Fonte

ISSN 1808-0715

Tecnologia da Informação na Gestão Pública

Ano 9 - Número 12

Dezembro de 2012

Distribuição gratuita

www.prodemge.gov.br

Segurança da informação em rede

A vida on-line e suas contingências

45 anos prodemge

Prodemge, há 45 anos conectando Minas ao futuro.

Há 45 anos, a Prodemge trabalha para oferecer à administração pública de Minas soluções tecnológicas inovadoras que auxiliam na modernização do Estado e facilitam o dia a dia do cidadão.

45 anos prodemge

www.prodemge.gov.br

Uma publicação da:
prodemge
Companhia de Tecnologia da Informação do Estado de Minas Gerais
Ano 9 - nº 12 - Dezembro de 2012

Governador do Estado de Minas Gerais
Antonio Augusto Junho Anastasia
Vice-Governador
Alberto Pinto Coelho
Secretária de Estado de Planejamento e Gestão
Renata Maria Paes de Vilhena
Diretora-Presidente
Isabel Pereira de Souza
Vice-Presidente
Antônio Alberto Moreira de Castro
Diretor de Desenvolvimento de Sistemas
Paulo Cesar Lopes
Diretor de Gestão Empresarial
Nathan Lerman
Diretora de Negócios
Maria Luiza Jakitsch
Diretor de Produção
Raul Monteiro de Barros Fulgêncio

CONSELHO EDITORIAL
Amílcar Vianna Martins Filho
Gustavo da Gama Torres
Isabel Pereira de Souza
Marcio Luiz Bunte de Carvalho
Marcos Brafman
Maurício Azeredo Dias Costa
Paulo Kléber Duarte Pereira

EDIÇÃO EXECUTIVA
Gerência de Marketing
Gustavo Grossi de Lacerda
Edição, Reportagem e Redação
Júlia de Magalhães Carvalho – MG 10249 JP
Colaboração
Isabela Moreira de Abreu
Carine Alves de Carvalho
Gabriel Sales
Artigos Universidade Corporativa
Flávia Fernanda Carvalho da Motta
Capa
Guydo Rossi
Coordenação da Produção Gráfica
Guydo Rossi
Consultoria Técnica
Carine Alves de Carvalho
Evandro Nicomedes Araújo
Revisão
André Luiz
Diagramação
Guydo Rossi
Impressão
Imprensa Oficial do Estado de Minas Gerais
Tiragem
3.000 exemplares
Periodicidade
Anual
Patrocínio/Apoio Institucional
Lívia Mafra
(31) 3915-4114 / revistafonte@prodemge.gov.br

A revista **Fonte** visa à abertura de espaço para a divulgação técnica, a reflexão e a promoção do debate plural no âmbito da tecnologia da informação e comunicação, sendo que o conteúdo dos artigos publicados nesta edição é de responsabilidade exclusiva de seus autores.

Prodemge - Rodovia Prefeito Américo Gianetti, nº 4.143 - Serra Verde - CEP 31630-901
Belo Horizonte - MG - Brasil
www.prodemge.gov.br
prodemge@prodemge.gov.br

Editorial

A presente edição da revista Fonte retoma a reflexão sobre Segurança da Informação, tema que a cada dia assume maior relevância no contexto da sociedade em rede. Sob o ritmo acelerado de nosso cotidiano on-line, é difícil conceber, hoje, quaisquer atividades ou processos de negócio – dos mais prosaicos aos mais críticos – que prescindam do suporte de algum tipo de infraestrutura tecnológica.

Trata-se de um cenário por vezes paradoxal. As novas tecnologias das redes e ambientes digitais descortinam oportunidades e viabilizam avanços sociais antes inimagináveis; ao mesmo tempo, essa ambiência virtual também dá ensejo a uma série de riscos, dilemas e inquietações. Desse modo, cinco anos desde que o assunto Segurança da Informação foi tratado pela primeira vez nas páginas desta revista, pode-se afirmar que ele se tornou uma das principais preocupações na pauta de gestores das áreas pública e privada. Mas, de lá até aqui, o que de fato mudou para motivar essa postura?

Aborda-se agora a Segurança da Informação em rede. O mundo está cada vez mais interconectado à rede e dependente dela. As implicações desse fenômeno são variadas e não se limitam ao campo tecnológico, movimentando também as searas política, econômica, jurídica, comunicacional e cultural. Vivenciamos o crescimento das redes sociais, que saem do âmbito privado para invadir o dia a dia corporativo, fato impulsionado pelo uso exponencial dos dispositivos móveis.

As organizações têm que se estruturar para proteger suas informações, preservar o legado informacional, conscientizar colaboradores e garantir a continuidade do negócio. Ocorrem ameaças e ataques cada vez mais diversificados, sofisticados e insidiosos por parte daqueles que se valem das conquistas tecnológicas como meio para cometer ilicitudes nas redes; crimes cibernéticos, vazamento de dados, quebra de sigilo e invasão de privacidade começam a provocar reações da sociedade.

Discute-se no país um novo marco regulatório, com um arcabouço legal que proteja os cidadãos, dinamize o mercado e possibilite respostas rápidas e eficientes para os novos imbróglios jurídicos surgidos. Tudo isso exige que se repense as políticas e normas de Segurança da Informação, adequando-as a essa nova realidade, inclusive frente às iniciativas voltadas à transparência e ao acesso às informações de interesse público.

Para revisitar uma temática que está em plena efervescência, contamos nesta edição com o apoio precioso de nossos colaboradores, os quais oferecem um painel reflexivo e multidisciplinar acerca da segurança da informação em rede. Vale destacar que a Segurança da Informação é compromisso e um pilar da atuação da Prodemge, hoje celebrando 45 anos de uma trajetória que coloca a tecnologia da informação a serviço da gestão publica em Minas.

Boa leitura a todos!

Diretoria da Prodemge

Sumário

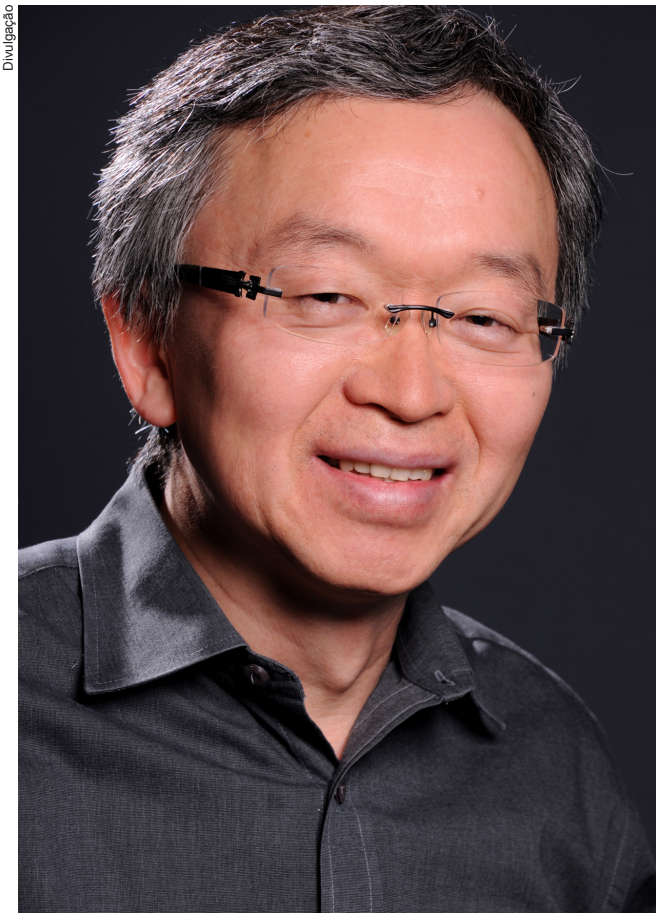
Fonte
Ano 9 - Dezembro de 2012
prodemge
Tecnologia de Minas Gerais

Diálogo

Segurança da Informação em rede

Os desafios trazidos por um mundo cada vez mais conectado e os impactos para usuários e organizações

Divulgação



Milton Kaoru

Para promover a qualidade técnica, inovação e disseminação dos serviços de internet no Brasil, um grupo formado por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica trabalha há 17 anos coordenando e integrando todas as iniciativas relacionadas à implantação, administração e uso da rede em território brasileiro. É o Comitê Gestor da Internet no Brasil (CGI.br). Suas decisões e projetos são implementadas pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), uma entidade civil sem fins lucrativos que mantém o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira (Cert.br) para estudar, responder e tratar incidentes de segurança no país.

Esse grupo também atua na conscientização sobre os problemas de segurança, na análise de tendências e correlações entre eventos na internet brasileira e no auxílio ao estabelecimento de novos grupos de segurança e resposta a incidentes (CSIRTs) no Brasil.

Para falar sobre os novos cenários que a segurança da informação enfrenta, a revista Fonte entrevistou o diretor de Projetos Especiais e de Desenvolvimento do NIC.br, Milton Kaoru Kashiwakura; a gerente-geral do CERT.br, Cristine Hoepers; e a analista de Segurança do CERT.br Miriam von Zuben.

Fonte: *Quais os problemas de infraestrutura que a internet enfrenta no Brasil?*

Milton Kaoru: O país tem as infraestruturas básicas da internet: cabos submarinos ligando o Brasil a outros países, fibras conectando o Brasil de norte a sul, Pontos de Troca de Tráfego (http://ptt.br), cópias de servidores DNS raízes (http://root-servers.org), servidores DNS do .br espalhados pelo Brasil e pelo mundo, alguns servidores DNS secundários de países como Coreia, Chile e Alemanha, servidores NTP (http://ntp.br) distribuídos pelo país com capacidade suficiente para sincronizar todos os computadores conectados no Brasil, data centers para prover serviços e conteúdos. Falta cobertura, espalhar os serviços de acesso à internet banda larga fixa, levando a internet para cidades ainda não atendidas e a bairros em cidades metropolitanas ainda não atendidos, ampliar a cobertura do acesso móvel 3G, instalar 4G e, a longo prazo, investir em cabos submarinos para ligar a outros continentes.

Os governos federal, estadual e municipal devem incentivar investimentos e propor políticas para que promovam a competição no serviço de acesso, além de criar condições que conduzam à redução de custo de infraestrutura para que o Brasil atraia conteúdos e serviços de internet para o país.

Divulgação

Miriam von Zuben

Fonte: *O Brasil tem 83,4 milhões de internautas, segundo o Ibope (os números são do primeiro trimestre de 2012). No mundo, são mais de 2,1 bilhões de usuários, de acordo com a empresa de monitoramento de sites Pingdom. Com o seu desenvolvimento e amplitude exponenciais, a internet está ficando mais segura ou insegura? Por quê?*

Miriam von Zuben: O cenário atual, composto pelo crescimento no número de internautas e pelo aumento da importância da internet no dia a dia de pessoas e empresas, acabou por resultar no aumento dos ataques em si.

Esse aumento é uma tendência mundial, uma vez que a internet passa a ocupar, cada vez mais, um importante papel na sociedade. Isso atrai interesse por parte de todos, incluindo aqueles que tentam obter alguma vantagem ilícita através do uso da rede.

Esse aumento em si não necessariamente torna a internet mais ou menos segura, uma vez que o que define isso é o conjunto de medidas preventivas que é tomado por todos aqueles que a utilizam.

Fonte: *O governo brasileiro está adotando o Plano Nacional de Banda Larga, que tem o objetivo de massificar até 2014 a oferta de acessos de internet banda larga para a população. Quais os impactos que essa inclusão digital pode causar?*

Cristine Hoepers: Do ponto de vista da segurança, o maior desafio será a parte de conscientização dos novos usuários. Nesse processo, os usuários terão não só o desafio de aprender a utilizar novas tecnologias, como também de aprender sobre os riscos e como se proteger.

