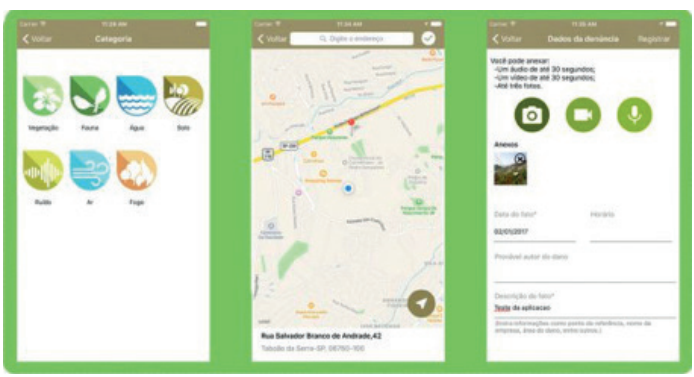
- **Redes Sociais** – interação da PMA com o cidadão por meio de uma página do Facebook, em que a PMA divulga suas ações e interage com quem se cadastra na página
- **Atividades e Serviços** – página que divulga os serviços prestados pela PMA, para consulta
- **Denúncia** – página para denúncias anônimas de ocorrências (crimes) na área ambiental. As denúncias preservam o anonimato do denunciante.
- **Localização de Unidade** – página usando a tecnologia de geolocalização do Google (Google Maps). A Figura 3.13, a seguir, mostra a localização do escritório da RMC (Região Metropolitana de Campinas). O mapa é interativo, e dá a informação referente à região clicada.

Figura 3.13 | Serviço de localização de escritório da Polícia Ambiental no Estado de São Paulo

Fonte: <http://www3.policiamilitar.sp.gov.br/unidades/cpamb/>. Acesso em 26 nov. 2017.

A Polícia Ambiental do Estado de São Paulo disponibiliza, ainda, um aplicativo para smartphones para denúncias ambientais. Disponível em sistemas operacionais Android e iOS, o aplicativo é gráfico e de fácil uso. A Figura 3.14, a seguir, ilustra o ícone do aplicativo e algumas telas de funcionamento. O aplicativo leva o nome de Denúncia Ambiente, e é gratuito.

Figura 3.14 | Aplicativo para celular Denúncia Ambiente



Fonte: <http://www.ambiente.sp.gov.br/2017/04/26/secretaria-lanca-aplicativa-para-denuncias-ambientais/>. Acesso em 26 nov. 2017.

A Polícia Ambiental do Estado de São Paulo é apenas um dos vários exemplos de unidades policiais brasileiras que se prestam a proteger o Meio Ambiente e, para tanto, se servem de TICs como ferramentas de apoio. As polícias de todos os Estados contam com unidades de proteção ambiental ligadas ao (e coordenadas pelo) SISNAMA.

Monitoramento por Satélite – SISFRON

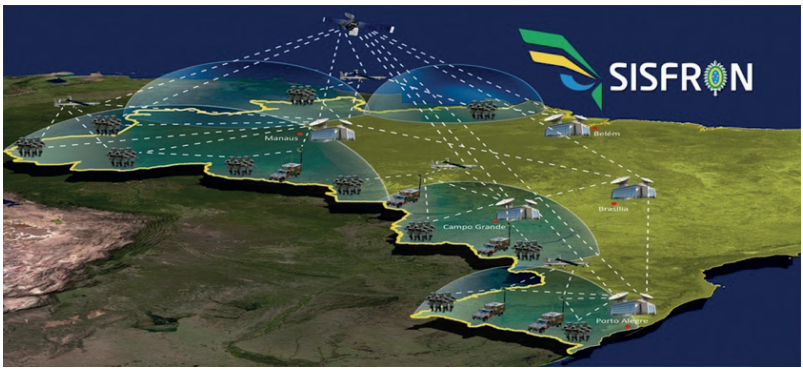
Sendo o maior país da América do Sul e, consequentemente, o país com maior extensão de fronteira, a vigilância desse território e, em especial, dessas fronteiras, é um trabalho hercúleo e constante (LANDIM, 2015).

De fato, o Brasil tem 23.102km de fronteiras, com 15.735km desse total sendo terrestres. Nosso País faz fronteira com quase todos os países da América do Sul, com exceção do Chile e Equador. Acompanhar as movimentações fronteiriças ao longo desses quase 16 mil quilômetros não seria possível sem as TICs. Em especial, como afirma Landim (2015), a tecnologia de satélites é fundamental nessa tarefa. Para tanto, foi desenvolvido o Sistema Integrado de Monitoramento de Fronteiras Terrestres, o SISFRON, combinando

- **Tecnologia de satélites** – no caso, o sistema todo é integrado por meio do BrasilSat, o satélite geoestacionário que orbita o planeta sobre o território brasileiro
- **Tecnologia de transmissão e recepção de dados** – via estações terrestres (por meio de antenas direcionais parabólicas de pequeno diâmetro)
- **Centro de Comando** – localizado em Brasília, coordenado pelo Exército, tem o papel de receber as informações e coordenar ações estratégicas e táticas
- **Centros Regionais** – localizados em Manaus, Campo Grande e Porto Alegre, coordenando as forças das sub-regiões sob sua tutela
- **Força Terrestre** – coordenada pelo centro de comando, a Força Terrestre é dividida em grupos com alto poder de coordenação, ação e mobilidade, localizadas em pontos estratégicos próximos às fronteiras, cobrindo uma faixa de aproximadamente 100kn de largura ao longo de toda a fronteira brasileira.

A Figura 3.15, a seguir, ilustra o SISFRON:

Figura 3.15 | Imagem ilustrativa do SISFRON



Fonte: <http://www.epex.eb.mil.br/images/Logomarcas/sisfron.jpg>. Acesso em 28 nov. 2017.

Pesquise mais

Em Landim (2015), nas páginas 140 a 143, você verá como o SISFRON é uma ferramenta primordial para a ampliação da diplomacia militar brasileira. Disponível em <https://periodicos.ufpe.br/revistas/politicahoje/article/view/3737/3039>. Acesso em 27 nov. 2017.

Sem medo de errar

Vamos dar continuidade ao nosso Projeto Simples de TIC na Segurança Pública, o nosso produto. Com o objetivo de implantar conexões ultra-seguras nas comunicações da Secretaria de Segurança Pública, o secretário Frederico das Neves poderá coordenar um projeto que se inicia com a adesão de roteadores com a capacidade de estabelecimento de VPNs em todos os escritórios da Secretaria de Segurança Pública. Podemos ter os seguintes pontos abordados no Quadro 3.3 que se segue.

Quadro 3.3 | Projeto de Tecnologia de Informação e Comunicações 3ª Parte

PROJETO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÕES – 3º PARTE (Apenas os Principais Aspectos)
OBJETIVO ESTRATÉGICO GERAL DO PROJETO: • Reduzir os índices de criminalidade, implementando ações de TICs.

ONDE: Escritórios da Secretaria de Segurança Pública

ONDE: Capital e cidades satélites

RESPONSÁVEIS: Sr. Frederico das Neves

AÇÕES A REALIZAR:

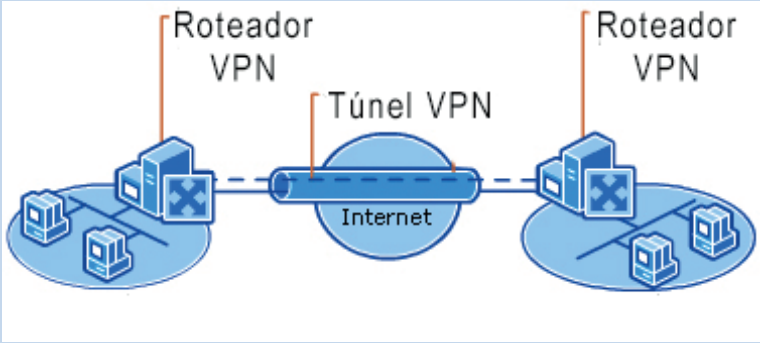
A VPN será estabelecida entre duas entidades comunicantes da Secretaria de Segurança Pública ou desta com órgãos com a mesma capacidade, quando as mesmas realizarem os seguintes passos:

1. As entidades comunicantes iniciam o protocolo de comunicação trocando certificados digitais atestando sua autenticidade;
2. Uma vez identificadas, as entidades comunicantes trocam chaves públicas de criptografia.
3. De posse das chaves públicas mútuas (que são seguras, porém lentas), ambas as partes entram em acordo sobre uma chave privada a ser usada (que permite comunicação bem mais rápida), sempre protegidas pela criptografia de chave pública.
4. Decidida a chave privada, as chaves públicas podem ser descartadas, e a comunicação efetiva tem início. A chave pública é usada apenas para a seção corrente, pois, mesmo que seja decifrada (o que demora, no mínimo vários meses ou mesmo anos), já não terá validade alguma para comunicações correntes.

Em adição, o projeto deve prever a integração do tunelamento VPN com os certificados digitais, já adotados previamente, garantindo que todo o material trafegado pela rede da Secretaria da Segurança Pública conta com mais uma camada de proteção: todo o material trafegado, sendo acompanhado de certificados digitais, terá sua proveniência, sigilo, integridade e autenticidade garantidos.

A Figura 3.10, a seguir, ilustra uma implantação de tunelamento VPN, a ser adotada nas comunicações da Secretaria de Segurança Pública.

Figura 3.10 | Duas redes se comunicando via tunelamento VPN



Fonte: elaborada pelo autor.

A adoção de VPNs garante a criptografia das comunicações por meios que só podem ser considerados inseguros: os canais de comunicação da Internet.

QUANDO: implantados até o ano de 2018.

FINALIDADE: Garantir proteção, sigilo, integridade e autenticidade de todo o material trafegado pela rede da Secretaria da Segurança Pública.

As informações acima podem ser apresentadas na forma de um projeto simples para o Sr. Frederico. Para tanto, um outro formato possível (não é o único, claro) seria apresentar essas informações em um documento com a seguinte organização:

1. Nome do Projeto
2. Nome do Responsável
3. Data da apresentação
4. Atividades para implantação do projeto, descritas e discriminadas individualmente
5. Tempo de início e de fim para cada atividade, discriminados individualmente
6. Responsável por cada atividade (com informações de contato)
7. Estimativa de custos esperados
8. Um cronograma de resumo das informações acima

Por meio da adoção de servidores de VPN, as comunicações da Secretaria de Segurança Pública estarão garantidas contra escutas e outras intervenções, todas indesejáveis. O tunelamento VPN garante o sigilo, a integridade e a autenticidade das comunicações da Secretaria de Segurança Pública. E com isso, o Sr. Frederico das Neves está com seu projeto de TICs bem mais robusto!

Avançando na prática

Ajudando a preservar contra o desmatamento predatório

Descrição da situação-problema

O sr. Geraldo Lima é morador de uma propriedade adjacente ao "Parque dos Jequitibás", uma área de preservação pertencente ao Estado, que compreende uma longa extensão de Mata Atlântica.

Recentemente o sr. Geraldo tem percebido movimentações estranhas no parque e, em recente caminhada com sua esposa, chegou a uma clareira onde vestígios de desmatamento são evidentes. Alguns dias depois, a área desmatada aumentou, e o sr. Geraldo decidiu procurar a Polícia Ambiental, onde foi atendido pelo Capitão Cerqueira, responsável pela unidade local.

Como o Capitão Cerqueira pode auxiliar o sr. Geraldo a colaborar de forma mais eficiente para que o desmatamento predatório identificado seja combatido?

Resolução da situação-problema

O Capitão Cerqueira poderá sugerir ao sr. Geraldo, que é proprietário de um smartphone simples, (mas que por mais simples e barato que seja, é capaz de executar o sistema operacional Android), a adotar o aplicativo gratuito da Polícia Florestal.

Com esse aplicativo, o sr. Geraldo poderá registrar futuras ocorrências, transmitindo-as de imediato para a Polícia Florestal, de forma que a ação da unidade local seja mais rápida e eficiente.

O Capitão Cerqueira poderá, também, indicar ao sr. Geraldo o telefone do disque denúncia ambiental, disponível naquela região, e que pode ser usado a qualquer hora do dia ou da noite para denúncias de crimes ambientais.

Pronto! A partir de agora o sr. Geraldo poderá ser mais eficiente em sua colaboração contra os crimes ambientais que porventura venham a ocorrer na região.