A nova estrutura da nossa Cartilha de Segurança para Internet (cartilha.cert.br) já levou em conta esse desafio. Ela foi pensada não apenas como um livro com dicas de segurança, mas como um conjunto de materiais que pode ser utilizado para multiplicar o conhecimento aos novos usuários entrantes. Os fascículos da Cartilha abordarão diversos assuntos específicos e serão acompanhados por slides, que podem ser usados em palestras, aulas ou qualquer outra iniciativa de conscientização.

> "A chave é realmente pensar que é um processo e, mais que isso, um processo que precisa envolver todos."

Fonte: *Como o crescimento da internet e o desenvolvimento de novas tecnologias, como os dispositivos móveis, estão impactando a segurança da informação nas redes?*

Miriam von Zuben: O crescimento da internet, a grande popularidade dos dispositivos móveis, a facilidade de conexão que esses equipamentos oferecem e a grande quantidade de informações que eles armazenam trouxeram novos desafios relacionados à segurança de informação. Novos sistemas e aplicativos foram desenvolvidos enquanto outros tiveram que ser adaptados.

Todo esse novo cenário traz impactos diretos à segurança da informação nas redes, exigindo a criação de novas políticas e/ou adaptação das já existentes.

Fonte: *Quais os passos necessários para uma organização construir sua política de segurança da informação?*

Miriam von Zuben: A política de segurança define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra.

O passo fundamental para a construção de uma política de segurança da informação é conhecer o ambiente ao qual ela se aplica e, com base nele, deixar claro o comportamento esperado de cada um. Dessa forma, casos de mau comportamento, que estejam previstos na política, podem ser tratados de forma adequada pelas partes envolvidas.

Fonte: *Quais os fatores de sucesso na implantação de um processo de segurança da informação?*

Cristine Hoepers: A chave é realmente pensar que é um processo e, mais que isso, um processo que precisa envolver todos. A administração superior precisa apoiar a implantação e dar o exemplo no cumprimento das políticas. Essas políticas devem ser desenvolvidas com participação de todos os setores, especialmente para que reflitam a realidade da organização, ou seja, que forneçam um nível aceitável de segurança, mas que não interfiram no negócio da organização. E, por fim, todos os funcionários precisam entender que fazem parte desse processo.

Miriam von Zuben: É importante lembrar que, para aumentar as chances de sucesso na implantação de um processo de segurança de informação, é importante que ele seja, de tempos em tempos, revisto e atualizado. Dessa forma, estará adequado às necessidades da empresa.

Fonte: *Qual a importância do usuário (internauta) para a eficiência de uma política de segurança da informação?*

Miriam von Zuben: O usuário tem papel fundamental para a eficiência de uma política de segurança da informação. Temos observado que nos últimos anos os atacantes têm concentrado esforços na exploração das fragilidades dos usuários, por meio de ataques de engenharia social.

Cristine Hoepers: Por isso, é cada vez mais importante que as organizações implementem programas de treinamento e conscientização, pois os usuários precisam não só entender os riscos, como saber como implementar as medidas necessárias de proteção.

Fonte: *Pensando em normas, certificações, modelos e boas práticas, empresas que têm um baixo nível de maturidade em suas operações de segurança da informação devem seguir qual modelo de evolução?*

Cristine Hoepers: O mais importante é que cada organização procure implementar políticas e procedimentos que estejam de acordo com sua cultura e que tenham o objetivo de mitigar os riscos identificados para a sua organização em particular – através de um processo de análise de riscos, por exemplo.

Para que a chance de sucesso seja maior, é importante que as diversas áreas da organização sejam envolvidas em um projeto de definição e implantação das políticas. As áreas de negócio precisam apontar o que é chave para cumprir a missão da organização, a área jurídica deve avaliar os impactos legais e as áreas técnicas para identificar como implantar as tecnologias necessárias.

Fonte: *Existe algum movimento de organizações, públicas ou privadas, buscando a união para tratar e enfrentar as ameaças de segurança da informação?*

Cristine Hoepers: Existem diversas iniciativas de cooperação em andamento, tanto no setor público quanto no setor privado. Existem grupos de trabalho, setores da indústria que se reúnem periodicamente, bem como fóruns para a discussão dos assuntos relativos a incidentes de segurança. Como as questões relativas à segurança das organizações são sensíveis, esses fóruns em geral não são públicos. A chave é que cada organização procure conhecer profissionais de segurança da comunidade e participar de congressos e reuniões da área. Um bom local para conhecer alguns desses profissionais são as reuniões do Grupo de Trabalho de Segurança do CGI.br (http://gts.nic.br/). Esse é um evento gratuito, que ocorre duas vezes ao ano, em que profissionais de segurança se reúnem para compartilhar boas práticas na área de segurança.

Divulgação

Cristine Hoepers

Fonte: *Quais os benefícios e as desvantagens para as empresas em aderir ao movimento Bring Your Own Device (BYOD), que incentiva os empregados a utilizarem seus próprios dispositivos móveis*

para realizar tarefas do trabalho?

Miriam von Zuben: Os benefícios e as desvantagens dependem muito de como esse movimento está sendo implementado na empresa, já que não existe uma forma única de implementação:

De forma geral, os benefícios para as empresas são:

- possível aumento de produtividade: já que os funcionários passam a usar equipamentos e sistemas de sua preferência aos quais, provavelmente, estão mais familiarizados;
- redução com custos de equipamentos, tanto de aquisição como para atualização tecnológica: devido ao constante lançamento de novos modelos, das promoções feitas por lojas/operadoras e do desejo dos usuários de sempre terem os modelos mais atuais, fica mais fácil para as empresas terem os equipamentos atualizados.

De forma geral, as desvantagens para as empresas são:

- maior possibilidade de vazamento de informações: uma vez que os dados empresariais ficam armazenados em equipamentos com maior possibilidade de perda ou furto, já que é mais difícil garantir a segurança física deles;
- dificuldade em prover suporte e manutenção a dispositivos de diferentes fabricantes e com diferentes versões de sistemas operacionais e aplicativos: isso pode também gerar incompatibilidade entre sistemas e aplicações;
- dificuldade em separar os contextos: é necessário que haja uma política clara sobre os direitos e deveres da empresa e dos funcionários relativos, por exemplo, ao dispositivo, aos aplicativos instalados e aos dados armazenados. Questões relativas aos custos relacionados ao acesso à internet ou a ligações feitas devem estar claras, assim como responsabilidades de reposição do equipamento em caso de perda ou furto ou de exclusão de dados em caso de desligamento da empresa.

> “De forma geral, os cuidados de segurança que um usuário de dispositivo móvel deve ter ao utilizar seu aparelho são os mesmos aplicados ao uso de computadores pessoais, como mantê-lo sempre atualizado...”

Fonte: *Quais os cuidados de segurança que um usuário de dispositivo móvel deve ter ao utilizar seu aparelho?*

Miriam von Zuben: De forma geral, os cuidados de segurança que um usuário de dispositivo móvel deve ter ao utilizar seu aparelho são os mesmos aplicados ao uso de computadores pessoais, como mantê-lo sempre atualizado e utilizar mecanismos de segurança (como antivírus e firewall pessoal).

Outros cuidados complementares a serem tomados são:

- ser cuidadoso ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e plug-ins;
- manter as informações sensíveis sempre em formato criptografado;
- fazer backups periódicos dos dados nele gravados;
- manter controle físico sobre ele, principalmente em locais de risco (procurar não deixá-lo sobre a mesa e ter cuidado com bolsos e bolsas quando estiver em ambientes públicos);
- configurar para que seja localizado e bloqueado remotamente, por meio de serviços de geolocalização (isso pode ser bastante útil em casos de perda ou furto).

Mais detalhes e outros cuidados a serem tomados estão disponíveis na Cartilha de Segurança para Internet, mais especificamente no capítulo 14, Segurança em Dispositivos Móveis (http://cartilha.cert.br/dispositivos-moveis).

Fonte: *Como o Direito e a Segurança da Informação podem ou devem trabalhar em conjunto para acompanhar as mudanças de tecnologia, as vulnerabilidades da rede e seus riscos?*

Cristine Hoepers: Um ponto importante é lembrar um dos Princípios para a Governança e Uso da Internet no Brasil: a inimputabilidade da rede. Esse princípio nos diz que "o combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos" (mais sobre os princípios em: http://www.cgi.br/regulamentacao/resolucao2009-003.htm). Ou seja, devemos lembrar que a internet é um meio para cometer determinados crimes, mas a tipificação diz respeito à conduta, não à tecnologia usada. Por exemplo, uma calúnia pode ser cometida por meio de revista, jornal, TV ou internet, mas será o mesmo crime, independente do meio. O mesmo vale para crimes como estelionato ou furto.

Claro que cada nova tecnologia traz novos desafios para a preservação e coleta de evidências, a realização de investigações e a formação de provas. Mas isso já ocorreu no passado, com inovações como armas de fogo, energia elétrica, automóveis, sistemas de telefonia, entre outros.

"Claro que cada nova tecnologia traz novos desafios para a preservação e coleta de evidências..."

Fonte: *O crescimento da internet, das redes sociais e do uso de dispositivos móveis está fazendo aumentar a quantidade de dados pessoais nas redes. Como as pessoas podem garantir a privacidade de seus dados?*

Miriam von Zuben: Para tentar preservar a privacidade e proteger os dados pessoais, há algumas medidas básicas que os usuários devem tomar, como:

- procurar diminuir a quantidade de informações pessoais que possam ser coletadas: restringindo e reduzindo as informações disponibilizadas;
- ser cuidadoso ao disponibilizar informações: considerar que está em um local público, que tudo que é divulgado pode ser lido ou acessado por qualquer pessoa, tanto agora como futuramente;
- pensar bem antes de divulgar algo, pois não há possibilidade de arrependimento;
- usar as opções de privacidade oferecidas pelos sites e procurar ser o mais restritivo possível;
- ser seletivo ao aceitar amigos/seguidores, pois quanto maior a rede de relacionamento maior é o número de pessoas com acesso às suas informações;
- ser cuidadoso ao fornecer a localização geográfica e ao elaborar as senhas de acesso.

Mais detalhes e outros cuidados a serem tomados estão disponíveis na Cartilha de Segurança para Internet, mais especificamente no capítulo 11, Privacidade (http://cartilha.cert.br/privacidade).

Fonte: *A Lei de Acesso à Informação entrou em vigor no país em maio de 2012. Um dos seus princípios diz respeito aos dados abertos, que permite a qualquer pessoa usá-los, reutilizá-los e redistribuí-los. A Lei também prevê que os sítios eletrônicos devem garantir a autenticidade e a integridade das informações disponíveis para acesso. Essas duas situações são compatíveis?*

Cristine Hoepers: Primeiramente, devemos olhar duas definições presentes no Capítulo 7 da Cartilha de Segurança para Internet:

- Integridade: proteger a informação contra alteração não autorizada.
- Não repúdio: evitar que uma entidade possa negar que foi ela quem executou uma ação.

A autenticidade está relacionada ao não repú-

dio, ou seja, à garantia de que uma informação esteja realmente sendo prestada por um determinado órgão.

Esses conceitos não só são compatíveis com o princípio de dados abertos, como essenciais para garantir a qualidade dos dados que estão sendo disponibilizados pelos órgãos governamentais.

Fonte: *Eugene Kaspersky, fundador da desenvolvedora de softwares de proteção de computadores Kaspersky Lab, que em 2009 descobriu o malware que infectou a rede que comandava centrífugas de urânio no Irã, afirmou em entrevista para o jornal* Folha de S. Paulo *que "estamos sentados sobre um barril de pólvora, e estamos serrando o galho que sustenta toda a internet, e junto toda a infraestrutura do planeta". Qual sua opinião sobre a afirmação de Eugene?*

Cristine Hoepers: Creio que seja sempre salutar avaliar qualquer declaração com cuidado.

Por um lado, a internet realmente não foi projetada levando em conta o seu uso tão disseminado. Está cada vez maior a dependência de diversos serviços críticos da internet, incluindo smart grids, comunicação e serviços financeiros. Mas, por outro, a implantação de medidas de segurança de forma planejada e bem avaliada pode trazer o uso da internet para níveis aceitáveis de risco. É sempre bom lembrar que não existe nenhuma atividade sem algum risco envolvido, e não é diferente na internet.