Faça valer a pena

1. A atividade de segurança pública – em especial a atividade policial – vem sendo beneficiada pelos avanços da Tecnologia da Informação. A mineração de dados em grandes bases de dados como grande exemplo desses avanços. Mineração esta que permite a identificação de comportamentos delitivos, o que antes da utilização de computadores e software específico era impossível, dado o volume intratável de dados a serem analisados (sob o ponto de vista da capacidade humana).

Assinale a alternativa que contém a denominação correta para a capacidade de se encontrar padrões de comportamento em documentação disponível publicamente sobre um indivíduo ou organização, determinando entre estes padrões os vínculos que potencialmente levarão este indivíduo ou organização a um comportamento delitivo, em futuro próximo:

a) Análise de Padrões
b) Vinculação de Padrões
c) Análise Combinatória
d) Análise de Vínculos
e) Inteligência Artificial

2. Observe os passos a seguir, para estabelecimento de uma VPN para comunicação segura:

1. Decidida a chave privada, as chaves públicas podem ser descartadas, e a comunicação efetiva tem início. A chave pública é usada apenas para a seção corrente, pois mesmo que seja decifrada (o que demora, no mínimo vários meses ou mesmo anos), já não terá validade alguma para comunicações correntes.
2. Uma vez identificadas, as entidades comunicantes trocam chaves públicas de criptografia.

3. As entidades comunicantes iniciam o protocolo de comunicação trocando certificados digitais atestando sua autenticidade;
4. De posse das chaves públicas mútuas (que são seguras, porém lentas), ambas as partes entram em acordo sobre uma chave privada a ser usada (que permite comunicação bem mais rápida), sempre protegidas pela criptografia de chave pública.

Assinale a alternativa que estabelece a correta sequência para estabelecimento da VPN:

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

3. Observe os elementos a seguir:

I. Tecnologia de satélites – no caso, o sistema todo é integrado por meio do BrasilSat, o satélite geoestacionário que orbita o planeta sobre o território brasileiro
II. Centro de Comando – localizado em Brasília, coordenado pelo Exército, tem o papel de receber as informações e coordenar ações estratégicas e táticas
III. Análise Descentralizada – o cidadão é convidado a analisar e fiscalizar os dados coletados, por meio de aplicativo para smartphone (Android e iOS), contribuindo para a fiscalização das fronteiras
IV. Força Terrestre – coordenada pelo centro de comando, a Força Terrestre é dividida em grupos com alto poder de coordenação, ação e mobilidade, localizadas em pontos estratégicos próximos às fronteiras, cobrindo uma faixa de aproximadamente 100km de largura ao longo de toda a fronteira brasileira.

Avaliando os elementos acima, assinale a alternativa que contém apenas aqueles que fazem parte do SISFRON

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

Referências

ALMEIDA, C., **Estudo: a importância de um mobiliário adequado para CFTV**, Site do Instituto CFTV, 2014. Disponível em <http://institutocftv.com.br/estudo-de-mobiliario-para-cftv---ellan.html>. Acesso em 19 nov. 2017.

BAYLEY, D. H., STENNING, P. C, **Governing the police: experience in six democracies**, Nova York: Routledge, 2016.

BOCK, E. C., POZZEBON, E., FRIGO, L. B., **Propostas para informatização de viaturas policiais como instrumento de segurança pública**, In: SPANHOL, F. J., LUNARDI, G. M., SOUZA, M. V., Tecnologias da Informação e Comunicação na Segurança Pública e Direitos Humanos, São Paulo: Blucher, 2016.

BRITISH TELECOM, **Durham Police to use artificial intelligence to aid custody decisions**, Site British Telecom, publicado em 25 mai. 2017. Disponível em <http://home.bt.com/tech-gadgets/future-tech/durham-police-harm-assessment-risk-tool-artificial-intelligence-custody-11364179599262>. Acesso em 26 nov. 2017.

BUCHMANN, J. A., KARATSIOLIS, E., WIESMAIER, A., **Introduction to Public Key Infrastructures**, Nova York: Springer, 2013.

CORRÊA, R., **Boletim de Ocorrência Online: como fazer o B. O. pela Internet?**, Site Rafael Corrêa, 2015. Disponível em <http://rafaelcorrea.com.br/boletim-de-ocorrencia-online/>. Acesso em 13 nov. 2017.

EPEX, **Integrando capacidades na vigilância e na atuação em nossas fronteiras**. Site do Escritório de Projetos do Exército, s. d. Disponível em <http://www.epex.eb.mil.br/index.php/sisfron>. Acesso em 27 nov. 2017.

FERRÚS, R., SALLENT, O., **Mobile broadband communicationsfor public safety: the road ahead through LTE technology**, Londres: Wiley, 2015.

GREENVILLE, Polícia de Greenville, Carolina do Sul, **Body-Worn Camera** Project, Site da Polícia de Greenville, 2017. Disponível em <https://www.greenvillesc.gov/1180/Body-Worn-Cameras-Project>. Acesso em 18 nov. 2017.

IDENTITYONE, **Fingerprint Technology Overview**. Site IdentityOne, s/d. Disponível em <http://www.identityone.net/BiometricTechnology.aspx>. Acesso em 13 nov. 2017.

JÚNIOR, C. M. F., DANTAS, G. F. L., **A descoberta e a análise de vínculos na complexidade da investigação criminal moderna**. Adquirido no site do Ministério da Justiça (http://www. mj. gov. br), 2006. Disponível em <http://egov.ufsc.br/portal/sites/default/files/anexos/13124-13125-1-PB.pdf>. Acesso em 25 nov. 2017.

LANDIM, H. G. C., **SISFRON: ferramenta de ampliação da Diplomacia Militar brasileira e fortalecimento do CDS**. Revista Política Hoje, vol. 24, n. 1, pp. 135-147. Publicado em 2 set. 2015. Disponível em <https://periodicos.ufpe.br/revistas/politicahoje/article/view/3737/3039>. Acesso em 27 nov. 2017.

LIMA E. B., **Elaboração de um sistema de indicadores de desempenho para o centro de operações policiais militares – COPOM/PMGO**, 2 jul. 2004, 130 fls., Dissertação, Universidade Estadual de Campinas, Campinas, 7 jul. 2004.

MANTONI, D., MAIO, D., JAIN, A. K., PROBHAKAR, S., **The Handbook of fingerprint recognition**, 2a ed., Londres: Springer-Verlag, 2009.

MARTINS, **E., O que é biometria?**, Site TecMundo, publicado em 19 nov. 2009. Disponível em <https://www.tecmundo.com.br/o-que-e/3121-o-que-e-biometria-.htm>. Acesso em 13 nov. 2017.

ROSA, E., **Redes sociais são aliadas da Segurança Pública**, Diário Gaúcho, publicado em 12 maio 2015. Disponível em <http://diariogaucho.clicrbs.com.br/rs/policia/noticia/2015/05/redes-sociais-sao-aliadas-da-seguranca-publica-4758637.html>. Acesso em 20 nov. 2017.

SINGH, S., **O Livro dos Códigos**, São Paulo: Record, 2002.

SISTEMA AMBIENTAL PAULISTA, **Polícia Militar Ambiental**, Site do Sistema Ambiental Paulista. Disponível em <http://www.ambiente.sp.gov.br/a-secretaria/instituicoes/policia-militar-ambiental/>. Acesso em 26 nov. 2017.

SPTC-SP, Superintendência da Polícia Técnico-Científica de São Paulo, **Certificação Digital**, Site da Polícia Científica, publicado em 2 mar. 2015, Disponível em <http://www.policiacientifica.sp.gov.br/laudo-digital/>. Acewsso em 13 nov. 2017.

SSPAP-PR, Secretaria da Segurança Pública e Administração Penitenciária do Paraná, **Polícia Científica já emite laudos oficiais assinados digitalmente**, Site da Polícia Científica do Paraná, publicado em 7 jun. 2016. Disponível em <http://www.policiacientifica.pr.gov.br/modules/noticias/article.php?storyid=122>. Acesso em 13 nov. 2017.

SSP-SP, Secretaria de Segurança Pública de São Paulo, Delegacia Eletrônica, Site da SSP-SP, 2017. Disponível em <http://www.ssp.sp.gov.br/nbo/>. Acesso em 13 nov. 2017.

Tecnologias aplicadas na segurança privada

Convite ao estudo

Olá!

Chegamos à última unidade de nosso livro didático. Até aqui você teve a oportunidade de conhecer vários aspectos das tecnologias digitais, aplicou esses aspectos à segurança e entendeu como essa tecnologia auxilia na segurança pública. Para fecharmos essa disciplina, é hora de entendermos como as tecnologias de informação e comunicação (Ticos) podem ser de imenso valor para a segurança no contexto privado.

Você já visitou alguma empresa em um condomínio empresarial? Se já fez isso, certamente já observou parte do aparato de segurança que faz parte do ambiente, não é verdade? Registro na portaria, crachá, catraca, seguranças observando o ambiente, e por aí vai. E olha que essa é só a "ponta do iceberg", no dizer popular. A grande maioria dos mecanismos e processos de segurança ocorre longe das vistas dos transeuntes, e efetivamente é esse conjunto de ações, processos e tecnologias que mantêm os ambientes seguros. Os crachás e as catracas são importantes, claro, mas a tecnologia que permite a efetiva identificação e também efetivamente controla o acesso dos presentes vai muito além deles. Você vai ver isso a partir de agora.

Lembrando que, identificando os principais aspectos da TIC na Segurança Pública e Privada, esta unidade tem o objetivo de dar condições de elaborar e implementar um Sistema de Monitoramento em Segurança. Ao final dela, você terá colaborado na produção de um projeto de monitoramento e controle de acesso.

O megaempresário Siderley Chubacy, fundador e sócio majoritário da empresa de tecnologia eletrônica Sider, acaba de anunciar planos ambiciosos para a construção de uma nova sede. Tendo adquirido uma área de 1 milhão de metros quadrados no novo distrito industrial da Capital, Siderley tem planos para criar uma planta moderna, confortável, e que seja um marco arquitetônico para a cidade.

Para tanto, ele está contratando os melhores provedores de soluções do mundo todo, desde arquitetos, empresas de engenharia, design de interiores e, obviamente, provedores de soluções de segurança. Sua empresa acaba de receber o convite para tornar a nova sede da Sider um local seguro, protegendo as pessoas e os segredos industriais que a sede abrigará. O sr. Siderley Chubacy espera que sua empresa apresente um projeto de monitoramento e controle de acesso à altura desse empreendimento monumental.

Como garantir a segurança em um empreendimento tão ousado e moderno? Que tecnologias e processos devem ser adotados? O que há de melhor no setor de segurança para oferecer a Siderley e à sua empresa?

Na primeira seção desta unidade, você vai conhecer um pouco mais de perto os elementos de uma solução de controle de acesso.

Na segunda seção, você vai se aprofundar nos elementos eletrônicos de controle de acesso.

Na terceira seção, vai entrar em contato com as soluções de TICs aplicadas à segurança privada.

Estamos quase lá. Vamos em frente!

Seção 4.1

Sistemas de monitoramento e controle de acesso

Diálogo aberto

Caro aluno,

Você já percebeu que para entrar em uma empresa não basta simplesmente chegar ao local e pedir instruções para chegar à sala certa? Já percebeu que antes de chegar ao local almejado você precisa se identificar e receber autorização para entrar? Pois então, esse é um procedimento padrão de qualquer empresa privada: mesmo que seja apenas uma secretária em uma mesa, ela vai lhe pedir para se identificar, e só vai liberar o acesso depois que se der por satisfeita sobre quem é você e o que vai fazer lá. Nada mais justo certo? Afinal de contas, ali trabalham pessoas e desenvolvem-se projetos que devem ser protegidos. Esse é o papel do controle de acesso.

Sua empresa foi convidada para participar do empreendimento da nova sede da Sider, sendo empresa global de tecnologia. Em seu projeto de segurança para nova sede, você deverá iniciar pelo mais primordial e básico: o controle de acesso. Seu projeto deverá especificar tecnologias que garantam que apenas as pessoas autorizadas terão acesso ao perímetro, aos ambientes e aos sistemas da Sider, e deve também conter uma justificativa para as soluções adotadas. Como controlar acesso à propriedade, considerando uma área tão grande? Como garantir que apenas pessoas autorizadas entrarão nos prédios? Como garantir que só entrarão nas áreas para as quais têm autorização? Como identificar que apenas pessoas autorizadas encontram-se em áreas sensíveis em algum momento arbitrário do dia? Essas e várias outras questões pertinentes ao controle de acesso deverão ser respondidas em seu projeto.