Encaro metáforas como essa da declaração uma tentativa de ilustrar o que pode acontecer caso as medidas necessárias de segurança não sejam tomadas.

Fonte: *Quais as novas tecnologias e soluções que estão sendo usadas na segurança da informação?*

Cristine Hoepers: Mais importante que utilizar a tecnologia mais recente, é aplicar a tecnologia certa no lugar certo.

Nenhuma tecnologia sozinha aumentará a segurança. Profissionais bem treinados, processos bem estabelecidos e usuários esclarecidos sobre os riscos e seu papel em mitigá-los são os fatores que realmente fazem a diferença na proteção das organizações.

Fonte: *Como você enxerga o futuro da internet e da segurança da informação?*

Cristine Hoepers: A internet já faz parte das nossas vidas e não temos mais como pensar na evolução da nossa sociedade sem conectividade. Muitas mudanças devem vir no futuro, incluindo novas versões de protocolos, como o IPv6, que substituirá o IPv4. A segurança das redes provavelmente será cada vez mais importante, pois os serviços on-line são cada vez mais prevalentes e a comodidade e agilidade são inegáveis.

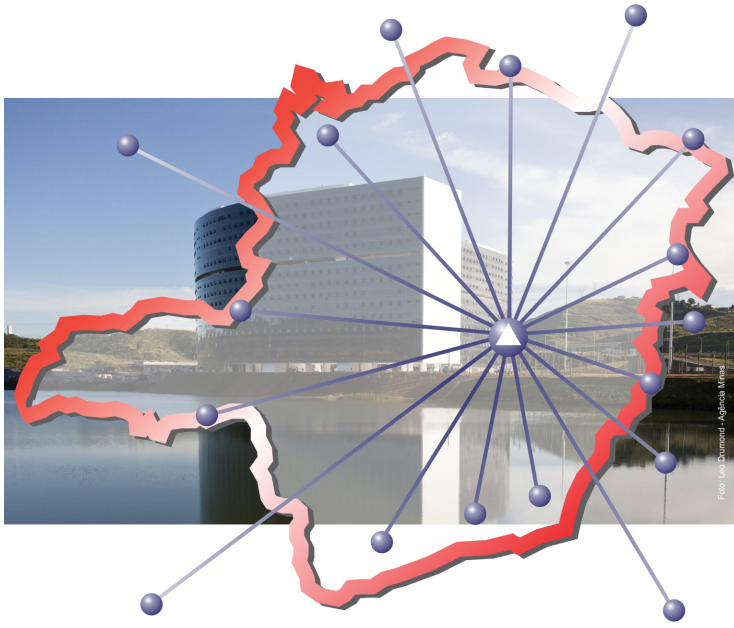
> "...a agilidade na detecção e no tratamento fará a diferença entre um incidente com grande impacto e um incidente do qual a organização se recupere facilmente."

Porém, as organizações precisam, por um lado, conscientizar-se de que os riscos existem e são diferentes daqueles a que elas estavam acostumadas. Por outro lado, não é possível ter uma segurança perfeita, não existe nenhuma atividade da sociedade que seja 100% livre de riscos. O que a sociedade terá que encontrar nos próximos anos é um nível aceitável de risco e de segurança on-line.

Também será necessário que as organizações criem estruturas eficientes de gestão de incidentes de segurança. Os incidentes ocorrerão, mas a agilidade na detecção e no tratamento fará a diferença entre um incidente com grande impacto e um incidente do qual a organização se recupere facilmente. A gestão de incidentes inclui um grupo de tratamento de incidentes, mas não é somente isso, é necessário ter uma integração entre as diversas áreas e um conjunto de processos que faça a comunicação fluir.

Rede IP Multisserviços,

a infraestrutura que conecta o Estado de Minas Gerais e todos os seus prédios públicos



Uma rede com alcance em todo o território mineiro, interconectando órgãos e transmitindo informações, além de serviços de voz, vídeo e imagem. Essa foi a ideia que nasceu em 2008 e começou a tomar forma em setembro de 2010, quando entrou em operação a Rede IP Multisserviços. Segundo o governo, ela permite ao Estado se instrumentalizar para "prover os serviços essenciais à sociedade com qualidade, rapidez e eficiência". Além disso, a Rede disponibiliza aos órgãos integrados acesso em tempo real e de forma segura às informações corporativas do governo e à internet.

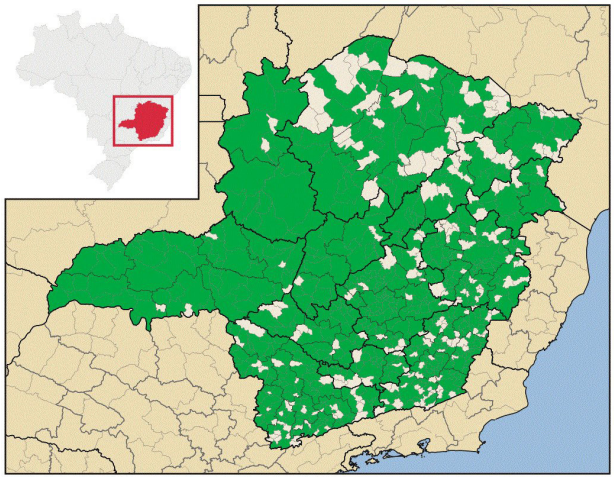
A Rede IP tem dois grandes objetivos: prover acessos a todos os municípios mineiros e interconectar 100% dos órgãos públicos. Ao fazer com que a infraestrutura de telecomunicações chegue ao Estado de Minas Gerais inteiro, o governo abre caminho para que as operadoras atendam também às demandas locais de rede da iniciativa privada, propiciando mais desenvolvimento para os municípios. E esse é o principal objetivo estratégico da Rede.

A Rede IP Multisserviços foi instituída por meio do decreto estadual 45.006/2009, que trouxe um novo modelo de gestão de contratos e de serviços da rede. Antes, os órgãos do Estado contratavam as linhas de dados diretamente com as operadoras, por meio de ata de registro de preços. A partir da criação da Rede, a Companhia de Tecnologia da Informação do Estado de Minas Gerais (Prodemge) é a representante do governo estadual, por meio da Unidade Gestora de Contrato (UGC) e da Unidade Gestora Operacional (UGO), junto às operadoras. Além de acompanhar e monitorar todo o serviço prestado por elas, faz a gestão dos contratos e de faturamento dos órgãos participantes. Desse modo, quem adere à Rede IP só utiliza e paga pelo serviço.

"Esse é um modelo inovador", afirma o superintendente de Redes da Prodemge, Evandro Araújo, "que permite à administração pública estadual um melhor aproveitamento de seus recursos". O decreto também formalizou a obrigatoriedade de todas as secretarias de Estado, órgãos e entidades dependentes de recursos do Tesouro Estadual se integrarem à Rede IP Multisserviços, para garantir o desempenho e a disponibilidade dos serviços e sistemas que são utilizados em meio digital.

Outra característica é que as operadoras vencedoras da licitação fornecem os acessos com roteadores próprios. A Prodemge é a responsável pelo planejamento, implantação e operação do modelo tecnológico de rede, o que permite a interoperabilidade entre as infraestruturas centrais de rede (backbone) das diferentes operadoras e garante a integração dos acessos que compõem a Rede IP Multisserviços. Para possibilitar essa interoperabilidade, a Companhia arquitetou um núcleo de rede baseado na tecnologia Multiprotocol Label Switch (MPLS).

Atualmente, a Rede conta com mais de 2.900 linhas ativas, número que deve chegar a 5.000 em um ano e meio – para efeito de comparação, a antiga rede do Estado contava com pouco mais de mil linhas. A cobertura já chega a mais de 620 cidades, abrangendo áreas urbanas e rurais. A maior concentração de velocidade na Rede IP está entre 384 Kbps e 512 Kbps (54,49%), enquanto que no Brasil ela aparece nas velocidades entre 512 Kbps e 2 Mbps (51%). "Mas é interessante notar que, quando se soma os percentuais de acessos com velocidade entre 512 Kbps e 2 Mbps na Rede IP e no Brasil, há certa similaridade nos números. O Brasil possui 51% da sua rede nesse entorno, enquanto a Rede IP possui 40,1%. A mesma observação se constata para os acessos que estão entre 2 Mbps e 34 Mbps.

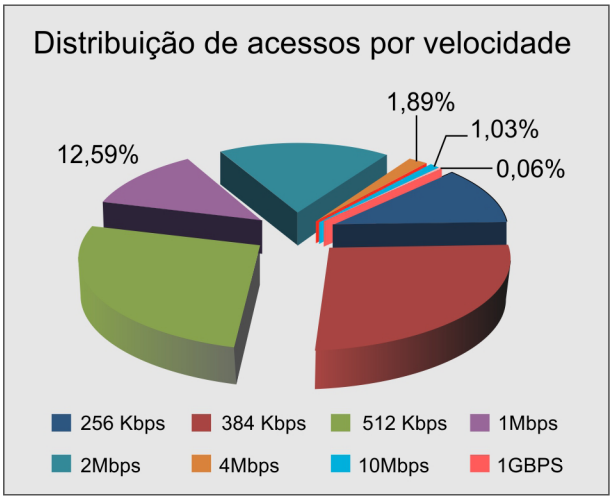


Fonte: Portal da Rede IP Multisserviços – acesso em outubro de 2012

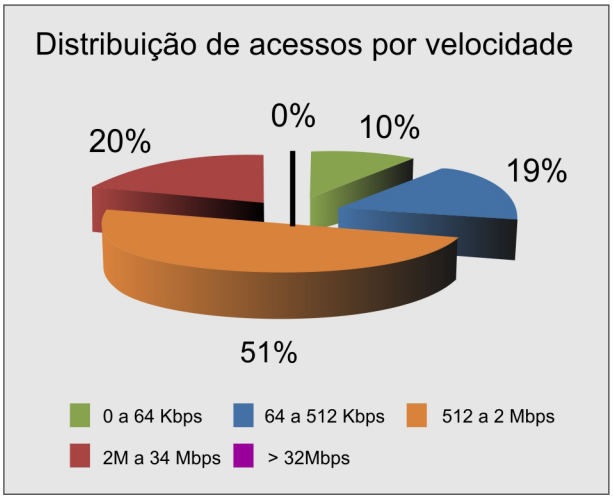
Mapa de cobertura da Rede IP no Estado de Minas – 624 municípios

A Rede IP está em torno de 21,18% e o Brasil, em 20%", ressalta Evandro.