Para ajudá-lo, nesta seção, vamos analisar alguns dos aspectos, processos e tecnologias pertinentes ao controle de acesso em organizações privadas, cobrindo desde sensores de movimento, cercas e alarmes; passando por crachás eletrônicos e biometria; por rastreadores e fechaduras eletrônicas; até chegarmos a circuitos fechados de TV e centrais de segurança.

E então, vamos em frente?

Não pode faltar

A partir de agora você vai entender melhor como funcionam os processos e tecnologias pertinentes à segurança empresarial.

Porém, antes de entrar "de cabeça" nas tecnologias, é importante observar que, como afirmam Brasiliano e Blanco (2003), a segurança privada (a que os autores chamam Segurança Empresarial) deve ser implementada na empresa por meio de um planejamento, e não de ações baseadas nas tecnologias em si. Da mesma maneira que a empresa planeja suas ações estratégicas e este planejamento inclui, digamos, o planejamento das ações de marketing e o planejamento de vendas, também deve haver um planejamento que se encaixe no planejamento estratégico que especifique as medidas de segurança a serem adotadas.

De acordo com os autores, o planejamento de segurança deve ter as seguintes características (BRASILIANO e BLANCO, 2003): deve atender à Política de Segurança da Empresa (que é o documento mais importante de segurança dentro de uma corporação; deve ser considerado uma função administrativa, e, portanto, deve ter precedência no planejamento global da empresa; deve ter grande penetração e abrangência, uma vez que estabelece parâmetros para o funcionamento de inúmeras outras áreas da corporação; deve ter sempre como alvo a maximização da segurança e, por consequência, a minimização das deficiências de segurança.

Assimile

O projeto de segurança deve fazer parte do planejamento da empresa e estar adequado com o planejamento estratégico da dela.

Sensores de Movimento, Alarmes e Cerca Virtual

Brasiliano e Blanco (2003) definem o sistema de sensoriamento como sendo o conjunto de tecnologias que detectam ocorrências tanto no que concerne à segurança patrimonial (presenças de pessoas, movimentações de pessoas e movimentações de objetos) como a segurança contra incêndio (aumentos de temperatura, presença de gases oriundos da combustão).

Os autores alertam para o fato de que tão importante quanto a

detecção é a comunicação dos eventos detectados, o que implica que os sensores devem ser conectados à rede da empresa (ou organização) e devem ter seus dados transmitidos para um sistema centralizado que registra as ocorrências e toma providências de acordo com o teor e a gravidade de cada uma delas. São basicamente duas as maneiras de se conectar os sensores à rede e, consequentemente, aos sistemas de segurança:

- **Sensores cabeados** – Conectados à rede por meio de cabeamento padrão (categoria 5 ou categoria 6 de pares trançados, como no caso dos demais dispositivos de rede e processamento). Um mecanismo extra de detecção de flutuações de resistividade ou mesmo um mecanismo de sinalização tipo *watchdog* (por meio do qual o sistema espera que o sensor envie um sinal de "estou vivo" a cada 30 segundos, por exemplo) identifica se o sensor for removido ou desabilitado.
- **Sensores sem fio** – Conectados à rede por meio de sinal de rádio ou – preferencialmente – por meio de sinal Wi-Fi, com endereço IP, o que o configura como dispositivo da Iota (Internet *of Things*, ou, em português, Internet das Coisas). Sendo um dispositivo IP, pode ser acessado como tal, e pode enviar suas informações até mesmo para interfaces móveis e ser operado remotamente.

Uma vez conectados ao sistema, os sensores alimentam-no com as informações coletadas, e uma central permite a visualização em tempo real de todos os acontecimentos.

Os sensores podem ser divididos nos seguintes tipos (BRASILIANO e BLANCO, 2003):

- Sensores Internos
  - **Por abertura (contato magnético)** – Usados para proteger portas, janelas e outros elementos de passagem/armazenamento;
  - **Por vibração** – Provocam contato elétrico uma vez que são movidos. São a base dos sismógrafos e mesmo de dispositivos que identificam a movimentação de objetos que devem permanecer estacionários (maquinário, por exemplo);

- **Por ruído** – Sensores baseados no efeito de microfonia, transformando vibrações sonoras em sinais elétricos como no caso dos microfones;
- **Por temperatura** – Identificam variações de temperatura pelo efeito de expansão e/ou contração de ligas metálicas;
- **Por variações químicas** – Identificam a presença e/ou ausência de elementos químicos no ambiente em que são instalados. O aumento de CO2, por exemplo, pode ser identificado, sendo um indício de incêndio;
- **Por variação de luminosidade** – Identificam mudanças mesmo que sutis na luminosidade do ambiente. Os movimentos de pessoas ou objetos em um ambiente, por exemplo, provocam variações de luminosidade que são facilmente detectáveis por esse tipo de sensor;
- **Por variação de frequência infravermelha** – Sensores que identificam pequenas variações de calor no ambiente. Diferentemente dos sensores de temperatura, esses sensores identificam variações bem mais sutis também ligadas ao movimento de corpos no ambiente.

- Sensores Externos
  - **Infravermelho ativo** – Emitem feixes de raios infravermelhos e aguardam pela leitura do sensor que recebe o sinal de volta, após sua reflexão em objetos próximos ou distantes;
  - **Cerca eletrificada** – Agem tanto como elemento de prevenção como de detecção. Além de emitir pulsos elétricos que provocam choques, as cercas eletrificadas identificam o ponto em que a invasão ocorre, uma vez que ocorra o curto-circuito entre cabos;
  - **Cabos microfônicos e de rádio frequência** – Instalados em Cercas Elétricas como sensores para identificar invasões. Não dependendo de curtos-circuitos elétricos, são mais eficientes em detecção de invasões;
  - **Câmeras** – (Podem ser usadas interna e externamente, claro). Permitem a vigilância perimetral sem a necessidade de rondas, ou mesmo complementando as rondas;

- **Espiras eletromagnéticas** – Instaladas sobre a pavimentação de rodagem, identificam a movimentação de veículos automotores.

Exemplificando

Um exemplo comum de sensor de variações químicas é o detector de fumaça, obrigatório em vários ambientes, em vários países. Trata-se de um dispositivo ativado pela presença de gases oriundos da combustão, que emite um som alto, contínuo e agudo, alertando para a presença de fumaça. Alguns desses dispositivos estão ligados via rede à Central de Segurança, permitindo que o evento sinalizado seja percebido e possa ser tratado mesmo à distância. A Figura 4.1, a seguir, mostra um dispositivo de detecção de fumaça:

Figura 4.1 | Detector de Fumaça

Fonte: <https://pixabay.com/pt/fumaça-detector-fogo-alarme-queima-315874/>. Acesso em: 10 nov. 2017.

Crachás Eletrônicos e Biometria

Os crachás e elementos de identificação biométrica fazem parte do sistema de controle de acesso de uma empresa, e devem estar integrados ao software que faz o registro de eventos de deslocamento autorizado em seu território. Mais especificamente, esses elementos permitem (ou negam) o acesso a ambientes diferentes daqueles ocupados pelos indivíduos em deslocamento. Dessa forma, se o indivíduo se encontra em um corredor ou hall e deseja se deslocar para uma sala, o ideal é que esta sala – caso contenha material ou pessoal

sensível ao negócio – seja protegida por um sistema de controle de acesso com base em algum elemento de identificação individual.

Brasiliano e Blanco (2003) assim tipificam esses elementos de controle de acesso:

- **Sistemas Manuais** – Sempre dependentes do elemento humano.
    - **Portarias Reais** – Locais de verificação de identidade operacionalizados por funcionários (porteiros) treinados para este papel. Os porteiros identificam o postulante por meio de documentação apropriada (documento de identificação ou crachá oficial da empresa). Em caso de falta de autorização, podem contatar funcionários.
- **Sistemas Semiautomáticos** – Misturam o elemento humano com elementos de automatização.
    - **Portarias Virtuais** – Locais de verificação em que os porteiros são substituídos por câmeras e portas trancadas abertas remotamente. Em local distante, os porteiros virtuais (pessoal treinado) fazem a identificação por câmera – identificação essa que pode ser corroborada por crachá, crachá eletrônico ou senha numérica a ser inserida em teclado eletrônico –, e garantem o acesso dos indivíduos autorizados.
    - **Sistemas de Senha/Contrassenha** – Quando da tentativa de acesso, o sistema emite uma senha para o postulante. Este responde com uma contrassenha (exemplo: cartões com tabelas de senhas temporárias utilizados por bancos). O profissional responsável pela garantia de acesso abre a porta para o postulante em caso de acerto, ou interage com ele em caso de erro.
- **Sistemas Automáticos** – Neste caso não há interação com seres humanos, e a garantia (ou negação de acesso) é realizada exclusivamente pelo sistema automatizado.
    - **Teclados Automáticos** – Teclados em que o postulante insere sua senha individual. Caso a senha esteja correta, o sistema permite o acesso (abre a porta). Duas vulnerabilidades deste sistema são a perda/esquecimento da senha ou a descoberta desta por parte de um indivíduo não autorizado.

- **Crachás eletrônicos** – Crachás chipados, isto é, contendo chips de processamento e antenas de transmissão, que enviam uma senha de acesso ao sistema quando são aproximados do sensor. O sensor, por sua vez, emite um campo eletromagnético que alimenta o crachá, permitindo a emissão da senha. Uma vulnerabilidade deste sistema é a perda ou o roubo do crachá que pode ser usado por algum indivíduo não autorizado.
- **Leitores Biométricos** – Identificam univocamente características biológicas do postulante, comparando-as com dados coletados pelo aparelho de leitura com dados armazenados em banco de dados do sistema. São vários os tipos de leitores biométricos, sendo que os mais comuns são: Leitores de digital; Leitores de veias da mão; Leitores de íris (olhos); Leitores de formato da face; Leitores assinatura (o postulante escreve sua assinatura em uma superfície sensível); Leitores de timbre de voz.

Rastreadores e Fechaduras Eletrônicas

Outro tipo de sistema de controle de acesso é o sensor de rastreamento, ou, como é popularmente conhecido, o rastreador. Trata-se de um mecanismo perfeito para localização de veículos, cuja precisão o torna útil na segurança de cargas e veículos de transporte de pessoas.

Silva (2017) nos mostra que o rastreador é uma tecnologia de sensoriamento baseada na rede GPS (*Global Positioning System*, ou, em português, Sistema de Posicionamento Global). O mecanismo funciona com base em um sensor instalado no veículo que, a todo tempo, está recebendo informações de satélite que lhe atribuem a localização geográfica real, com alguns poucos metros de imprecisão.

O sistema também é capaz de identificar se o dispositivo foi desabilitado, o que permite à central saber que há alguma coisa de errado com o veículo. Uma ligação para o celular do motorista com uma senha e contrassenhas previamente acordadas permitirá à central saber se está tudo bem, sendo um caso apenas de religar o rastreador, ou se de fato algo mais grave está acontecendo (roubo ou sequestro, por exemplo).

As fechaduras eletrônicas funcionam não com chaves mecânicas,

como utilizamos desde a Antiguidade, mas sim por meio de sinais eletrônicos que abrem o mecanismo de fechadura. Esses sinais são enviados apenas quando o indivíduo tentando abri-las conhece o código (senha). A Figura 4.2, a seguir, apresenta um dos vários modelos disponíveis no mercado:

Figura 4.2 | Fechadura Eletrônica

Fonte: <https://upload.wikimedia.org/wikipedia/commons/6/63/Electronic_lock_with_number_pad.jpg>. Acesso em: 9 dez. 2017.

Este tipo de fechadura pode, inclusive (dependendo do modelo), ser conectado à Central de Segurança, onde os eventos de abertura e tentativas frustradas podem ser registrados para auditorias futuras.

Diferentemente das fechaduras mecânicas, em que não é possível saber quem abriu a porta (uma vez que todas as chaves são iguais), a fechadura eletrônica permite essa identificação, já que cada usuário autorizado pode, no caso, ter uma senha diferente.

CFTV / Central de Segurança

Segundo Brasiliano e Blanco (2003), o principal valor dos circuitos fechados de TV – o verdadeiro valor das câmeras aparentes, geralmente

adotadas para este tipo de solução, é a dissuasão, ou seja, o fato de atuarem como agentes dissuasivos de situações indesejadas. Afinal de contas, qualquer comportamento fora da norma será capturado pelas câmeras. Nesse sentido, algumas empresas e mesmo usuários domésticos às vezes optam por soluções mais baratas, tais como as câmeras falsas, que nada mais são do que invólucros vazios, algumas vezes com uma lâmpada de LED (o que exige o uso de uma pilha) que fica acessa ou piscando o tempo todo. Os transeuntes não sabem diferenciar a câmera real da câmera falsa, e raros são os que arriscam um comportamento proibido, uma vez que temem ser identificados pelas supostas imagens.