Hoje, a Rede IP interconecta mais de 500 centrais telefônicas IP localizadas nas várias unidades do governo pelo Estado. Essas unidades, incluindo



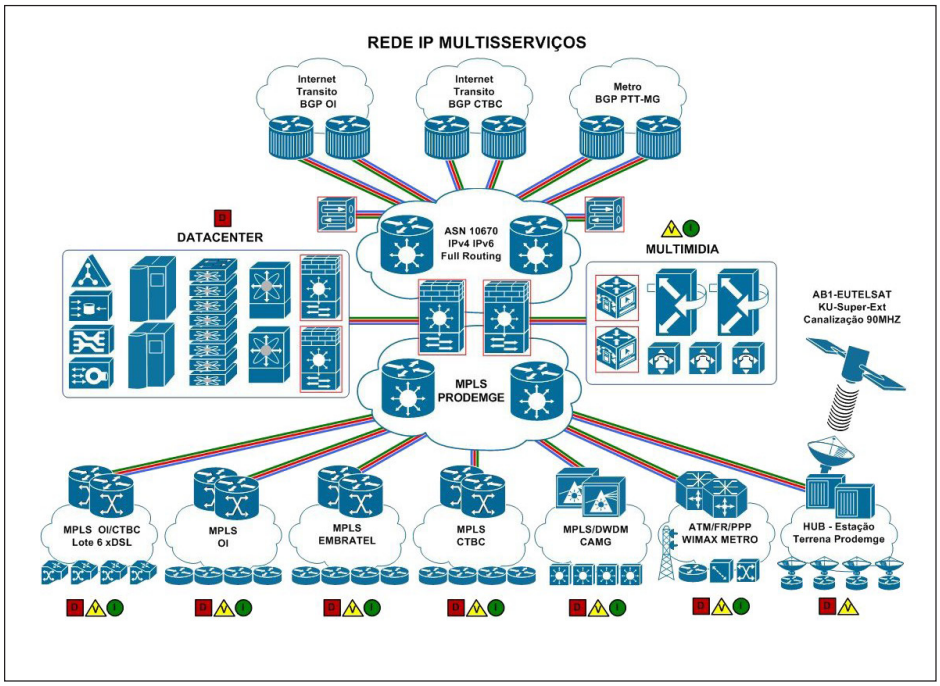
Perfil da distribuição dos acessos por velocidade na Rede IP



Perfil da distribuição dos acessos no Brasil

a Cidade Administrativa Presidente Tancredo Neves (nova sede do governo estadual, inaugurada em 2010), podem fazer ligações telefônicas intragoverno a custo zero por meio da tecnologia de voz sobre IP (VoIP) – estima-se que a economia gerada chegue a 40%.

O sistema de videoconferência também está reduzindo custos de viagens e hospedagens, tendo em vista que reuniões, encontros e capacitações po-



dem acontecer remotamente. Atualmente, três secretarias (Educação, Saúde e Ciência, Tecnologia e Ensino Superior), a Cidade Administrativa, a Fundação Hospitalar do Estado de Minas Gerais e o Instituto de Previdência dos Servidores do Estado de Minas Gerais fazem parte desse sistema, que poderá receber novos integrantes quando um registro de preços para aquisição de end points for lançado. Como a Rede já disponibiliza o MCU (equipamento central para disponibilização do serviço de vídeo conferência), órgãos e secretarias não precisarão adquiri-lo.

Trabalhando na administração de toda essa infraestrutura, existe um centro de gerência chamado de Network Operation Center (NOC). Nele, equipes da Prodemge e das operadoras Oi, Embratel, Auriga e CTBC trabalham continuamente, 24 horas por dia, sete dias por semana, para fazer o monitoramento pró-ativo da rede. Mais de 2.800 ocorrências por mês são tratadas, o que exige uma forte atuação entre as equipes da Prodemge e das operadoras para cumprir os níveis de serviços acordados. “Essa atuação mais próxima é benéfica e diminui o tempo de resposta a qualquer incidente ou problema verificado nos acessos da rede”, conta Evandro.

Outra frente de atuação é o Portal da Rede Governo, sistema desenvolvido especificamente para atender à Rede e aos seus clientes. Com o objetivo de dar mais agilidade e eficiência na prestação dos serviços de rede, ele gerencia e controla todo o processo do serviço, desde a solicitação do acesso pelo órgão, sua instalação, monitoração e acompanhamento de desempenho, o registro de incidentes, a qualidade, o contrato e o faturamento.

Buscando garantir a integridade de toda a informação que trafega na Rede IP Multisserviços, a Prodemge estruturou um sistema de segurança integrado, redundante e com alta capacidade de processamento de dados, utilizando soluções desenvolvidas internamente na empresa e soluções de mercado. Esse sistema é composto por roteadores de alta capacidade, soluções de Firewall e Intrusion Prevention System (IPS) com capacidade de through-put de rede acima de 10 Gbps. “A equipe da Prodemge conseguiu desenvolver uma ferramenta que é capaz de inspecionar, analisar e mitigar ataques internos e externos de rede, a exemplo do syn flood e ataques de domain name server (DNS). Trata-se do Synistro, que hoje compõe o nosso parque de soluções de segurança de redes e bloqueia mais de 20 milhões de tentativas de ataques por semana”, informa Evandro. Outra característica da segurança é a segmentação lógica entre as redes dos órgãos por meio de tecnologia VPN/MPLS. Qualquer comunicação que se faça necessária entre redes locais de órgãos distintos deve, obrigatoriamente, ser autorizada e inspecionada pelo sistema de Firewall. Toda essa infraestrutura de rede está hospedada no data center da Prodemge que segue os padrões de qualidade EIA/TIA 942, Tier 3 e ABNTNBR 15247.

Centro de Operações de Segurança

A Companhia está trabalhando, desde o começo de 2012, na estruturação do Security Operations Center ou centro de operações de segurança (SOC na sigla em inglês), que vai concentrar todas as ações operacionais de segurança, sempre tendo em vista os negócios da empresa. "A Prodemge é o núcleo central de conectividade da Rede IP Multisserviços. Por isso, a atuação do SOC, que é relacionada ao core da Rede, vai beneficiar indiretamente as secretarias e órgãos ligados a ela", explica o superintendente de Planejamento e Monitoramento da Prodemge, Flávio Chagas.

De acordo com a RSA, a divisão de segurança da EMC Corporation, um centro de operações de segurança "monitora continuamente o ambiente de segurança de uma empresa, responde a ameaças imediatas e vulnerabilidades em longo prazo, e proporciona aconselhamento e orientação sobre questões de segurança tanto para o gerenciamento sênior, quanto para as unidades de negócios". A partir desse conceito, foi definido que o objetivo inicial do SOC da Prodemge será monitorar, detectar, analisar e tratar os incidentes de segurança que afetam a disponibilidade da infraestrutura da rede. Para isso, o Centro foi concebido para desempenhar cinco funções: monitoramento, registro, operação, tratamento e gestão de qualidade.

Após elaborar esse modelo funcional, o grupo responsável pela estruturação do SOC está trabalhando no levantamento dos procedimentos, processos e tecnologias já existentes na Companhia para, em seguida, definir a forma de trabalho do Centro. Esse trabalho inclui ainda a identificação de quais serão as integrações necessárias entre processos e onde estão as informações que o Centro precisará para atuar. "Concentrando e fazendo a correlação dos dados, o SOC conseguirá extrair inteligência dessa informação", conta Flávio.

Júlia Magalhães

Flávio Lima Chagas

Os centros de operações de segurança são uma tendência em unir as atividades de segurança dos ativos das empresas sob responsabilidade de diversas áreas. "Essa disciplina é relativamente nova no mercado brasileiro, por isso não há uma receita pronta. Cada instituição está estudando e descobrindo o melhor jeito para implantar o seu SOC, que pode ter diferentes focos de atuação, como fraudes, vazamento de informações, infraestrutura de rede, servidores ou aplicações", analisa Flávio. O superintendente cita como exemplo as experiências do Banco do Brasil, do Serviço Federal de Processamento de Dados (Serpro) e da Telefônica. Internacionalmente, Estados Unidos e Inglaterra são os países onde essa cultura está mais sedimentada: "Os relatos mais antigos de iniciativas como essa são de dez anos atrás", conclui.

Ataques à estrutura de rede

"O ataque hacker às páginas da Presidência da República, Portal Brasil e da Receita na madrugada desta quarta-feira foi o maior já sofrido pela rede de computadores do governo brasileiro. De acordo com o Serviço Federal de Processamento de Dados (Serpro), o ataque – que não causou danos às informações disponíveis nas páginas – partiu de servidores localizados na Itália. Para derrubar os sites, os hackers utilizaram sistemas que faziam múltiplas tentativas de acesso ao mesmo tempo, técnica batizada de 'negação de serviço' e conhecida pelas iniciais em inglês DDoS (Distributed Denial of Service). O objetivo dessa ação é tornar o serviço indisponível. A ação foi reivindicada pelo grupo LulzSecBrazil, que teria ligações com o LulzSec, responsável por ataques recentes a empresas de videogame como Sony e Nintendo, às redes de televisão americanas Fox e PBS e a órgãos governamentais americanos como a CIA (agência de inteligência americana) e o FBI (polícia federal), além do serviço público de saúde britânico, o NHS."

Essa notícia foi divulgada pelo portal G1 em junho de 2011 e é apenas um exemplo dos vários ataques a sites do governo brasileiro conduzidos por hackers neste ano. Segundo o gerente de Redes da Prodemge, Rafael Freitas, esse tipo de ação, que atinge a infraestrutura da rede, está crescendo. "Hoje o foco são os ataques que atingem a 'raiz' da rede, derrubam um site ou param a rede; sem que haja necessariamente roubo ou vazamento de informações", explica.

O DoS (Denial of Service, ou negação de serviço), por exemplo, consiste na perda de desempenho proposital de serviços ou sistemas, impossibilitando o uso pelas pessoas que os acessam. Apesar de ser fácil de detectar, é difícil de ser sanado, já que geralmente utiliza outras técnicas para esconder a origem real do ataque. Sua variante é o DDoS, técnica utilizada no ataque ao sítio da Presidência da República em 2011. Pelo fato do ataque ter origens diversas, o trabalho de mitigá-lo se torna ainda mais complexo. Normalmente, máquinas "zumbis" são utilizadas para fazer o ataque – o que, inclusive, está se tornando um negócio, com pessoas na internet vendendo ou alugando máquinas e servidores para fazer esse 'serviço'.

Outro tipo de ataque é o defacement (termo em inglês que significa modificar ou danificar a superfície ou aparência de algum objeto), que modifica a página inicial de um sítio na internet – o autor do ataque geralmente coloca uma mensagem ou imagem de cunho político. Um exemplo desse tipo de ataque foi o sofrido pelo sítio do Instituto Brasileiro de Geografia e Estatística, em 24 de junho de 2011. Nesse dia, a página foi alterada por uma imagem de um olho com as cores da bandeira do Brasil e uma mensagem explicando a ação. "Entendam tais ataques como forma de protesto de um grupo nacionalista que deseja fazer do Brasil um país melhor. Tenha orgulho de ser brasileiro, ame o país, só assim poderemos evoluir!"

Também está crescendo o ataque que atinge o servidor DNS (Domain Name System), responsável por converter o endereço digitado pelo usuário para o endereço IP. Nesse caso, ao tentar acessar um site, a pessoa é redirecionada a um site falso, que pode conter vírus ou roubar informações do seu computador. Normalmente, o usuário tem dificuldade em reconhecer esse tipo de ataque.

"Estamos enfrentando uma mudança de paradigma. Antes, a principal preocupação da segurança era com identidade e acesso: aquela pessoa está tentando acessar algo a que ela tem acesso? Hoje, os incidentes relacionados com ataques distribuídos, que derrubam e indisponibilizam sites cresceram muito. As equipes que trabalham com segurança estão se mexendo para enfrentar essa nova realidade", conta Flávio Chagas.

Hacker e cracker são diferentes

Embora muitas vezes sejam usados como sinônimos, hacker e cracker são diferentes e é bom não confundir.

Hacker é a pessoa que utiliza seu conhecimento para testar os recursos de segurança de uma empresa. Ele também, muitas vezes, é o responsável por encontrar vulnerabilidades de sistemas e softwares. Há um movimento de hackers – conhecido como hacktivismo – que realizam ataques a sites como forma de protesto. Além de derrubarem esses sites, eles podem mudar sua página principal, deixando mensagens.

Os crackers são indivíduos que utilizam seu conhecimento para beneficio próprio. Eles invadem computadores e roubam informações confidenciais, por exemplo, para aplicar golpes na internet. “São os responsáveis pela maioria dos crimes virtuais divulgados que envolvem perdas financeiras ou de informações para a empresa invadida”, explica o superintendente de Redes da Prodemge, Evandro Araújo.

Entrevista com Edison Fontes

Divulgação

Mestre em Tecnologia, professor e consultor em segurança da informação. É autor de cinco livros sobre proteção da informação na organização, sendo o mais recente *Políticas e Normas para a Segurança da Informação*.

Há diferença no modo como os setores público e privado tratam a segurança da informação? Quais os principais erros que eles cometem nessa área?

Edison Fontes: Os segmentos com mais legislação sobre a proteção da informação são os que melhor possuem a segurança da informação. Exemplo, as instituições financeiras, sejam instituições públicas ou instituições privadas. Bancos públicos e bancos privados no Brasil, hoje, possuem uma excelente proteção de informação.

As demais organizações vão levando. E, nesse caso, entendo que o maior erro que as organizações cometem é o fato de que as ameaças e os riscos que afetam a informação e podem causar impactos financeiros, de imagem ou operacional, não são va-

lidados pelos acionistas (donos). Os acionistas são aqueles que têm o maior interesse na continuidade da organização e com certeza tomarão medidas mais adequadas à segurança da informação.

Quais os passos necessários para uma organização construir sua política de segurança da informação?

Edison Fontes: Primeiramente, a organização deve saber o seu grau de maturidade em segurança da informação. Depois, precisa priorizar suas ações nesse segmento. Nesse momento (provavelmente) ficará claro que a organização deve priorizar a definição e implantação das suas políticas e normas para a segurança da informação. A partir daí, a organização deve ter um recurso dedicado para o projeto de políticas e normas, seja para criação, seja para melhoria. É necessário apoiar a construção dos regulamentos em uma arquitetura. No meu recente livro, *Políticas e Normas para a Segurança da Informação*, eu defino uma arquitetura, indico mais detalhadamente os passos para a construção de políticas e, para exemplificar, apresento trinta exemplos de políticas. O projeto de elaboração de políticas deve ser encarado como um projeto como outro qualquer.

Existe um fator crítico de sucesso: a direção da organização precisa participar e definir a proteção que se deseja. Sempro digo que "toda organização tem a segurança que define". Outros fatores de sucesso são: existência de um profissional responsável (interno ou externo) pelo processo de segurança da informação, existência de cultura profissional na organização, definição de políticas e normas, treinamento e conscientização dos usuários, e agradável clima organizacional.

Como a segurança da informação se relaciona com as boas práticas de governança de TI, traduzidas pelos Objetivos de Controle de Informação e Tecnologia Relacionada (Cobit) ou pela Biblioteca de Infraestrutura para a Tecnologia da Informação (Itil)?

Edison Fontes: O Cobit trata de segurança assim como o Itil, mas com enfoque complementar. O Cobit tem como objetivo a governança e a gestão da TI. A Itil se preocupa com a entrega de serviços pela TI. Então, ambos consideram a segurança da informação de uma maneira complementar. A Norma ISO/IEC 27.002/2005 trata especificamente a segurança da informação. Seu objetivo é prover um grande roteiro de itens que devem ser considerados pela organização que deseja proteger adequadamente a suas informações.

Você acredita que a adoção do Cobit e da Itil pelas organizações, tanto públicas quanto privadas, está incentivando a adoção de políticas de segurança da informação? Ou o movimento é contrário?

Edison Fontes: O uso do Cobit e da Itil incentiva as organizações a terem seus processos de segurança da informação, principalmente o Cobit, que considera a segurança como um fator da governança ou na gestão de TI. A Itil também colabora muito quando ela exige gestão de mudanças, gestão de problemas, gestão de incidentes e similares. A existência dessas frentes facilita o processo de segurança da informação.

Qual a melhor forma de alinhar a segurança da informação com a segurança do negócio de uma empresa e a segurança do negócio de seus clientes?

Edison Fontes: Defendo que a área de segurança da informação deva obrigatoriamente ter um plano de ação para os próximos três anos. Esse plano deve ser validado com a alta direção ou com um comitê executivo. É bom lembrar que a segurança da informação é um processo organizacional que tem por objetivo garantir que a organização alcançará os seus objetivos de negócio no que depende da informação e dos recursos da informação. A segurança só existe porque o negócio existe primeiro e precisa ser protegido.

Consumerização é tendência

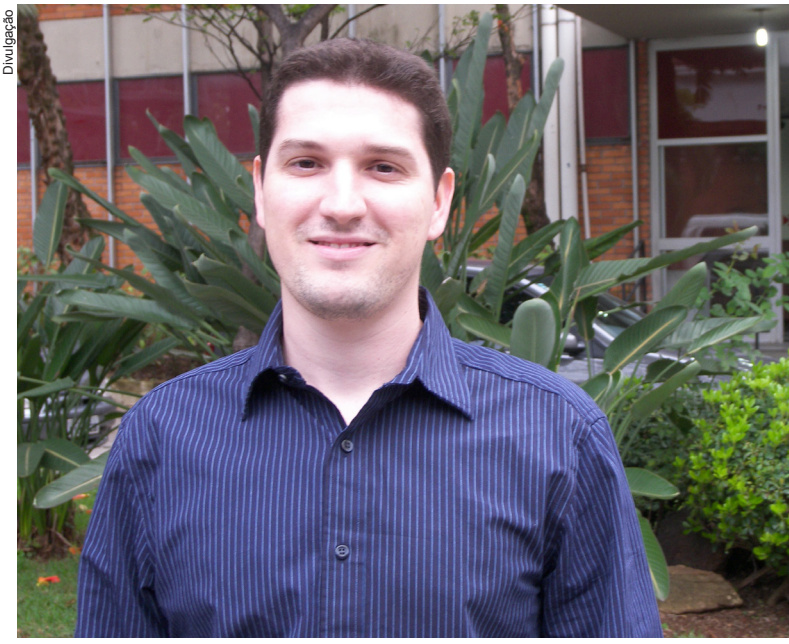
"O dispositivo móvel vai revolucionar o modo como se lida com a segurança da rede", afirma o gerente de Redes da Prodemge, Rafael Freitas. O desafio é resultado do aumento do número desses equipamentos que podem acessar a internet a qualquer momento de qualquer lugar com acesso à rede. Dados da E.life mostram que a quantidade de usuários que usaram celulares e/ou smartphones para navegar na internet subiu de 44,8% em 2011 para 56,2% em 2012. Via tablet, o acesso passou de 5,6% para 11,5%. Segundo o ministro das Comunicações, Paulo Bernardo, o ano de 2011 registrou mais de 40 milhões de novos assinantes de um plano de acesso móvel à internet.

Nesse cenário, um movimento crescente nas organizações é o Bring Your Own Device (BYOD), ou traga seu próprio dispositivo, em tradução livre. As empresas estão liberando os empregados a levarem seus smartphones, tablets ou notebooks para o ambiente corporativo, utilizando-os para trabalhar.

Mesmo as empresas que ainda não aderiram ao BYOD se deparam com funcionários utilizando seus equipamentos pessoais na rede corporativa, durante o horário de trabalho. Pesquisa realizada pela empresa Accenture com mais de quatro mil funcionários em 16 países mostra que quase 25% deles usam frequentemente seus dispositivos pessoais no ambiente de trabalho para cumprir suas tarefas. Há também aqueles que acessam aplicações não permitidas pela política de segurança para fazer realizar seu trabalho: quase 50% já fizeram isso pelo menos uma vez. A pesquisa também mostrou que esses números crescem significativamente no Brasil, China, Índia e México – os quatro países emergentes com maior crescimento que participaram do questionário.

Isso está trazendo uma nova demanda à área de TI: como tratar a segurança da informação e dos dados corporativos?

Divulgação



Rafael Freitas

A mobilidade exige do dispositivo que ele seja de fácil uso e pequeno. Pode-se dizer que ele é um minicomputador que possui os mesmos recursos que um PC, mas, por causa do tamanho, sem o mesmo poder de processamento ou capacidade de memória. "Os mecanismos e ferramentas de segurança para um smartphone, por exemplo, não são tão eficazes quanto os da máquina de uma estação de trabalho", explica Rafael.

Outro desafio é o controle: como identificar quem está acessando a rede, o que esse usuário está fazendo e como? Que tipo de informação está sendo recebida ou enviada? "Esse é um problema que atinge também os desktops, mas que foi potencializado nos dispositivos móveis, que permitem à pessoa ter a informação na palma da mão", analisa Rafael. Para enfrentar essa nova realidade, existem soluções técnicas como a VPN, a NAC e a Sandbox.

A tecnologia VPN (Virtual Private Network) cria um canal criptografado entre o dispositivo e a infraestrutura da rede corporativa. Ela já é utilizada

em estações de trabalho e pode ser adaptada para os dispositivos móveis. A NAC (Network Access Control) também é uma solução antiga que pode ser adaptada para ser utilizada em smartphones, tablets e PDAs. Segundo Rafael, ela autentica o usuário, identifica de onde é o acesso e permite o controle por perfil, além de verificar a saúde do dispositivo. A terceira solução é um aplicativo que usa o conceito de sandbox, virtualizando uma porção do sistema do dispositivo móvel.

Segundo Rafael, essas opções são técnicas que devem ser estudadas e estruturadas para a realidade da empresa. Além disso, é importante lembrar que toda ação operacional de segurança da informação deve estar alinhada com os normativos e a política de segurança da organização.

Questões trabalhistas

Além da segurança, as empresas devem ficar atentas às questões trabalhistas que podem surgir com o uso de dispositivos móveis pelos empregados. Sobreaviso e sobrejornada são os principais riscos, segundo a advogada Patrícia Peck Pinheiro, especialista em direito digital. "A sociedade digital trouxe um novo modelo de trabalho, em que a empresa não detém mais o monopólio da ferramenta de trabalho. Isso significa que a maioria das pessoas consegue realizar atividades tendo um celular e uma conexão de internet. Logo, o maior risco da mobilidade, no aspecto trabalhista, é a discussão sobre sobreaviso e sobrejornada", analisa.

Isso demanda das empresas que elas estabeleçam regras claras sobre esse assunto, assim como tenham controle sobre o uso desses equipamentos. De acordo com a lei 12.551/2011, "não se distingue entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado a distância, desde que estejam caracterizados os pressupostos da relação de emprego. Os meios telemáticos e informatizados de comando, controle e supervisão se equiparam, para fins de subordinação jurídica, aos meios pessoais e diretos de comando, controle e supervisão do trabalho alheio".

Essa mudança na Consolidação das Leis Trabalhistas equipara legalmente o trabalho realizado no ambiente físico da empresa e o que acontece remotamente, independentemente de quem pertença o dispositivo. Por isso, Patrícia afirma que a falta de normas e controles pode gerar, principalmente, questionamentos sobre hora extra: "É comum que pessoas que tenham acesso a dispositivos móveis acabem fazendo uso deles a qualquer horário e dia

Divulgação

Patrícia Peck

da semana, mesmo sem que isso tenha sido solicitado". E esses questionamentos acabam por aumentar o custo financeiro da empresa.

Para se proteger desses riscos, a advogada tem três recomendações: "A primeira medida é ter a regra clara – normas, políticas, contratos. Depois, tem que realizar campanhas educativas sobre o uso ético, seguro, saudável e legal das ferramentas tecnológicas. Por último, é importante monitorar".

Boas práticas de segurança para o usuário de um dispositivo móvel

- Instale um programa antivírus antes de instalar qualquer tipo de aplicação e mantenha-o sempre atualizado. Mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações.
- Evite modificar o sistema, o que pode tornar o aparelho mais vulnerável e sem proteções do fabricante. Instale apenas aplicativos (apps) confiáveis. Pesquise na internet antes de instalar e verifique as avaliações dos usuários. Aplicativos de redes sociais, principalmente os baseados em geolocalização, podem comprometer a sua privacidade.
- Tenha cuidado ao usar redes Wi-Fi públicas. Procure usar conexão segura sempre que a comunicação envolver dados confidenciais.
- Desligue o Bluetooth (ou outras interfaces de comunicação, como infravermelho e wi-fi) quando não estiver usando. Também é importante escolher bem a senha utilizada no Bluetooth e mudá-la com frequência; e configurar a conexão para que seu dispositivo não seja identificado por outros dispositivos.
- Bloqueie a tela com uma senha. Se possível, configure-o para aceitar senhas complexas.
- Mantenha as informações sensíveis em formato criptografado.
- Faça backups periódicos dos dados gravados. Há aplicativos que criam cópias de segurança automaticamente do smartphone para o computador ou para algum servidor na internet.
- Instale um app de controle a distância que você possa usar, por exemplo, para apagar seus dados, caso o aparelho seja roubado.
- Ao se desfazer do dispositivo móvel, apague todas as informações nele contidas e restaure as opções de fábrica.