No entanto, ainda que tal tipo de solução seja atrativo sob o ponto de vista de investimento, os custos de soluções reais, com câmeras baratas e integradas à rede TCP/IP, trazem inúmeras vantagens adicionais, entre elas: manutenção do efeito dissuasivo; registro efetivo de imagens que podem ser usadas em investigações forenses posteriores; integração, via protocolo TCP/IP, às demais soluções de sensoriamento e controle de acesso da empresa; integração com solução de portaria virtual.

Reflita

Uma das principais preocupações quando da adoção de soluções de circuito fechado de TV é o equilíbrio entre a segurança e o direito à privacidade. Em uma empresa financeira, por exemplo, onde seria apropriado implantar câmeras? Onde a implantação de câmeras configuraria invasão de privacidade?

Pesquise mais

Para saber mais sobre a integração de um projeto de monitoração e controle de acesso, você pode consultar este sucinto, porém completo, artigo de Da Cruz (2017), intitulado "Proposta de Projeto: Sistema de Segurança Eletrônica", publicado em 2017 pela *Universidade do Planalto Catarinense*, SC. Concentre-se nas páginas de 10 a 23.

Disponível em <https://revista.uniplac.net/ojs/index.php/engeletrica/article/download/3029/1201>. Acesso em: 13 abr. 2018.

Sem medo de errar

Com o objetivo de ganhar o contrato da Sider, você deverá apresentar um projeto ao senhor Siderley Chubacy, e nesta primeira fase, o projeto deve se concentrar nas tecnologias de controle de acesso.

Este projeto poderia ser realizado de várias maneiras, com várias proposições diferentes, sendo que se todos os requisitos de segurança são atendidos, o projeto está basicamente correto. Em sua proposição, você deve adicionar uma descrição do ambiente do cliente (no caso, a Sider), de forma a servir de justificativa para os elementos do projeto proposto. Em que pese haver várias soluções possíveis, uma maneira racional de se propor o projeto é dividi-lo em áreas de atuação, como apresentado a seguir:

- Infraestrutura
    - **Rede de comunicação** – Por mais que haja soluções de sinalização proprietárias e bastante eficientes, vamos sugerir que a infraestrutura de todas as soluções propostas seja a rede TCP/IP da Sider, de forma que os resultados de coleta de todo o parque de sensoriamento, todas as câmeras, todas as fechaduras eletrônicas, toda a segurança perimetral etc. tenham seus dados concentrados em uma única central de controle, capaz de gerenciar todo o controle de acesso.
        - Os sensores próximos e/ou com acesso ao cabeamento podem ser cabeados para facilitar e baratear o acesso à rede;
        - Os sensores distantes podem ser conectados via Wi-Fi.
    - **Servidores** – Em que pese fazerem parte da mesma infraestrutura de rede TCP/IP, sugere-se que tanto os sensores e equipamentos de controle de acesso e CVTV quanto os servidores (aplicativos, bancos de dados, central de controle) pertençam a uma rede lógica separada, de maneira a não permitir o acesso de terceiros aos dados de segurança e controle de acesso.
    - **Processo** – O pessoal de segurança que opera a

Central de Segurança da Sider, bem como o pessoal de campo, deve estar treinado para atuar diante de intercorrências que venham a surgir no ambiente. Os seguranças devem estar treinados para lidar com pessoal sem direito de acesso, tentando entrar no ambiente, pessoal sem direito de acesso identificado fora de sua área de acesso (em violação de direito de acesso), perda e/ou roubo de crachás, preservação de evidências (logs, registros e filmagens).

- Controle de Acesso
  - **Crachás Eletrônicos** – Crachás de aproximação que identificam o usuário. Esses crachás devem ser pessoais e intransferíveis com uso obrigatório todo o tempo em que o funcionário estiver no ambiente da Sider. São adequados para acesso perimetral, isto é, para locais de uso comum de funcionários da empresa, tais como as portarias de entrada da Sider, os locais de uso comum e de passagem a locais restritos.
  - **Leitores Biométricos** – Sugerir leitores baseados em digitais para acesso a locais internos sensíveis para o negócio da Sider, tais como laboratórios e salas de trabalho.
  - **Fechaduras Eletrônicas** – Para Armários, almoxarifados, salas de suprimentos e mesmo salas de reunião.
  - **Portarias Virtuais** – Em locais de acesso de pouco trânsito, sem acesso do público, portarias virtuais serão implantadas, conectadas à Central de Controle, com câmeras e leitores faciais permitindo o acesso dos indivíduos autorizados.
  - **Sensores de Movimento** – Implantados em toda a área interna e externa da Sider, ativos na área interna em locais e horários sem nenhuma circulação, e na área externa 24 h por dia. Conectados e gerando eventos diretamente na Central de Controle.
- Segurança Perimetral
  - Cerca eletrificada com sensores de movimento nos

fios externos, identificando tentativas de invasão, e câmeras acopladas a cada 20 metros, com visão de todo o perímetro.

- Circuito Fechado de TV
    - Utilizando câmeras reais em todo o perímetro e em todo o interior da Sider, conectadas à Central de Controle e emitindo suas imagens em tempo real, 2 horas horas por dia, armazenadas em banco de dados e conectadas ao sistema de reconhecimento de face da Sider.
- Central de Controle
    - Console central tipo "telão" com mapa representativo de cada aspecto do local a ser controlado, com eventos em tempo real. A central também deverá ser equipada com mesas com terminais e telefones para os operadores, cuja responsabilidade será análise em tempo real de cada parâmetro em cada ponto de controle.

Desta maneira, tem-se um projeto coerente e coeso de Controle de Acesso para a Sider.

Avançando na prática

Impedindo a coletivização da senha

Descrição da situação-problema

Marileuza Bentossi é analista de segurança no Granaki, um banco de investimentos localizado na Capital. Ela foi chamada por Marcos, o gerente de TI da empresa, que lhe apresenta uma situação inusitada. A sala-cofre onde se encontram os servidores da empresa tem amanhecido com o ar-condicionado desligado, com a temperatura interna na casa dos 31o C. Este "fenômeno" vem ocorrendo com certa frequência, e Marcos teme que isso possa danificar os servidores se o comportamento persistir. Parece ser um ato de sabotagem, e o pior é que é impossível identificar quem o está perpetrando, pois, a única pista é a senha usada na fechadura eletrônica da porta que dá acesso à sala-cofre. Infelizmente, a senha utilizada pertencia a uma

faxineira que já não trabalha na Granaki faz vários meses, e não há outra maneira de identificar o perpetrador do ato.

Como ajudar Marileuza a corrigir a situação?

Resolução da situação-problema

Sendo uma competente profissional de segurança da Granaki, Marileuza sabe que o curso de ação mais adequado passa primeiramente por identificar o que ocorre. Ela vai à Central de Controle e solicita as filmagens internas da Sala-Cofre, e em alguns minutos identifica a razão para a ocorrência. A senhora Marinelba Jofre, faxineira da empresa, é vista digitando a senha da ex-colega, entrando na sala-cofre, subindo em um armário, desconectando o ar-condicionado da tomada, e usando a tomada para conectar seu aspirador de pó industrial. Ocorre que o pluge de eletricidade do aspirador de pó não é compatível com as tomadas padrão da empresa, e apenas a tomada do ar-condicionado é compatível. Dona Marinelba usa a tomada para conectar seu aspirador, para, assim, poder aspirar a sala onde os analistas trabalham, que é anexa à sala-cofre. Ao final de seu expediente, já cansada, ela apenas puxa o fio e desconecta o aspirador, sem se dar o trabalho de conectar o ar-condicionado novamente.

Pronto, a primeira parte está resolvida: Marileuza identificou o que ocorre. Como ela vai resolver a situação?

Bem, a solução por ela proposta é dividida em três partes: em primeiro lugar, a fechadura eletrônica baseada em senha é substituída por um sistema de reconhecimento de face, uma vez que a sala-cofre é um dos locais mais sensíveis da empresa. A partir daí, não há mais possibilidade de não se saber quem está tentando entrar na sala a cada momento, uma vez que não é possível "compartilhar" rostos. Em segundo lugar, Marileuza realiza uma auditoria nas senhas em uso, em busca de senhas ativas de funcionários que não fazem mais parte da organização, revogando-as imediatamente. Por fim, Marileuza solicita a instalação de uma tomada industrial do lado de fora da sala-cofre, rente ao chão, de forma a facilitar a vida de Dona Marinelba, a faxineira.

Pronto! Problema resolvido!

Faça valer a pena

1. Da mesma maneira que a empresa planeja suas ações estratégicas e este planejamento inclui, digamos, o planejamento das ações de marketing e o planejamento de vendas, também deve haver um planejamento que se encaixe no planejamento estratégico que especifique as medidas de segurança a serem adotadas.

Acerca do texto citado, podemos concluir que:

a) A Segurança Empresarial é um conjunto de tecnologias que determinam quem deve e quem não deve ter acesso ao ambiente da empresa.
b) A Segurança Empresarial é menos importante que o planejamento de marketing ou o planejamento de vendas da corporação, e por isso deve vir depois desses.
c) A Segurança Empresarial não é importante no contexto da empresa.
d) A Segurança Empresarial deve ser implementada na empresa por meio de um planejamento, e não de ações baseadas nas tecnologias em si.
e) A Segurança empresarial não é tarefa técnica, mas sim estritamente administrativa.

2. Identificam univocamente características biológicas do postulante, comparando-as com dados coletados pelo aparelho de leitura com dados armazenados em banco de dados do sistema. São vários os tipos, sendo que os mais comuns são os leitores de digital.

O texto citado se refere a qual tipo de mecanismo de controle de acesso?

a) Mecanismo de sena e contrassenha.
b) Mecanismo e crachá eletrônico.
c) Mecanismo de leitor biométrico.
d) Mecanismo de fechadura eletrônica.
e) Mecanismo de portaria virtual.

3. Jeremias tem notado que mercadorias em sua loja de roupas femininas têm desaparecido com certa frequência. Estando apertado no tocante a recursos financeiros, o que o impede de comprar um sistema de câmeras para filmar todos os pontos da loja, ele decide investir em algumas câmeras falsas, apenas invólucros plásticos realistas, que instala em um fim de semana em vários pontos da loja. Na segunda-feira, ele informa

a todos os funcionários e fornecedores que implantou um novo sistema de segurança na loja, que grava na nuvem as filmagens do CFTV e envia alarmes para seu celular.

De acordo com o texto citado, qual o nome do efeito sobre o qual se alicerça esta solução, e qual o resultado esperado por Jeremias?

a) Efeito dissuasivo. Jeremias espera que os furtos não mais ocorram pelo medo que o ladrão teria de ser captado pelas câmeras no ato do roubo.
b) Efeito persuasivo. Jeremias espera que na possibilidade de ser descoberto por algum produtor televisivo, o ladrão seja persuadido a roubar novamente.
c) Efeito dissuasivo. Jeremias espera que as câmeras captem o ladrão no ato do roubo, e que as imagens, mostradas a ele (ou ela) o deixem com vergonha, dissuadindo-o de agir assim novamente.
d) Efeito persuasivo. Jeremias espera que as câmeras captem o ladrão no ato do roubo, e que as imagens, mostradas a ele (ou ela) vão persuadi-lo a parar com esse comportamento.
e) Efeito opressivo. Jeremias espera usar as imagens captadas pelas câmeras para processar o ladrão.

Seção 4.2

Sistemas eletrônicos avançados

Diálogo aberto

Olá!

Você já percebeu como os ambientes públicos vêm sendo municiados com elementos tecnológicos que cada vez mais visam "penetrar" nos transeuntes, avaliando com maior profundidade os riscos potenciais que possam trazer consigo? Os detectores de metais e sistemas de raios X, antes confinados aos aeroportos, cada vez mais estão presentes em nosso cotidiano, em bancos, hospitais e mesmo escolas adotando tais tecnologias como forma de manter a segurança dos presentes em seu perímetro. Pois é isso que veremos na presente seção.