Fonte: Cartilha de Segurança para Internet, do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Segurança dos dados pessoais e privacidade

O crescimento da internet não aumentou a preocupação e o cuidado dos usuários com suas senhas e dados pessoais. Os criminosos se aproveitam disso e enviam, por exemplo, e-mails maliciosos, que pedem ao usuário para alterar sua senha, muitas vezes alegando falha de segurança. O estudo Norton Cybercrime Report, divulgado anualmente pela empresa de segurança Symantec, apontou que 28 milhões de brasileiros foram vítimas de fraudes na internet, o que representa mais de 34% dos internautas no país. Os prejuízos chegaram a R$ 15,9 bilhões nos últimos 12 meses – uma média de R$ 562 por brasileiro.

Ameaças nas redes sociais também são comuns: 40% revelam terem sido vítimas nesse tipo de ferramenta e 23% já tiveram seu perfil invadindo, mostra o relatório. E a tendência é que os ataques virtuais passem a surgir nas redes sociais e nos celulares. Segundo a empresa de segurança NetQin, o número de vírus para celulares aumentou 155% em 2011. Somente no primeiro semestre de 2012, 13 milhões de smartphones foram invadidos.

Essa situação aponta para outro problema, que também está crescendo junto com a popularização das redes sociais: a vastidão de informações que as pessoas postam e compartilham nas redes sociais,

como fotos da viagem de férias, o vídeo do nascimento do filho, um comentário sobre o último filme a que assistiu.

Elas fazem parte de um novo tipo de usuário da rede, que surgiu com a evolução da web: gente que produz e compartilha seu próprio conteúdo. E elas são muitas. A empresa de pesquisa eMarketer afirmou que 2012 deve terminar com cerca de um quinto da população mundial cadastrado em alguma rede social.

Outra evolução tecnológica permite que elas permaneçam on-line cada vez mais tempo: os dispositivos móveis. Esses aparelhos permitem que a pessoa esteja presente no mundo virtual praticamente em qualquer lugar, a qualquer tempo. E, com isso, mais e mais informações são despejadas no mundo virtual.

A falta de cuidado para lidar com a sua segurança no mundo virtual se estende para o conteúdo daquilo que é colocado nas redes sociais. A preocupação com a privacidade parece diminuir à medida que elas expõem todo tipo de informação sobre sua vida para que amigos e amigos de amigos possam ver, curtir, compartilhar, comentar... Os usuários se esquecem de que dificilmente se elimina alguma informação que está na rede.

Além disso, o que é feito com essas informações? No primeiro semestre de 2012, a Google unificou a política de privacidade de mais de 60 de seus produtos, o que permite à empresa cruzar informações pessoais dos usuários e entregar a eles resultados personalizados. "Coletamos informações para fornecer serviços melhores a todos nossos usuários – desde descobrir coisas básicas, como o idioma que você fala, até coisas mais complexas, como os anúncios que você achará mais úteis ou as pessoas on-line que são mais importantes para você", afirma a empresa em sua política de privacidade (você pode ver o conteúdo completo em http://www.google.com.br/intl/pt-BR/policies/privacy/).

Boas práticas de segurança para o usuário de rede social

Considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa, tanto agora como futuramente.

Pense bem antes de divulgar algo, pois não há possibilidade de arrependimento. Após uma informação ou imagem se propagar, dificilmente ela poderá ser totalmente excluída.

Use as opções de privacidade oferecidas pelos sites e procure ser o mais restritivo possível.

Mantenha seu perfil e seus dados privados, permitindo o acesso somente a pessoas ou grupos específicos.

Procure restringir quem pode acessar seu endereço de e-mail.

Seja seletivo ao aceitar seus contatos, pois quanto maior for a sua rede, maior será o número de pessoas com acesso às suas informações.

Não acredite em tudo que você lê. Nunca repasse mensagens que possam gerar pânico ou afetar outras pessoas, sem antes verificar a veracidade da informação.

Seja cuidadoso ao se associar a comunidades e grupos, pois por meio deles muitas vezes é possível deduzir informações pessoais, como hábitos, rotina e classe social.

Seja cuidadoso ao fornecer a sua localização: observe o fundo de imagens; não divulgue planos de viagens e nem por quanto tempo ficará ausente da sua residência; procure se registrar (fazer check-in) em locais movimentados e quando sair do local, ao invés de quando chegar.

Proteja o seu perfil: seja cuidadoso ao usar e elaborar as suas senhas; habilite, quando disponível, as notificações de login; use sempre a opção de logout para não esquecer a sessão aberta; denuncie casos de abusos.

Proteja sua vida profissional: antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode atrapalhar um processo seletivo que você venha a participar; verifique se sua empresa possui um código de conduta e procure estar ciente dele; evite divulgar detalhes sobre o seu trabalho; preserve a imagem da sua empresa e, indiretamente, você mesmo; proteja seu emprego e use redes sociais ou círculos distintos para fins específicos.

Fonte: Cartilha de Segurança para Internet, do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

A medida provocou reações pelo mundo: os ministérios do Interior e Comunicações e da Economia, Comércio e Indústria do Japão notificaram a empresa de que as novas políticas devem respeitar as leis internas; a Comission Nationale de L'Informatique et des Libertés (autoridade francesa de proteção de dados), escolhida para liderar a posição das autoridades europeias de proteção de dados nesse tema, escreveu ao CEO da Google solicitando a suspensão da implementação da nova política unificada de privacidade; o Transatlantic Consumer Dialogue, em nome de mais de 50 entidades não governamentais de proteção à privacidade e do consumidor, fez o mesmo.

A Google não é a única empresa que enfrenta questionamentos sobre o modo como lida com as informações e a privacidade de seus usuários. Junto com Amazon, Apple, Microsoft, Research In Motion (fabricante do BlackBerry) e Hewlett-Packard, ela assinou um acordo com o estado da Califórnia (EUA), no começo de 2012, para informar com mais clareza quais dados pessoais são coletados por aplicativos para smartphones e tablets.

O acordo parece ter surtido algum efeito. A organização Future of Privacy Forum (FPF) divulgou em julho de 2012 uma pesquisa que revelou o aumento no número de aplicativos para dispositivos móveis desenvolvidos com políticas de privacidade para seus usuários. Os números mostram que os aplicativos grátis disponibilizados na plataforma iOS com algum tipo de política de privacidade chegaram a 84% em junho de 2012; valor que foi de 64% para os aplicativos pagos. Na plataforma Android, a percentagem foi de 76% para aplicativos grátis e 48% para os aplicativos pagos.

Outra grande empresa que está no centro das discussões sobre privacidade é o Facebook. A rede social criada por Mark Zuckerberg fatura em cima das informações de mais de um bilhão de usuários (no Brasil, são 36 milhões), vendendo espaço de anúncio publicitário a empresas interessadas. Segundo o jornal *O Estado de S. Paulo*, informações como e-mail, número de telefone e hábitos de navegação em outros sites da web estão disponíveis para que essas empresas direcionem suas ações de marketing. Além disso, uma equipe interna de pesquisadores estuda os dados armazenados nos servidores do Facebook e produz conhecimento sobre padrões de comportamento, comunicação e interação entre usuários.

Em entrevista à publicação *Tecnhology Review*, o coordenador dessa equipe, Cameron Marlow, afirmou que a pesquisa tem o objetivo de saber quais são as regras da vida social on-line e entender o que acontece no Facebook para adaptar a plataforma e oferecer às pessoas as experiências que elas desejam. Discurso similar ao da Google, mas que pode não convencer usuários que veem seus dados pessoais sendo explorados por essas empresas sem regras claras e públicas. Em um mundo cada vez mais conectado, no qual cerca de 20% da população faz parte de alguma rede social (segundo dados da empresa eMarketer), esse é um assunto polêmico que está sendo discutido por governos, empresas e sociedade civil.

Regulamentação

A privacidade e a proteção de dados pessoais na internet ainda não são regulamentadas no Brasil. Até o fechamento desta edição, o que existe são anteprojetos de lei, que foram construídos com a participação da sociedade, mas vêm trilhando lentamente o caminho para se tornarem leis.

O anteprojeto de lei nº 5.403/2011, conhecido como Marco Civil da Internet, estabelece direitos e responsabilidades dos internautas, provedores de conteúdo e poder público no Brasil. Sobre a privacidade, ele propõe que o usuário possa solicitar a exclusão definitiva dos seus dados de registros dos sites, garante o direito à inviolabilidade da intimidade e da vida privada, além de estabelecer que o sigilo das comunicações pela internet só pode ser quebrado mediante ordem judicial.

O texto está parado na Comissão Especial da Câmara dos Deputados, onde deve ser votado – até o fechamento desta edição, três sessões de votação já foram canceladas (nas duas primeiras, por falta

de quórum; na terceira, por orientação do Executivo, que temia a "desfiguração" do texto). Depois, seguirá para votação na própria Câmara ou em outra Comissão e só então entra na pauta do Senado, que também deve aprová-lo antes de ir para promulgação (ou veto) presidencial. Por isso, não há previsão de quando o Marco Civil entrará em vigor no país.

O Ministério da Justiça é responsável, junto com a Fundação Getúlio Vargas, pelo texto inicial de outro anteprojeto de lei que está sendo discutido no país e tem relação direta com o Marco Civil. Já chamado de Lei de Proteção de Dados Pessoais, tem como objetivo estabelecer um marco regulatório sobre o assunto, assegurando ao cidadão o controle e a titularidade sobre suas informações pessoais. O anteprojeto foi baseado em diversas leis internacionais em vigência, como, por exemplo, a Diretiva Europeia de Proteção de Dados Pessoais e a Lei de Proteção de Dados canadense. Assim como o Marco Civil, a consulta pública aconteceu pela internet, em um blog da plataforma Culturadigital. O debate terminou em abril de 2011, mas o projeto ainda não foi enviado ao Congresso.

Marco Civil – a constituição da internet

A importância do Marco Civil da Internet se estende para além da questão da privacidade. Seu objetivo principal é garantir direitos, observando os princípios de liberdade de expressão, privacidade do indivíduo, respeito aos direitos humanos e preservação da dinâmica da internet como espaço de colaboração. Por isso, é conhecido como a constituição da internet. "Faz sentido. Seu objetivo é traduzir os princípios constitucionais para a rede", afirma o professor do Centro de Tecnologia e Sociedade (CTS) da Escola de Direito da Fundação Getúlio Vargas, Ronaldo Lemos.

Se aprovado, prevalecerá na rede o direito à opinião. Conteúdo considerado infringente (como, por exemplo, calúnia ou difamação) só deverá ser retirado após decisão judicial. Provedores também não poderão ser responsabilizados civilmente por causa de publicação de internautas nem retirar da rede conteúdo que considerarem ofensivo.

Outro ponto do Marco Civil é a neutralidade da rede. O texto garante que a qualidade do acesso à internet tem que ser igual para todos, sem discriminação: "O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, conteúdo, serviço, terminal ou aplicativo, sendo vedado estabelecer qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos destinados a preservar a qualidade contratual do serviço" (artigo 12).

O assunto está causando polêmica. As empresas de telecomunicações argumentam que a nova regra vai exigir altos investimentos para modernizar a transmissão de dados e defendem um modelo que priorize o tráfego de dados dos sites que pagarem pelo acesso mais rápido. O governo é contra. Outra discussão é sobre quem regularia as exceções da neutralidade prevista em lei. O texto do anteprojeto estabelece o Comitê Gestor da Internet, composto por representantes do governo, do setor privado e da sociedade civil. Mas o governo e as empresas de telecomunicações preferem que a Agência Nacional de Telecomunicações (Anatel) seja a responsável por essa regulação.

O texto inicial do anteprojeto foi elaborado pela Secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com o CTS, e recebeu colaborações através de um portal desenvolvido especialmente para incentivar as contribuições e promover o debate entre usuários, academia, iniciativa privada, parlamentares e representantes do governo. Foram mais de duas mil contribuições diretas, que dão ao Marco Civil o título de primeira legislação elaborada colaborativamente no país. Segundo Ronaldo, ele está sendo considerado um dos textos mais avançados do mundo e recebeu menções positivas da ONU e do Parlamento Europeu. "Se aprovado, o país terá uma legislação abrangente e avançada, que protege as características mais importantes da internet e os direitos dos usuários", conclui.

Entrevista com Ronaldo Lemos
sobre o Marco Civil da Internet

Divulgação

Ronaldo Lemos é advogado, coordenador do Centro de Tecnologia e Sociedade (CTS) da Escola de Direito da Fundação Getúlio Vargas e professor visitante na Universidade de Oxford. Referência quando se fala em internet no Brasil, é fundador do projeto Overmundo e diretor do Creative Commons no Brasil, licença internacional para produtos com direitos autorais abertos. Foi nomeado em 2012 como membro do Conselho Nacional de Combate à Pirataria, coordenado pelo Ministério da Justiça, e do Conselho Nacional de Comunicação. Escreveu o livro *Direito, Tecnologia e Cultura.*

Qual o cenário do debate sobre regulamentação da rede no Brasil?

Ronaldo Lemos: O Brasil está atrasado na regulamentação da rede. Já se passaram mais de 15 anos desde que o acesso comercial à internet no Brasil começou a se disseminar e desde então ainda não estabelecemos um marco legal para o uso da rede no país. Essa ausência de lei, em vez de assegurar liberdade no uso da rede, está gerando distorções. Na ausência de lei, as decisões dos juízes estão sendo contraditórias. Há juízes que decidem em um sentido e outros em sentido exatamente contrário. Com isso, há uma incerteza jurídica. Isso é ruim para a inovação e para o desenvolvimento de novos serviços baseados na internet no país.

O Marco Civil da Internet, anteprojeto de lei em fase de votação na Câmara, tem o propósito de regular a internet. Quais serão as mudanças que a nova lei vai causar, quando aprovada?

Ronaldo Lemos: O Marco Civil vem sendo chamado de "A Constituição da Internet". Faz sentido. Seu objetivo é traduzir os princípios constitucionais para a rede. Seu principal efeito será estabelecer uma moldura legal para as decisões judiciais sobre a internet no Brasil, bem como consolidar princípios importantes, como a privacidade, a neutralidade da rede e os contornos da liberdade de expressão.

Quais os principais avanços que o texto atual do Marco Civil, se aprovado, vai trazer para usuários da internet?

Ronaldo Lemos: O avanço é significativo. O usuário da rede hoje é, ao mesmo tempo, consumidor e produtor de conteúdo. O Marco Civil reforça

essa posição e garante que usuários que produzem conteúdos não sejam responsabilizados com base em critérios pouco claros. Além disso, ele assegura a privacidade dos usuários, por exemplo, o direito de exigir a remoção dos seus dados de um determinado serviço da rede quando decidir parar de utilizá-lo. E mais importante: assegura a neutralidade da rede, que garante que a qualidade do serviço de acesso à internet seja igual para todos, evitando, por exemplo, que serviços como Skype ou o acesso a vídeos na internet possam ser bloqueados pelos fornecedores de acesso.

Comente sobre o direito de liberdade de expressão que o Marco Civil garante aos usuários.

Ronaldo Lemos: O Marco Civil traduz na prática os princípios constitucionais sobre liberdade de expressão. Ele diz que alguém só pode ser responsabilizado se for acionado judicionalmente e descumprir a ordem judicial. Isso estabelece um controle prévio pelo judiciário de quaisquer medidas que possam ser aplicadas pelo uso da rede. Vale lembrar que a situação de incerteza hoje gera inúmeros problemas. Por exemplo, quando um juiz em São Paulo mandou tirar do ar todo o YouTube por conta de um vídeo envolvendo a modelo Daniela Cicarelli. Com o Marco Civil essas decisões extremadas são evitadas.

Desde que o anteprojeto foi enviado ao Congresso, aconteceram alterações relevantes no texto? Quais as principais críticas que ele sofre?

Ronaldo Lemos: A principal alteração introduzida foi com relação à neutralidade da rede. O projeto original estabelecia a regra da neutralidade e outorgava à Anatel a responsabilidade de regular a questão. Na versão mais recente, foi incluída uma necessidade de consulta ao Comitê Gestor da Internet. Isso vem desagradando as teles, que gostariam de continuar lidando com o mesmo ente regulatório ao qual estão vinculadas, qual seja, a Anatel.

Qual é o estatuto do Marco Civil em relação a outras leis?

Ronaldo Lemos: O Marco Civil vem sendo considerado um dos textos mais avançados do mundo com relação às questões que regula. Foi mencionado positivamente na ONU, no Parlamento Europeu e em vários fóruns internacionais. Vale lembrar que o Brasil está chegando tarde à regulação da rede. Países como o Chile já adotaram sua regra sobre neutralidade da rede desde 2010. No entanto, a vantagem é que se o Marco Civil for aprovado, o país terá uma legislação abrangente e avançada, que protege as características mais importantes da internet e os direitos dos usuários.

A privacidade no Marco Civil da Internet

"O usuário de Internet tem direito à inviolabilidade e ao sigilo de suas comunicações, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (…) a informações claras e completas constantes dos contratos de prestação de serviços, estabelecendo o regime de proteção dos seus dados pessoais; (…) à não divulgação ou uso de seus registros de conexão e registros de acesso a serviços de internet, salvo mediante seu consentimento expresso ou em decorrência de determinação judicial." (artigo 7º, capítulo II)

"A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet."

"O exercício do direito à privacidade e à liberdade de expressão autoriza aos usuários de internet a livre opção por medidas de segurança direcionadas a salvaguardar a proteção de dados pessoais e o sigilo das comunicações." (artigo 8º, capítulo II)

Legado informacional

Organizações que utilizam a gestão documental para lidar com o seu legado informacional têm duas vertentes de atuação: uma é a digitalização, que converte o acervo dos documentos em formato analógico para a mídia digital; a segunda é a não geração de novos documentos em papel, criando-os diretamente no formato digital – caminho escolhido pelo governo mineiro e que está sendo implantado através do projeto Governo sem Papel (leia mais na página 27).

Aliando essas duas ações com a utilização de ferramentas de gestão de conteúdo (ECM, sigla para Enterprise Content Management), adaptadas segundo as especificidades de cada acervo e as necessidades da organização, ganha-se em produtividade e, principalmente, segurança. Sistemas de gestão garantem a acessibilidade, facilitando a busca e a tramitação de documentos, e a descentralização, ao permitir que pessoas em diferentes locais e estações de trabalho acessem o documento. Essa tecnologia também garante o controle de acesso, o versionamento de documentos e acompanha o ciclo de vida deles (que tem três fases: corrente, intermediária e permanente). A flexibilidade na indexação também possibilita a recuperação da informação de diversas formas.

Há também que se destacar outra forma de segurança, obtida pela hospedagem desses sistemas em um data center. "Esse tipo de ambiente é uma instalação profissional que trabalha com proteção física, controle de acesso, segurança da rede, redundância e níveis de serviço, o que garante a integridade dos dados e do legado informacional, e a disponibilidade das informações em qualquer momento", detalha o gerente de Conteúdo Digital da Prodemge, Nelson Spangler. A capacidade do data center é outro fator importante, pois aplicações de ECM demandam grande volume de armazenamento.

Entretanto, mesmo o suporte digital apresenta algumas fragilidades, que devem ser motivo de atenção dos dirigentes. "Tecnologias podem se tornar obsoletas e mídias ainda são frágeis. Entretanto, a evolução tecnológica caminha para formatos permanentes e padronizados, que facilitam o acesso e uso de arquivos em diferentes equipamentos e versões de softwares", explica.

Usuários também devem ter cuidado com a quantidade e a qualidade da informação produzida no mundo digital. Da mesma maneira que se gera lixo no mundo analógico, é possível gerar lixo digital. E-mails, por exemplo, são um novo tipo de documento, que não existia na sociedade do papel. "O que fazer com a quantidade de e-mails gerada atualmente? Devemos guardar? Jogar tudo fora?", questiona Nelson. Ele faz ainda um alerta: "Temos que pensar a produção, a gestão e o descarte de documentos digitais, para não trocar um problema que temos com o suporte papel por outro maior ainda."

Adoção gradual

Não existem números oficiais sobre a quantidade de papel guardada em acervos – para se ter uma ideia da ordem de grandeza que envolve essa situação, as estimativas são de que o governo mineiro produza anualmente 20 milhões de novas páginas. Cada organização, seja ela pública ou privada, tem um tipo de acervo, com suas peculiaridades, e cuida dele seguindo suas próprias regras. Ao se deparar com esse volume de documentos, é possível encontrar problemas como espaço inadequado e pouco seguro para guardar grande quantidade de papéis; número de funcionários insuficientes e, às vezes, mal preparados para lidar com o acervo; desconhecimento sobre o que de fato está guardado.

Esse cenário prejudica iniciativas de digitalização, que ainda são incipientes e pontuais no Brasil. São três as principais estratégias adotadas pelas organizações: a digitalização de todo o acervo, assim como da documentação corrente; a cessão da produção analógica de documentos e, posteriormente, a digitalização do acervo – o que está sendo feito no projeto Governo sem Papel; e a digitalização do acervo sob demanda.

Segundo o bibliotecário e analista de Gestão Documental da Prodemge, Sândalo Salgado, um dos principais problemas enfrentados é o alto custo necessário para se preparar os documentos que serão convertidos em formato digital. Como cada acervo é diferente e muitas vezes não há padronização nos tipos de documentos guardados, o tempo necessário para organizar todo o material é outro fator que desestimula a conversão.

Divulgação

Dirigentes também paralisam processos de digitalização quando é necessário reduzir o orçamento. "Projetos de digitalização ainda não são prioritários e por isso, em situação de crise financeira mundial e contenção de despesas, eles sofrem cortes ou são paralisados", conta Sândalo.

O analista explica que a adesão ao formato digital é um processo longo e cita exemplos positivos de organizações que já adotaram a nova cultura: "Os tribunais estaduais e federais já trabalham com processos eletrônicos, através do sistema Processo Judicial Eletrônico. Os bancos também aderiram à automatização. Cheques em papel, por exemplo, são eliminados em cinco dias, só restando a sua forma eletrônica. Há que se destacar também os órgãos certificadores de certificação digital".

Iniciativas como a lei 12.682, promulgada em 9 de julho de 2012 e que trata da elaboração e do arquivamento de documentos em meios eletromagnéticos, contribuem para a incorporação da digitalização. "Ela fortalece a certificação digital e o documento eletrônico", elogia Sândalo. A lei federal estabelece que o "processo de digitalização deverá ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)". Ainda segundo o texto, "os meios de armazenamento dos documentos digitais deverão protegê-los de acesso, uso, alteração, reprodução e destruição não autorizados".

A ressalva ao texto final da lei é que o descarte de documentos originais em papel e que foram digitalizados, antes deles cumprirem seu ciclo de vida, não é permitido: "Os registros públicos originais, ainda que digitalizados, deverão ser preservados de acordo com o disposto na legislação pertinente", estabelece o artigo 6º. Na prática, isso significa que documentos impressos e digitalizados ainda não tem o mesmo valor no país. Para Sândalo, "essa falta de clareza prejudica a adesão de órgãos públicos ao processo de conversão de documentos para a mídia digital".