Para tanto, lembremos que sua empresa foi convidada para participar do empreendimento da nova sede da Sider, sendo empresa global de tecnologia. Em seu projeto de segurança para nova sede, você deverá, nesta fase, aprofundar o projeto de controle de acesso. Nesse sentido, deverão ser incluídos sistemas de monitoramento por infravermelho por raio X, bem como a inclusão de portarias virtuais para locais de pouca circulação e circulação controlada. Há benefícios em se utilizar novas tecnologias no monitoramento? Quais?

Nessa seção veremos o sensoriamento via raios X e infravermelho. Em seguida, veremos os *drones* como elementos de sensoriamento e também como dispositivos ativos de segurança. Veremos, também, os processos envolvidos nas portarias virtuais, uma vez que já vimos as tecnologias em sessões anteriores. Por fim, veremos os sistemas inteligentes de segurança.

E aí, todo mundo pronto?

Então vamos lá!

Não pode faltar

A partir de agora, você vai conhecer alguns elementos mais especializados da tecnologia aplicada à segurança. Estes elementos se integram às soluções vistas até aqui, claro, e já são usados em inúmeros locais públicos e privados.

Emissão de Raio X / Infravermelho

Brasiliano e Blanco (2003, p. 69), afirmam que estes equipamentos buscam identificar "imagens interiores de corpos opacos mediante emissão de raios X. Geralmente são empregados para a identificação de contrabando, isto é, da tentativa de transporte de material considerado ilícito pela lei. Em muitos casos este contrabando se refere a armas e drogas, mas de fato pode englobar qualquer tipo de substância ou objeto regulados pela legislação do país em que busca entrada por meios ilícitos. Vinholes (2015) aponta principalmente os objetos pontiagudos e artigos inflamáveis, mas a lista é bem mais longa:

- Tecnologias controladas (eletrônicos, criptografia, frutos de pesquisas consideradas estratégicas para a nação, etc.);
- Fauna/Flora controlados;
- Medicamentos e/ou compostos químicos controlados;
- Elementos que geram risco potencial ao voo e aos passageiros.

Os dispositivos em uso para sensoriamento de raios X, nos dias de hoje se baseiam na tecnologia *Backscatter*, e divergem dos aparelhos de raios X utilizados para fins médicos. Enquanto os aparelhos de raios X para fins médicos emitem partículas que atravessam os corpos e sensibilizam por contraste uma placa de filme, que deve ser revelado a posteriori.

Já os raios X baseados em tecnologia *Backscatter*, emitem feixes menos intensos de raios X (e, portanto, menos potencialmente perigosos), e mensuram seu reflexo quando incidem em corpos e objetos. Os feixes de raios X refletidos são coletados por sensores reutilizáveis, e formam a imagem em tempo real, como pode ser visto na Figura 4.3, a seguir:

Figura 4.3 | Imagem gerada por um aparelho de raios X do tipo Backscatter

Fonte: iStock.

Pela baixa intensidade dos raios X, os aparelhos baseados em tecnologia *Backscatter* também trazem a vantagem de que as emissões podem ser contidas, sem riscos de vazamento, e consequentemente sem risco para os operadores ou para os passageiros (TSA, s.d.).

Também é importante observar que as informações coletadas pelos aparelhos de raios X baseados em tecnologia *Backscatter* são complementadas por outros sensores presentes no aparelho. Estes sensores podem ser dos tipos:

- **Químico** – coletam traços de componentes químicos presentes na mala, ainda que apenas traços sejam perceptíveis;
- **Eletromagnéticos** – emitem ondas eletromagnéticas e coletam seu reflexo, conseguindo identificar, por meio das frequências de refração e reflexão as ligas metálicas, plásticas e orgânicas (madeira, fibras) presentes nos objetos dentro da mala;
- **Ultrassom** – Como no caso dos aparelhos médicos de ultrassom, esses sensores emitem frequências não sensíveis ao

aparelho auditivo humano, que penetram superfícies e refletem em seu interior. A captação desses reflexos gera as imagens.

Todos esses sensores complementam os dispositivos de raios X, adicionando camadas extras de segurança.

É importante notar que a tecnologia, apenas, não garante a eficiência do sistema. Dois outros elementos devem ser levados em consideração e cuidados constantemente para que os raios X possam oferecer o máximo de segurança possível:

- **Processo** – Cada passo do processo de escrutinização (vistoria) de bagagens, pessoas e objetos deve ser formalizado. A ordem de leitura e análise deve ser estritamente seguida, e nenhum passo deve ser suprimido ou resumido pelos operadores. E mais: as ações e procedimentos quando há alguma ocorrência deve ser sempre seguida à risca: a comunicação do fato, a descrição detalhada da ocorrência, as ações imediatas e posteriores. Tudo deve ser formalizado e registrado, sem que faltem evidências fotográficas da ocorrência para análise posterior e consequente feedback (realimentação e aprendizado) do sistema;
- **Treinamento** – Tanto para a operação dos aparelhos quanto para a realização dos processos de segurança, o pessoal responsável deve ser devidamente treinado e passar por reciclagem periódica do conhecimento. Vinholes (2015) nos mostra que os operadores devem ser treinados a sempre fazerem três perguntas para todos os objetos que avaliam: O que está sendo procurado? Como o objeto procurado se parece? Como o objeto procurado se apresenta dentro de uma mala, isto é, qual seu aspecto quando empacotado?

Assimile

A tecnologia *Backscatter* permite o uso seguro de aparelhos de raios X, uma vez que os feixes são de menor intensidade e permitem o encapsulamento que evita o vazamento, não sendo nocivos ao público nem aos operadores.

Drones

Rogers e Hill (2014) apontam para o fato de que a elevação e amplidão permitem ao aeronauta uma perspectiva do teatro de ações (no sentido militar desta expressão) que não está disponível ao soldado ou ao marujo. De fato, o soerguimento, seja de equipamentos de sensoriamento ou de pessoas, permite uma visão mais completa do terreno. Esta visão mais completa permite tanto decisões quanto ações mais precisas. Não é à toa, continuam os autores, que esforços vêm sendo desenvolvidos no sentido de se aproveitar melhor o voo e os céus em operações de defesa e em exercícios de guerra.

Nesse sentido, continuam Rogers e Hill (2014), a partir de 2001 os UAVs (*Unmanned Aerial Vehicles* – Veículos Aéreos Não Tripulados) e UCAVs (*Unmanned CombatAerial Vehicles* – Veículos Aéreos de Combate Não Tripulados) vem sendo desenvolvidos e utilizados em dois processos fundamentais à segurança e à defesa:

- **Coleta de informações** – por meio de sensores e câmeras;
- **Ações militares** – por meio de armamento (mísseis explosivos ar-terra).

Os *drones* são veículos voadores, mas diferentemente dos aviões e helicópteros, não são tripulados. Nesse sentido, assemelham-se a aeromodelos, uma vez que devem ser operados (pilotados) por pessoal capacitado de posse de controles remotos que se comunicam com os veículos por meio de ondas eletromagnéticas. Diferentemente dos aeromodelos, distância de comunicação entre a base e o veículo pode ser de várias centenas de quilômetros, o que lhes permite incursões profundas em territórios onde a presença de artilharia colocaria os soldados e/ou aviadores em perigo. No caso dos aeromodelos, o sinal de controle não ultrapassa 10 km, e ainda assim, em condições ótimas de operação (sem tempestades ou outros emissores de ondas de rádio próximos).

A Figura 4.4, a seguir, mostra um drone modelo MQ-9 Reaper, da empresa General Atomics, armado com um único míssil ar-terra:

Figura 4.4 | Drone modelo MQ-9 Reaper

Fonte: iStock.

Marin e Krajcikova (2016) apontam para o uso de drones no patrulhamento de fronteiras, o que demanda outro tipo de equipamento. Enquanto os drones de defesa devem primar pela autonomia (longas distâncias de alcance) e velocidade, os drones de patrulhamento devem ser capacitados a coletar informações precisas e detalhadas sobre o ambiente. O tipo mais indicado para a tarefa de policiamento é, portanto, o chamado quadicóptero, que permite movimentações precisas, operação em posicionamento estático (podem ficar parados no ar como qualquer helicóptero).

Coletas de dados visuais (filmes e fotografias), portanto, podem ser obtidas com maior qualidade a partir deste tipo de dispositivos, o que os torna bastante adequados para vigilância.

Não é por outo motivo que Marin e Krajcikova (2016) afirmam que a vigilância de fronteiras em países europeus, com *drones* sendo operados por mistos de inteligência artificial e operação manual. No caso, temos a seguinte divisão de funções:

- **Inteligência artificial** – controle de caminho a ser seguido,

controle de estabilidade do dispositivo, evasão em caso de situação anormal;

- **Operação manual** – controle fino do dispositivo quando da ocorrência de alguma situação de interesse que mereça ser registrada por filme e/ou foto. Controle fino em caso de necessidade de manobra.

Pesquise mais

A cidade de São Paulo se prepara para receber centenas de drones para vigilância urbana. Armados de câmeras e controlados à distância, estes devem ser ferramentas valiosas nas mãos do poder público e a serviço da população. Veja nesse vídeo do Olhar Digital, de 0:07:03-00:08:30. (1 minuto e 27 segundos de reportagem). Disponível em: <https://youtu.be/moIL7E6R9Ik?t=7m3s>. Acesso em: 13 abr. 2018.

Estes *drones* podem ainda operar em modo de *swarm* (enxame) em caso de necessidade de vigilância de muitos pontos de interesse ao mesmo tempo.

A Figura 4.5, a seguir, mostra uma formação de enxame, controlada por inteligência artificial, que coordena os voos individuais de maneira que possam voar em formação sem risco de colisão:

Figura 4.5 | Drones tipo quadicóptero voando em formação de *swarm*

Fonte: iStock.

É importante observar, ainda, que estes sistemas de vigilância por meio de drones pode e deve ser integrado à central de segurança da organização, com imagens e dados coletados sendo alimentados diretamente no sistema central, com acesso via console central de operação. Alarmes e relatórios, por exemplo, podem ser gerados a partir de suas informações, filmes e fotografias, e ações podem ser disparadas a partir de suas coletas de dados.

Reflita

Uma vez que os drones podem comportar armas (explosivos, por exemplo) e podem ser comandados por inteligência artificial, quais as implicações éticas de unirmos as duas possibilidades? Seria adequado termos drones armados controlados por inteligências artificiais? Quais consequências poderiam surgir se assim fosse feito?

Portaria Virtual

Na seção 4.1, já vimos as tecnologias que alicerçam e possibilitam as portarias virtuais. Retomando, são basicamente quatro tipos de tecnologias por trás das mesmas:

- **Câmeras** – Fixas nos arredores e também em local capaz de identificar as feições do postulante com precisão;
- **Sistema de Comunicação bidirecional** – Permite o pedido e recebimento de informações verbais do postulante;
- **Sistema de Identificação** – pode ser por meio de crachá eletrônico, teclado para inserção de senha, ou leitor biométrico. O importante é que o postulante seja identificado com precisão;
- **Fechadura Eletrônica** – Acionada pela portaria, após o fornecimento de credencial adequada por parte do postulante;
- **Central de Atendimento** – Todos os mecanismos e sistemas devem alimentar uma central de atendimento, com console de operação que exiba as ocorrências e imagens do sistema de câmeras, e que permita o registro de todas as ações.

Em que pese todos esses dispositivos e sistemas serem

imprescindíveis, eles não devem ser considerados suficientes para que a portaria eletrônica seja eficiente nos serviços de identificação e controle de acesso que provê.

O que falta? Bem, Brasiliano e Blanco (2003) dividem qualquer projeto de segurança em três áreas fundamentais (p. 36):

- **Meios Tecnológicos** – Já vistos: são os equipamentos e sistemas compostos de mecanismos, hardware, software e redes utilizados para compor a solução;
- **Meios Humanos** – Pessoal treinado, capacitado a agir em todas as situações que a portaria pode encontrar em seu período de funcionamento;
- **Meios Organizacionais** – Aqui os autores listam os aspectos documentais do projeto (como no caso da política de segurança, que deve reger quaisquer ações e procedimentos de segurança dentro da organização). É nessa categoria, também, que se encontram os processos, que são fundamentais para que as pessoas envolvidas (profissionais de operação da portaria eletrônica) possam utilizar adequadamente a tecnologia em seu favor, tornando assim a portaria no mecanismo eficiente que deve ser.

Os processos são, segundo Kirchmer (2017) conjuntos contínuos de ações realizadas em uma ordem específica e seguindo regras formalmente definidas, cujo resultado é a geração de valor para um cliente interno ou externo. Analisando esta definição, temos alguns pontos fundamentais a serem considerados nos processos:

- **São compostos por ações formais** – processos são tarefas realizadas, e estas tarefas devem ter sido formalmente definidas. Isso exclui dos processos o improviso, o que é fundamental para a padronização e para a obtenção de eficiência na execução das tarefas;
- **São contínuos** – uma vez iniciado, um processo ocorre de maneira contínua, enquanto as operações da organização dele depender de alguma forma. Terminada uma execução, outra se inicia automaticamente. Uma vez atendida uma pessoa em uma portaria eletrônica, por exemplo, os

operadores se preparam para a próxima que em algum momento virá;

- **Geram valor** – o objetivo de um processo é gerar algum tipo de valor por meio do desempenho de suas ações. Alguém ou algum departamento deve sempre se beneficiar da realização de um processo (caso contrário, o processo não teria razão para existir e ser executado);
- **São voltados para clientes internos ou externos** – Um processo de venda, por exemplo, atende um cliente externo (o cliente que compra o produto ou serviço), enquanto um processo de contabilização de impostos atende ao setor financeiro, que é um cliente interno. Os processos de portaria eletrônica servem a clientes externos e internos: de um lado, os postulantes tentando entrar na empresa são clientes externos e a garantia de sua correta identificação e subsequente autorização de entrada são os valores que derivam deste processo. Por outro lado, todos os departamentos da empresa são clientes internos, seja porque é para algum deles que o postulante se dirige, seja pela segurança oferecida a todos pelo processo de identificação e autorização (ou negação) de entrada.

Outro benefício das portarias virtuais é a redução de custos, uma vez que o mesmo serviço de portaria, utilizando os mesmos profissionais e o mesmo equipamento em uma central de operações pode servir a várias portarias em locais diferentes, permitindo a divisão dos custos.

Exemplificando

Um exemplo de redução de custos por meio das portarias virtuais pode ser visto no vídeo da Reportagem sobre Portaria Virtual no Jornal Nacional: Disponível em: <https://www.youtube.com/watch?v=NTMYGudFrm4>. Acesso em: 13 abr. 2018.

Sistemas de Segurança Inteligentes

Os sistemas inteligentes de segurança são, como nos mostram Solanas e Ballesté (2010) a junção das Tecnologias de Informação e Comunicação com os processos de segurança e operados pelo pessoal devidamente treinado, mas com uma adição importante: os sistemas de inteligência artificial.

A inteligência artificial, como afirmam os autores, pode ter um papel importante nas soluções de segurança, uma vez que trazem várias vantagens potenciais aos sistemas em que é implantada:

- **Automatização de ações** – A inteligência Artificial pode ser usada para tomar decisões consistentes e corretas com base em situações que a ela se apresente, evitando que o erro humano possa ocorrer por acidente ou negligência;
- **Agilidade e Dependabilidade** – a Inteligência Artificial está sempre pronta a realizar as tarefas a seu cargo, desempenhando essas funções m tempo hábil, sem faltas ou atrasos;
- **Isenção e Consistência** – A inteligência artificial não tem predileções e sempre realizará as tarefas de maneira isenta, apresentando resultados consistentes em 100% das situações que enfrentar.

Uma vez que seja adequadamente treinada, uma solução de inteligência artificial é uma ferramenta das mais precisas e valiosas a serviço da segurança.

Sem medo de errar

Lembrando que sua empresa foi convidada para apresentar um projeto de segurança para a Sider, a pedido do dono da empresa, o senhor Siderley Chubacy. Agora é o momento de inserir os elementos de monitoramento por raio X e a portaria virtual.

Para tanto, você pode usar das seguintes ações:

- Sistema de monitoramento por raio x
    - Adoção da tecnologia *Backscattering* (mais seguro e bastante eficiente na averiguação de objetos).
    - Implantação bidirecional.
        - Verifica objetos e invólucros na entrada e na saída.
    - Implantação em área de carga e descarga, entrega de pacotes.
        - Previne o aporte de substâncias nocivas e objetos que podem pôr em risco a vida dos presentes na Sider.
        - Previne o roubo de tecnologias sendo desenvolvidas na Sider.
    - Implantação na Portaria Central.
        - Aferição de maletas e mochilas em poder dos transeuntes.
            - Evitar o transporte de dispositivos nocivos.
            - Evitar roubo de tecnologias sendo desenvolvidas.
    - Interligar com detectores de metal nas portas de entrada das portarias.
- Portarias Virtuais
    - Implantadas no perímetro, em locais de baixa circulação e/ou apenas para entregas de pequenos volumes.
    - Integradas à Portaria Central, que controla o registro e a entrada e saída dos transeuntes daqueles locais.

Dessa maneira, o projeto continua integrado, fornece benefícios e informações valiosas para a segurança, garante controle de acesso e, adiciona dois elementos fundamentais à segurança:

- Exame minucioso de objetos para garantir que são seguros e que não configuram contrabando/roubo;
- Redução de custos por meio do aproveitamento da portaria central para atendimento em locais do perímetro que precisem de controle de aceso, mas sem aumento de pessoal.

Agora seu projeto já está mais robusto, e você tem mais chances de ganhar este certame, o que será excelente para sua empresa de segurança.

Avançando na prática

Uma solução mais sensata

Descrição da situação-problema

O senhor Eleutério Ganza é Presidente de um novo *shopping center*, recém-inaugurado na capital. Preocupado com a segurança dos frequentadores, ele cogita a implantação de um raio X do tipo *Backscatter*, como representado pela Figura 4.6, a seguir:

Figura 4.6 | Exemplo de Raio X para pessoas

Fonte: iStock.

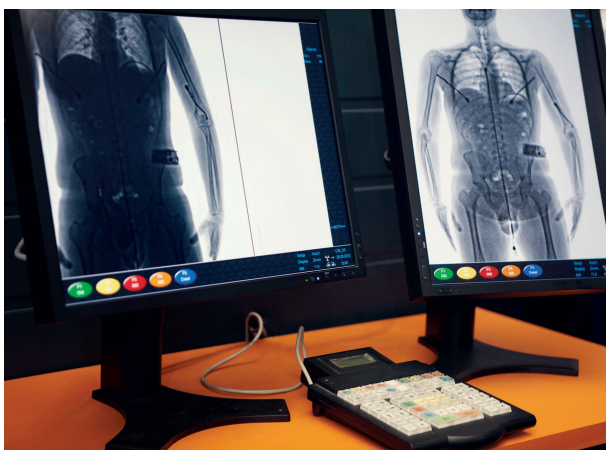
Você, consultor renomado de segurança, foi contratado para emitir seu parecer sobre este projeto. É adequada a adoção deste tipo de tecnologia para um shopping center? Por quê? Há alternativas? Quais?

Resolução da situação-problema

Em que pese ser interessante a preocupação de Eleutério, a solução apresentada é descabida, e por várias razões:

- **Desproporcionalidade** – Em um país como o Brasil, a violência em shopping centers não é um caso que mereça uma solução tão radical quanto a implantação de raios X;
- **Imagem** – Uma solução desse tipo tende a ferir a imagem do shopping center, espantando os consumidores, ao invés de convidá-los a frequentar o local;
- **Custo** – Uma solução desse tipo custa caro, tanto na implantação, quanto na manutenção, quanto na operação (pois demanda pessoal de operação durante todo o tempo em que há entrada de gente no shopping);
- **Privacidade.** A Figura 4.7, a seguir mostra a imagem de uma pessoa por meio do dispositivo. Um órgão governamental como a Infraero tem responsabilidade civil sobre as imagens, mas a mesma responsabilidade pode não existir nos operadores do dispositivo no shopping center. A divulgação desse tipo de imagem é altamente nociva para o público e para a imagem do shopping, e o mesmo não deve correr este risco.

Figura 4.7 | Imagem coletada pelo raio X de Backscatter



Fonte: iStock.

Como endereçar, então, a preocupação do Presidente do *Shopping*?

Considerando que se trata de um local de diversão e compras, o foco da segurança deve ser a discrição e a não-intrusão. Desta maneira, uma solução tradicional com vigilância do perímetro e do interior pode ser realizada da seguinte maneira:

- Câmeras de vigilância em todo o perímetro e em todas as áreas comuns do interior do shopping (corredores, pátios, praças de alimentação etc.);
- Vigias patrulhando o interior do *shopping*;
- Central de comando na área administrativa (longe dos olhos dos transeuntes, reunindo as imagens e filmagens, e com comunicação direta com os vigias.

Pronto, com isso o sr. Eleutério tem uma solução adequada para a segurança dos frequentadores.

Faça valer a pena

1. Os autores Brasiliano e Blanco (2003, p. 69) afirmam que os equipamentos de raios X buscam identificar "imagens interiores de corpos opacos mediante emissão de raios X. Geralmente são empregados para a identificação de contrabando".

Quando utilizados em aeroportos, os equipamentos de raios X têm a função de identificar "contrabando" com que objetivo principal?

a) Evitar evasão de divisas do país.
b) Evitar fuga de tecnologias desenvolvidas no país.
c) Garantir a segurança dos voos.
d) Evitar desequilíbrio nas contas públicas.
e) Controlar estatisticamente tudo o que entra e sai do país.

2. A partir de 2001 os UAVs (*Unmanned Aerial Vehicles* – Veículos Aéreos Não Tripulados) e UCAVs (*Unmanned CombatAerial Vehicles* – Veículos Aéreos de Combate Não Tripulados) vem sendo desenvolvidos e utilizados em dois processos fundamentais à segurança e à defesa.

Os dois processos a que o texto base se refere são:

a) Sobrevoo de Regiões em Conflito e Ações Militares.
b) Exercícios Militares e Sobrevoo de Regiões em Conflito.
c) Pressão Psicológica e Guerra Bacteriológica.
d) Coleta de Informações e Ações Militares.
e) Recreação e Ações de Marketing Militar.

3. Observe na coluna da esquerda os meios fundamentais por meio dos quais se implementam os projetos de segurança, e na coluna da direita exemplos desses meios:

I.	Meios Tecnológicos	A.	Operadores
II.	Meios Humanos	B.	Processos
III.	Meios Organizacionais	C.	Câmeras
		D.	Administradores
		E.	Política de Segurança
		F.	Leitores Biométricos

Assinale a alternativa que faz a correta correspondência das colunas:

a) I-AB, II-CD, III-EF
b) I-AC, II-DF, III-BE
c) I-DF, II-AE, III-BC
d) I-AE, II-CF, III-BD
e) I-CF, II-AD, III-BE

Seção 4.3

Aplicações da TIC na segurança privada

Diálogo aberto

Já ouvimos notícias de como as autoridades têm soluções de reconhecimento de face instaladas em vários aeroportos no mundo todo, 24 horas por dia buscando identificar terroristas e outros procurados internacionais. Porém, não é apenas o poder público ou as agências internacionais que têm acesso a estas tecnologias: a iniciativa privada já tem acesso aos mesmos dispositivos, podendo utilizá-los em seus projetos de segurança, e deles se beneficiando sobremaneira.

Nessa presente seção vamos entender como funcionam os localizadores de veículos, o monitoramento inteligente por meio de câmeras e radares, o controle de acesso a eventos e o reconhecimento facial na segurança privada.

Desta forma, propomos a seguinte atividade. Sua empresa foi convidada para participar do empreendimento da nova sede da Sider, sendo empresa global de tecnologia. Em seu projeto de segurança para nova sede, você deverá, nesta fase, atender a uma demanda da Sider quanto à realização de eventos. Na propriedade está sendo construído um anfiteatro com capacidade para 3.000 pessoas, onde a empresa pretende realizar os lançamentos anuais de seus produtos (computadores, tablets, smartphones e outros dispositivos de processamento e comunicação pessoal e empresarial). O projeto deve contemplar que tecnologias devem ser implantadas para garantir a segurança do local durante os eventos. Como garantir a segurança dos presentes sem causar inconvenientes? Como manter a eficiência do sistema de identificação em meio a tanta gente presente ao mesmo tempo?

Pronto para finalizar essa disciplina?

Então vamos lá!

Não pode faltar

Para esta última seção da disciplina de Tecnologias Aplicadas aos Sistemas de Segurança, vamos observar mais detalhadamente algumas tecnologias bastante aplicadas à segurança privada.

Localizador de Veículos

Brasiliano e Blanco (2003) nos mostram que as soluções que compõem um projeto de segurança devem realizar uma ou mais das seguintes funções, dentro de suas atribuições de segurança:

- **Detectar** – identificar o risco antes que ele provoque impactos negativos no ambiente. Exemplo: antivírus (nível lógico), sensores de movimento (nível físico);
- **Inibir/Dissuadir** – provocar o agressor no nível psicológico de maneira que este desista de interagir de maneira não-autorizada com o sistema. Exemplo: registros de ação e janelas de aviso (nível lógico), câmeras e placas de aviso do tipo "sorria, você está sendo filmado" (nível físico);
- **Impedir** – criar barreiras físicas e/ou lógicas que impeçam a presença do agressor de maneira não-autorizada no sistema. Exemplo: Firewall (nível lógico), fechaduras eletrônicas com teclado para inserção de senha ou sensor de crachá eletrônico (nível físico);
- **Retardar** – criar mecanismos que atraiam a atenção do agressor, de maneira que sua presença não-autorizada no sistema seja identificada, mas que o atrasem em seu intento de provocar dano, dando assim a oportunidade de os administradores reagirem e evitarem esta ação danosa. Exemplo: *honeypot*, isto é, uma área "convidativa" no servidor, mas com acesso controlado e dados falsos para atrair o agressor, assim como um pote de mel (tradução do termo) atrai moscas (nível lógico). Portas corta-fogo e materiais não inflamáveis usados na construção (nível físico);
- **Responder** – permitir que, diante de uma agressão qualquer, os responsáveis pela segurança respondam ao incidente de maneira eficiente. Exemplo: Registros e logs de acesso, mais sistema de acesso remoto (nível lógico), extintores de incêndio (nível físico).

Quando analisamos os localizadores de veículos sob esta óptica, é fácil perceber que são classificados na segunda, na terceira e na quinta categorias, isto é, agem como inibidores, servem para impedir a ação dos agressores, e permitem a resposta à agressão.

Assimile

Uma solução de dissuasão visa provocar um estado psicológico de desestímulo no potencial agressor.

No primeiro nível, veículos com este tipo de tecnologia instalada sempre adotam algum tipo de placa ou adesivo informando de sua presença. A Figura 4.8, a seguir, mostra um adesivo comumente afixado em local de fácil visibilidade no veículo que utiliza rastreadores/localizadores:

Figura 4.8 | Adesivo avisando da presença de um localizador no veículo

Fonte:<http://www.rumosgeograficos.com/2017/06/sistema-global-de-posicionamento.html>. Acesso em: 10 jan. 2018.

O localizador atua, assim, como inibidor, uma vez que o agressor, diante deste adesivo, no mais das vezes vai contemplar a possibilidade de agir sobre outro veículo, que não utilize esta tecnologia. Claro que tal medida não é sempre 100% efetiva, uma vez que o agressor pode estar preparado para atacar um veículo mesmo quando este esteja equipado com um rastreador, mas ainda assim, vários agressores em potencial podem se ver desestimulados quando veem esta placa.

O rastreador funciona no segundo nível como empecilho, isto é, atua no sentido de impedir a ação do agressor. Isto porque uma vez que o rastreador identifica, digamos, uma parada não pré-programada, ou um desvio de rota, pode automaticamente acionar elementos secundários de proteção, tais como cortes no fornecimento de energia elétrica para o veículo, acionamento de cadeados e travas eletrônicas em compartimentos de cargas e medidas similares. Desta maneira, o veículo abordado tem proteção contra a ação dos agressores.

O rastreador funciona, ainda, em um terceiro nível, permitindo a resposta ao incidente. Em contato 24 x 7 (24 horas por dia, 7 dias por semana) com uma central de monitoramento, o rastreador avisa da ocorrência da agressão, e a central de monitoramento pode, rapidamente, acionar a força policial ou mesmo filiais de segurança privada localizadas próximas ao local onde ocorreu a agressão. Dessa maneira, agindo com rapidez e com informações acerca da localização geográfica do veículo no momento da agressão, aumentam as chances de evitar que os agressores venham a realizar seus intentos (no mais das vezes, roubo da carga e/ou do veículo).

Monitoramento Inteligente (Câmeras e Radares)

Quando pensamos em monitoramento inteligente por câmeras e radares nos remetemos inicialmente ao monitoramento rodoviário. Contudo, como nos mostra Pereiro (2017), este tipo de tecnologia – acoplando dispositivos de monitoramento tais como câmeras e sensores, a dispositivos de processamento e inteligência artificial – pode ser utilizado com muitas vantagens pela iniciativa privada no monitoramento tanto de processos industriais quanto de pessoas no perímetro da empresa.

Pereiro (2017) alerta para a redução de custos desse tipo de solução, o que permite que a indústria encontre cada vez mais usos para a mesma. Exemplo disso, como cita o autor, é a monitoração inteligente de concessionárias de energia, empresas de energia renovável ou óleo/gás, além de uma gama enorme de indústrias químicas e de transformação.

O sistema computacional a que as câmeras e sensores são acoplados é muito mais do que um sistema de registro de imagens e eventos: é uma inteligência artificial capaz de reagir às informações

das câmeras e dos sensores, atuando como um vigilante com 100% de atenção e 100% de eficiência a qualquer hora do dia ou da noite.

Os sistemas de monitoramento inteligente podem:

- **Registrar imagens** – as câmeras capturam o que ocorre em seu campo de visão e as imagens/cenas são armazenadas em disco para uso posterior, quando necessário;
- **Registrar eventos por meio de sensores** – sensores físicos (temperatura, pressão, vazão, massa, velocidade, entre vários outros) captam eventos ocorrendo no sistema. Quando os eventos em ocorrência estão dentro do padrão previsto e pré-acordado, o sistema apenas registra que tudo ocorre dentro da normalidade;
- **Reagir a eventos** – Contudo, quando da ocorrência de algum evento (ou seja, caso a ocorrência tire o sistema de sua normalidade), o sistema de monitoração inteligente pode tomar uma de várias ações, como por exemplo:
    - Registrar tipo, data e hora da ocorrência;
    - Enviar alerta para outro sistema ou para algum operador do sistema que deva ser avisado da ocorrência;
    - Iniciar protocolo de resposta, com acionamentos automáticos do próprio sistema ou de outros sistemas de segurança;
    - Acionar, por meio de mensagem eletrônica escrita ou falada, as autoridades acerca da ocorrência;
    - Iniciar processos de desligamento;
    - Iniciar medidas contra incêndios.

Reflita

Caso uma câmera de monitoração de um processo industrial qualquer capte imagens de um crime qualquer, estas imagens podem ser usadas em um julgamento como evidência do crime, mesmo não tendo sido captadas para este propósito?

Estas soluções de monitoramento inteligente podem, inclusive, se acoplar aos sistemas de automação industrial, os sistemas SCADA (Supervisor *Control and Data Acquisition*, ou, em português, controle de supervisão e aquisição de dados), contribuindo com

dados e informações para o melhor gerenciamento do sistema como um todo.

No campo do gerenciamento da segurança de pessoas, os sistemas de monitoramento inteligente podem, ainda, fornecer informações para fins de seguro e de acionamento legal em caso de sinistros no perímetro da empresa. Estas informações, desde que adequadamente fornecidas e armazenadas, podem ter validade legal.

Exemplificando

Algumas indústrias químicas adotam soluções de segurança para caldeiras que monitoram 24 x 7 os seguintes elementos:

- Temperatura
- Pressão
- Vazão
- Quantidade e pressão do combustível (se a óleo)
- Taxa de consumo de energia (se elétrica)

Controle de Acesso a Eventos

Uma das principais preocupações do poder público, segundo Ensslin (2012) é a segurança dos presentes em eventos, isto é, em situações em que há aglomeração de pessoas em locais fechados ou abertos. O aumento da densidade (pessoas por m2) durante os eventos gera preocupação quanto à segurança dos presentes. Em que pese o autor focar seus estudos em eventos esportivos, especificamente em jogos de futebol em estádios brasileiros, é visível que as preocupações se estendem a todos os tipos de eventos onde ocorre a aglomeração temporária de pessoas, como por exemplo:

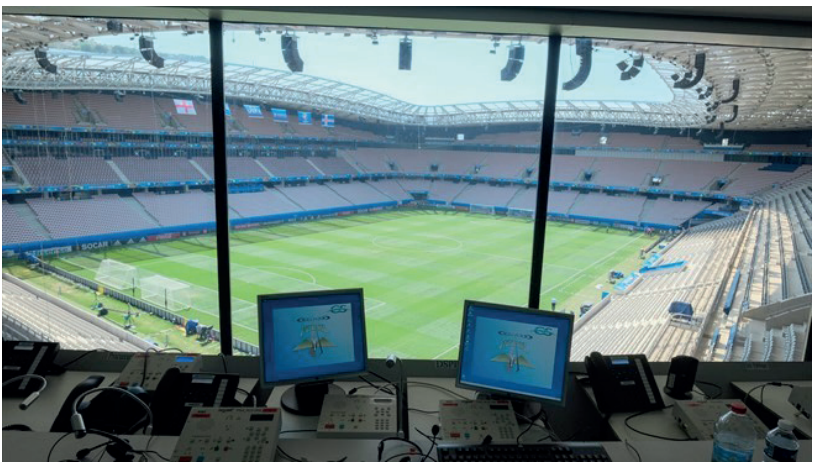
- Shows e apresentações musicais e/ou teatrais;
- Comícios;
- Festas particulares em salões preparados para tanto.

Nos estádios de futebol – que representam grande parte dos eventos e apresentam todas as dificuldades possíveis: presentes

apaixonados, local confinado, grande volume de pessoas – as medidas de segurança e controle de acesso devem ser meticulosamente planejadas e executadas (Uefa, 2017). Os elementos de segurança e controle de acesso devem estar disponíveis em todos os eventos e compõem uma solução completa de controle de acesso.

A Figura 4.9, a seguir, mostra o primeiro e principal elemento de uma solução de segurança e controle de acesso: a central de controle. No caso de um estádio de futebol — seja durante partidas ou durante shows e eventos agendados — esta central de controle deve ter visibilidade de todo o estádio, seja visibilidade direta, ou por meio de câmeras, centralizadas em um ou mais de seus monitores.

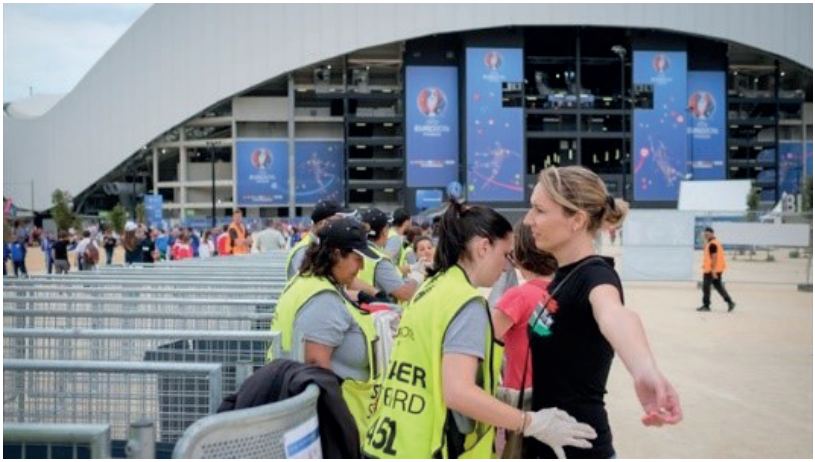
Figura 4.9 | Central de Controle em um Estádio



Fonte: <http://pt.uefa.com/insideuefa/protecting-the-game/security/index.html>. Acesso em: 3 jan. 2018.

Outro elemento fundamental é o elemento humano. Por mais que a tecnologia tenha papel preponderante nos projetos de segurança e controle de acesso a eventos, nenhum projeto é efetivo sem a participação de pessoal treinado e capacitado para lidar tanto com o público e situações de normalidade, quanto com ocorrências de várias naturezas. A Figura 4.10, a seguir, mostra pessoal capacitado em ação na entrada de um estádio, fazenda a vistoria dos postulantes à entrada:

Figura 4.10 | Pessoal capacitado fazendo vistoria na entrada do evento



Fonte: <http://pt.uefa.com/insideuefa/protecting-the-game/security/index.html>.
Acesso em: 3 jan. 2018

As câmeras de segurança — todas conectadas à central de monitoramento, também são fundamentais em uma solução de segurança e controle de acesso a eventos. As imagens podem e devem ser alimentadas em sistemas complementares de reconhecimento de face e eventos, alertando automaticamente os operadores de eventos e/ou pessoas de interesse (potenciais iniciadores de comportamentos indesejáveis) e incitadores de violência. A Figura 4.11, a seguir, mostra uma dessas câmeras em operação:

Figura 4.11 | Pessoal capacitado fazendo vistoria na entrada do evento

Fonte: <http://pt.uefa.com/insideuefa/protecting-the-game/security/index.html>.
Acesso em: 3 jan. 2018

Outro elemento importante na solução é a catraca biométrica, que garante a identidade dos presentes no evento. O cadastro é rápido, simples, e pode ser centralizado, o que significa que o espectador pode usufruir de um cadastro único em todos os eventos realizados naquele local, ou mesmo em outros locais, desde que organizados por empresa com acesso à central de cadastros biométricos utilizada. A Figura 4.12, a seguir, mostra uma catraca biométrica para locais de grande circulação. A catraca em questão funciona pela leitura da digital do usuário, garantindo o acesso dos usuários cadastrados.

Figura 4.12 | Catraca Biométrica

Fonte: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1250/1/CT_ENGELN_2012_2_01.pdf>. Acesso em: 3 jan. 2018.

Reconhecimento Facial na Segurança Privada

No que concerne a segurança privada, o reconhecimento facial já tem bastante aceitação, especialmente no controle de acesso a eventos, como visto acima. De fato, o reconhecimento facial é ferramenta bastante útil na prevenção de incidentes:

- Identificação de torcedores e/ou espectadores com ações violentas ou de incitação à violência no passado;

- Identificação de perpetradores de furtos em supermercados, lojas de departamentos e shoppings;
- Identificação de incitadores em comícios.

Os exemplos acima não são, obviamente exaustivos, e há várias outras situações em que a identificação de um indivíduo em meio a um grupo é útil na manutenção da segurança coletiva. Em especial, o poder público em conjunto com a iniciativa privada podem, por exemplo, usar os sistemas de reconhecimento de face em conjunto com bancos de dados de elementos procurados para averiguar sua frequência em locais públicos, como no caso de shopping centers. Ações policiais podem ser realizadas nas imediações do local (e nunca no local, por razões óbvias), apreendendo-se o suspeito em batidas policiais em algum dos caminhos que deixam o local.

A identificação facial requer que uma imagem da face do indivíduo seja coletada. De posse dessa imagem, o sistema extrai informações de mensuração de distâncias dos elementos da face. Estas informações geram um arquivo único de identificação, que pode ser recuperado por meio de outras imagens da mesma face, mesmo que o indivíduo esteja de perfil, utilize óculos (mesmo escuros), esteja de barba ou bigode.

A Figura 4.13, a seguir, ilustra o processo de mensuração da faca para extração das distâncias usadas para composição do arquivo de identificação:

Figura 4.13 | Extração de informações da face

Fonte: <https://goo.gl/Hnzkp4>. Acesso em: 3 jan. 2018.

Pesquise mais

Feitosa (2016) descreve com bastante didática o processo de reconhecimento de face por meio de múltiplas imagens coletadas. Veja com mais detalhes nas páginas 38 a 41 de sua tese de dissertação "Reconhecimento Facial em Vídeo com uma amostra por pessoa utilizando Stacey Supervised Auto-encoder." Disponível em: <http://www2.dbd.puc-rio.br/pergamum/tesesabertas/1422395_2016_completo.pdf>. Acesso em: 13 abr. 2018.

Sem medo de errar

Para atender à demanda da Sider quanto à realização de eventos, você e sua empresa devem considerar que um anfiteatro com capacidade para 3000 pessoas deve ser monitorado, desde a postulação de entrada e durante todo o evento.

Uma maneira de arquitetar esta fase do projeto de segurança da Sider é o seguinte:

- **Segurança Perimetral** – Câmeras e sensores de movimento para o perímetro do anfiteatro, conectados à central de controle;
- **Acesso principal** – Catracas Biométricas, com cadastro prévio dos convidados e autorização específica para cada evento;
- **Acesso de funcionários** – Os funcionários deverão ter um acesso próprio, separado, monitorado por câmeras e catracas biométricas com base de dados separada, de pessoas cadastradas compostas exclusivamente de funcionários autorizados;
- **Segurança Interna** – Câmeras nas dependências internas com reconhecimento de face, mesmo que não seja esperado nenhum tipo de intercorrência por parte dos presentes. Como são VIPs e membros da imprensa, todo cuidado é pouco;
- **Equipe de Segurança** – Composta por pessoal treinado e capacitado em controle de público e evacuação (treinamento padrão de brigada de incêndio), discretamente presentes no ambiente do teatro;

- **Central de monitoramento** – Com vista para o teatro, monitores contendo informações em tempo real coletadas por:
    - todas as câmeras;
    - todos os sensores de movimento;
    - todos os sensores de temperatura;
    - todos os detectores de fumaça, previamente instalados como parte do projeto principal do edifício.

O modelo apresentado anteriormente é útil e robusto, mas, claro, admite variações e adições que podem ser propostas por você e sua empresa a fim de conseguir o contrato da Sider.

As informações acima deverão ser apresentadas sob forma de projeto contendo:

- Nome do Projeto
- Data de emissão
- Nome do responsável
- Ações a serem realizadas (implantação passo a passo das tecnologias listadas acima)
- Cronograma de implantação (separando ação por ação)
- Custo individual de cada ação

Pronto! Seu projeto de monitoramento/controle de acesso está entregue e concorrendo ao contrato valioso da Sider!

Avançando na prática

Melhorando a segurança do transporte de cargas

Descrição da situação-problema

O senhor Denézio Lengrius é dono da Transportadora Tanaporta, que trabalha com cargas de insumos para a indústria (em geral, amido, glicose, malte e outros insumos necessários para a indústria alimentícia.

Em várias ocasiões os caminhões de Denézio – sempre guiados por motoristas qualificados e experientes – se envolveram em

acidentes que exigiram o acionamento do seguro por parte da Tanaporta, uma vez que os envolvidos alegaram não ter culpabilidade. Como a Tanaporta não pode deixar de fazer suas entregas, Denézio optou por arcar com os valores das franquias do que envolver seus caminhões em longos períodos de análise pericial.

Ocorre que os acidentes seguidos de acionamento do seguro tendem a provocar aumento dos valores quando da renovação. Denézio está desesperado com o aumento de seus custos, e não quer que no futuro cresçam ainda mais. Sua empresa é especializada em segurança no setor de transporte, e inclusive já implantou os sistemas de rastreamento que hoje protegem as cargas da Tanaporta. Como ajudá-lo?

Resolução da situação-problema

Uma solução interessante para a Tanaporta é a associação das tecnologias de segurança para locais (segurança perimetral) com a segurança para veículos automotivos. Para tanto, podemos utilizar as câmeras de segurança, com armazenamento local nos caminhões, o que demandará a implantação de um pequeno computador com amplo espaço em isco para armazenamento das imagens.

Esta solução pode incluir:

- uma câmera frontal, filmando o que ocorre na frente do caminhão;
- uma câmera traseira, filmando os veículos ultrapassados ou que se aproximam para ultrapassagem;
- câmeras laterais, filmando o tráfego que passa ao largo do caminhão.

As câmeras colhem vídeos de toda a viagem. E caso de normalidade, as imagens podem ser apagadas; porém em caso de acidente, as imagens podem ser utilizadas para determinação de culpabilidade. Como os motoristas da Tanaporta são treinados, a determinação de responsabilidade pode poupar a Tanaporta de gastos com franquias e reduzir o valor da renovação das apólices de seguro. Já em caso de responsabilidade do motorista da Tanaporta, a empresa pode usar as imagens para novos treinamentos e reciclagens para seus motoristas.

Faça valer a pena

1. Observe as funções de soluções de segurança na coluna da esquerda e exemplos dessas características na coluna da direita:

I.	Inibir/Dissuadir	A.	Extintor de Incêndio
II.	Impedir	B.	Material de construção não-inflamável
III.	Retardar	C.	Firewall
IV.	Responder	D.	Câmera de Segurança

Assinale a alternativa que contém a correspondência correta entre as colunas:

a) I-A, II-B, III-C, IV-D
b) I-D, II-B, III-C, IV-A
c) I-C, II-D, III-B, IV-A
d) I-D, II-C, III-A, IV-B
e) I-D, II-C, III-B, IV-A

2. Um sistema inteligente de monitoramento que envia um alerta para outro ou para algum operador do sistema que deva ser avisado da ocorrência, a qual de fato incidiu sobre o ambiente monitorado está realizando uma tarefa específica. Tal tarefa é inerente aos sistemas inteligentes de monitoramento.

Assinale a alternativa que contém a tarefa a que o texto base se refere:

a) Registrar imagens.
b) Registrar eventos por meio de imagens.
c) Registrar eventos por meio de sensores.
d) Responder a eventos.
e) Responder a eventos por meio de sensores.

3. Um elemento fundamental é o _____. Por mais que _____ tenha papel preponderante nos projetos de segurança e controle de acesso a eventos, nenhum projeto é efetivo sem a participação de _____ para lidar tanto com o público e situações de normalidade, quanto com ocorrências de várias naturezas.

Assinale a alternativa que contém os termos que completam corretamente o texto apresentado.

a) tecnológico, a segurança, tecnologia confiável
b) humano, a tecnologia, pessoal treinado
c) tecnológico, o efetivo policial, leis e regulamentos
d) humano, o efetivo militar, leis e regulamentos
e) tático, a estratégia, planejadores

Referências

BRASILIANO, A. C. R.; BLANCO, L. **Manual de Planejamento Tático e Técnico de Segurança Empresarial.** São Paulo: Sicurezza, 2003.

BRASILIANO, A. C. R., BLANCO, L., **Planejamento Tático e Técnoco em Segurança Empresarial.** São Paulo: Sicurezza, 2003.

DA CRUZ, F. C. **Proposta de projeto:** sistema de segurança eletrônica. REPOSITÓRIO DE RELATÓRIOS-Engenharia Elétrica 1 (2017). Disponível em: <https://revista.uniplac.net/ojs/index.php/engeletrica/article/download/3029/1201>. Acesso em: 10 dez. 2017.

ENSSLIN, L., Um estudo sobre segurança em estádios de futebol baseado na análise bibliométrica da literatura internacional. **Revista Perspectivas em Ciência da Informação**, v. 17, n. 2, 2012.

FEITOSA, R. Q., **Reconhecimento Facial em Vídeo com uma amostra por pessoa utilizando Stacked Supervised Auto-encoder**. Tese de Doutorado, PUC-Rio, 2016. Disponível em: <http://www2.dbd.puc-rio.br/pergamum/tesesabertas/1422395_2016_completo.pdf>. Acesso em: 3 jan. 2018.

KIRCHMER, M. **High performance Through Business Process Management**. 3. ed. Nova York: Springer, 2017.

MARIN, L., KRAJCIKOVA, K. **Deploying Drones in Policing Southern European Borders: Constraints and Challenges for Data Protection and Human Rights, in Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance.** Nova York: Springer, 2016.

PEREIRO, W. C., **Sistema de Monitoramento Inteligente Radar Tech**, Site Linked In, publicado em 29 maio 2017. Disponível em: <https://pt.linkedin.com/pulse/sistema-de-monitoramento-inteligente-radar-tech-carvalho-pereiro>. Acesso em: 3 jan. 2018

ROGERS, A., HILL, J. **Unmanned: drone warfare and global security**. Toronto: Plutopress, 2014.

SILVA, J. E. **Rastreador de carro**: como funciona e quais as vantagens. Site Seguro

Auto, publicado em 05 jun. 2017. Disponível em: <https://www.seguroauto.org/rastreador-de-carro>. Acesso em: 9 dez. 2017.

SOLANAS, A. B., A. M. **Advances in Artificial Intelligence for Privacy Protection and Security.** Nova York: World Scientific, 2010.

TSA, Transportation Security Administration. **How It Works: Advanced Imaging Technology.** Site Web Archive. Disponível em: <https://web.archive.org/web/20101203034020/http://www.tsa.gov/approach/tech/ait/how_it_works.shtm>. Acesso em: 19 dez. 2017.

UEFA, União Europeia de Associações de Futebol, **Estádios e Segurança**, Site da UEFA, 2017. Disponível em: <http://pt.uefa.com/insideuefa/protecting-the-game/security/index.html>. Acesso em: 03 jan. 2018.

VINHOLES, T. **Como o raio-x dos aeroportos enxergam por dentro das malas.** Site Airways, publicado em 23 dez. 2015. Disponível em: <https://airway.uol.com.br/como-o-raio-x-dos-aeroportos-enxergam-por-dentro-das-malas/>. Acesso em: 19 dez. 2017.

Anotações

Anotações

ISBN 978-85-522-0639-2