Governo sem Papel

Desde 1º de setembro de 2012, as secretarias de Estado de Fazeda (SEF) e de Planejamento e Gestão (Seplag) de Minas Gerais não mais imprimem os documentos gerados durante a execução orçamentária e financeira (empenho, liquidação e ordem de pagamento). A medida vai ser ampliada para todos os órgãos do governo mineiro a partir de 1º de janeiro de 2013 e deve gerar uma economia de mais de R$ 200 mil por ano aos cofres públicos.

A ação faz parte do projeto Governo sem Papel, que busca diminuir a geração de papel nos processos administrativos do Estado, tornando-os eletrônicos. Além da redução de custos, essa nova forma de trabalho está liberando a atuação de servidores nas atividades-fim do órgão e trazendo mais segurança, pois os documentos são gerados e armazenados em sistemas. "O governo de Minas Gerais está empenhado em desburocratizar seus procedimentos internos, buscando uma maior eficiência da máquina pública, que reflita em benefícios na prestação do serviço. Para que a gente possa realmente gastar mais com o cidadão e menos com o governo", explica Milla Fernandes, gestora do projeto na Subsecretaria de Gestão da Estratégia Governamental da Seplag.

O projeto teve início com a execução orçamentária e financeira, porque esses documentos já eram gerados eletronicamente e recebiam assinatura digital no Sistema Integrado de Administração Financeira de Minas Gerais (Siafi-MG) desde 2007. Mesmo assim, eram impressos para auditoria do Tribunal de Contas do Estado de Minas Gerais (TCE-MG). Para mudar essa cultura, a Seplag buscou um entendimento conjunto com o Tribunal, que publicou uma diretriz interna orientando os auditores a não exigir impressão: a auditoria pode ser feita digitalmente, desde que os documentos tenham sido produzidos de forma eletrônica e assinados digitalmente.

Divulgação

Equipe que trabalha no projeto Governo sem Papel: Amanda Dias, Milla Fernandes e Robson Campos

Divulgação

Robson Campos em capacitação para auditores do Tribunal de Contas do Estado, quando eles aprenderam a consultar documentos de execução orçamentária e financeira no Siafi-MG

"O TCE-MG foi um grande parceiro. Ele também entende que precisa fazer um uso racional e sustentável dos recursos e lançou um projeto para evitar a geração de papel, o Controle sem Papel", conta Milla. Outro resultado dessa parceria foi uma capacitação para todos os auditores do Tribunal, com o apoio da equipe do Siafi-MG. Mais

de cem auditores aprenderam o passo-a-passo de como consultar os documentos da execução orçamentária e financeira no Sistema e um tutorial foi desenvolvido especificamente para esse fim.

Com a determinação de não imprimir, amparada por uma deliberação da Câmara de Coordenação Geral, Planejamento, Gestão e Finanças, o governo vai conseguir economizar 3,8 milhões de folhas por ano. Se forem consideradas apenas 3 folhas por processo, chega-se ao valor de R$ 200 mil por ano. "Mas tem processos com centenas de folhas", observa Robson Campos, coordenador de projetos da Subsecretaria de Gestão da Estratégia Governamental da Seplag.

Mas o benefício não se refere somente ao montante que se está deixando de imprimir e os valores gastos com essa ação. Há também custos associados, como o tempo. O antigo procedimento exigia do operador responsável pelo empenho bancário e pela liquidação que imprimisse, pegasse as folhas, as furasse, anexasse no processo, carimbasse, rubricasse... Atividades que, somadas, tomavam tempo de trabalho que não precisa mais acontecer.

A auditoria também será beneficiada, porque vai acontecer via sistema, já que o documento original está dentro dele. Isso permitirá que o auditor cruze informações – o que ele não conseguia fazer no processo em papel.

Os atos de aposentadoria – que em 2011 foram 8.652, impressos e assinados manualmente – são o segundo tipo de documentos que não mais será impresso, dentro do projeto Governo sem Papel. Para concretizar isso, a Companhia de Tecnologia da Informação de Minas Gerais (Prodemge) desenvolveu um workflow que permite que o ato seja gerado eletronicamente, receba a assinatura digital da secretária de Planejamento e Gestão e faça sua tramitação via sistema – incluindo a publicação pela Casa Civil e depois a auditoria do TCE-MG.

Uma das principais conquistas do projeto Governo sem Papel é a segurança. Sistemas eletrônicos são mais protegidos do que arquivos físicos e seus bancos de dados estão em servidores localizados em um data center protegido segundo normas internacionais. Além disso, eles diminuem a tramitação física do processo em papel, possibilitam um maior controle e evitam substituições indevidas e perdas de folhas. Esses sistemas também fornecem ao TCE-MG aquilo que ele precisa: informação segura e disponível a qualquer momento.

Divulgação

Documentos serão gerados e armazenados em sistemas, eliminando a necessidade de imprimir milhares de papéis.

Milla conta a próxima etapa do projeto: "A partir desse piloto, com a execução orçamentária e financeira e os atos de aposentadoria, queremos evoluir para outros documentos, identificando oportunidades de inclusão de assinatura digital e geração em sistemas, e, em parceira com o Tribunal de Contas, parar de exigir sua impressão. A tendência é evoluir para processos maiores e complexos".

O processo de compras, por exemplo, no qual a execução orçamentária e financeira está incluída, começa com a solicitação de compra por uma unidade demandante. A partir daí, o processo é instruído com justificativa, propostas comerciais, registro de preços; em seguida, acontece o registro no Portal de Compras do Estado da documentação do processo licitatório, edital, contrato assinado, documentação do fornecedor e notas fiscais. Segundo Milla, é uma geração de documentos enorme. Imprimi-se tudo que é considerado interessante ou relevante, o que acaba por tornar um processo de compra um calhamaço de papel.

O objetivo da Subsecretaria de Gestão da Estratégia Governamental é organizar todo esse processo eletronicamente. Por isso, está levantando quais são os documentos que precisam estar no processo de compra, em qual ordem e formato de arquivo eletrônico. Em paralelo a esse mapeamento, será implantada a assinatura digital. "Dessa maneira, será possível ter um sistema inteligente, com uma única opção de consulta, o que vai facilitar o trabalho do servidor ou do auditor. No futuro, eu vou entrar no sistema, colocar o número do processo e conseguirei ver todos os documentos pertinentes ao processo, desde o início até a execução", detalha Milla. E conclui: "É um desafio enorme. Mas significa redução de custos, otimização de trabalho, mais produtividade pro servidor e pro governo. E sobra mais dinheiro para investir em áreas como saúde, educação, transporte".

Programa Estruturador

O projeto Governo sem Papel faz parte do Programa Estruturador Descomplicar, do governo de Minas, que desde 2007 vem implantando ações de simplificação de procedimentos da administração pública, facilitando as relações do Estado com os cidadãos, as empresas e o próprio Estado.

Certificação Digital

Uma assinatura eletrônica que garante a autoria, a autenticidade, a privacidade, a integridade e o não repúdio de um documento eletrônico, dando validade jurídica a ele ou a qualquer outro processo ou transação que aconteça no mundo digital. Essa é a característica de um certificado digital, tecnologia baseada em criptografia assimétrica que imprime segurança e confiabilidade às informações que trafegam na rede.

No Brasil, a medida provisória 2.200-2/2001 implantou o sistema nacional de certificação digital e estabeleceu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). O Instituto Nacional de Tecnologia da Informação (ITI) é a primeira autoridade da cadeia de certificação e é responsável por auditar o sistema, além de cuidar da constante melhoria das suas normas e requisitos. Em 2012, por exemplo, entrou em vigor a segunda versão da ICP-Brasil, que aumentou os níveis de segurança e o algoritmo das chaves criptográficas de usuários para 2.048 bits. "A próxima evolução é a implantação de biometria nas autoridades de registro (AR), para garantir maior segurança no processo de identificação dos titulares de certificados. O piloto já está funcionando em São Paulo e no Rio de Janeiro; na Bahia está funcionando a primeira AR totalmente digital", conta a gerente de Operações de AR da Prodemge, Jacira Xavier.

O uso da certificação digital está consolidado nos setores público e privado. Empresas, governos e órgãos públicos aderiram à tecnologia por causa dos seus benefícios, como desburocratização e simplificação de processos, redução de custos, economia de papel, validade jurídica de transações virtuais, redução de fraudes e maior transparência. Os dois grandes alavancadores desse processo foram a Receita Federal, que oferece diversos serviços a pessoas físicas e jurídicas através da sua Central Virtual de Atendimento ao Contribuinte (e-CAC); e a Caixa Econômica Federal, cujo programa Conectividade ICP permite às empresas enviar e acessar os dados do FGTS.

Outras iniciativas importantes, enumera Jacira, são o Sped (escrituração das empresas enviadas ao fisco por meio de arquivos eletrônicos assinados com a certificado digital), a Nota Fiscal Eletrônica

de Serviços (em Belo Horizonte, por exemplo, desde 2009 é possível gerar a nota de serviço no site da Prefeitura ou através de aplicativo próprio) e o sistema judiciário (regulamentou o processo eletrônico e está implantando iniciativas de simplificação e redução de custos processuais). Na administração pública mineira, destacam-se projetos implantados tais como: Empenho Eletrônico do Siafi-MG (assinatura em lote dos empenhos pelos ordenadores de despesa do governo); Geicom (transferência eletrônica de recursos da Secretaria de Estado de Saúde de Minas Gerais a municípios e entidades utilizando certificação digital); os atos de aposentadoria (assinados e tramitados digitalmente via workflow e certificação digital); Governo sem Papel; e PCnet (solução web para gestão eletrônica e integração das informações da Secretaria de Estado de Defesa Social de Minas Gerais).

Segundo Jacira, a massificação da certificação digital para pessoas físicas deve acontecer com a implantação do Registro de Identidade Civil (RIC), a nova carteira de identidade, que trará os dados do cidadão (inclusive os biométricos) e sua identidade digital em um cartão com chip. “Esse cartão, que terá um número único no país inteiro, será a identidade eletrônica e a assinatura eletrônica da pessoa”, explica Jacira. De acordo com o governo federal, a substituição do RG atual pelo novo documento será feita de forma gradual, ao longo de nove anos (iniciados em 2011) e possibilitará a disponibilização de inúmeros serviços para o cidadão.

Gabriel Sales

“Nos últimos 11 anos, vários desafios foram superados para consolidar a tecnologia de certificação digital: a dificuldade das pessoas em utilizar a tecnologia; a mudança de cultura para diminuir a impressão de papel; a substituição do login e senha para a certificação; a desconfiança jurídica, vencida pelo amparo legal da ICP-Brasil”, conta Jacira. Para ela, o modelo da infraestrutura de chaves públicas brasileira é outro fator de sucesso. Por estabelecer padrões e requisitos, a ICP-Brasil facilita a interoperabilidade das aplicações que utilizam a certificação digital”, conta Jacira. Além disso, a capilaridade das autoridades de registro (ARs) no país contribui para a adesão ao certificado. A AR trabalha como interface entre o usuário e a Autoridade Certificadora. São mais de mil no território brasileiro. A estrutura conta ainda com dez autoridades certificadoras de 1° nível e 33 autoridades certificadoras de 2° nível.

ENTREVISTA

Divulgação

Renato Martini

Diretor-presidente do ITI

Após 11 anos, desde que foi editada a Medida Provisória 2.200, como você avalia a implantação da infraestrutura de chave pública brasileira e da certificação digital no país?

Renato Martini: São exatos 11 anos exitosos de operação do sistema nacional de certificação digital da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), que nos remetem para o grande desafio de disponibilizar ao cidadão não apenas o documento eletrônico, mas verdadeiros balcões on-line repletos de serviços que facilitam sua vida e a desburocratizam a partir do uso dos certificados digitais ICP-Brasil.

A implantação da ICP-Brasil é um sucesso. Inúmeras entidades, em especial as públicas, adotaram-na como ferramenta exclusiva de tecnologia. O sistema financeiro brasileiro com a compensação de cheques por imagem, a Receita Federal com a nota fiscal eletrônica e portal e-CAC e o Conectividade Social ICP, canal de comunicação entre as empresas que recolhem o FGTS e a Caixa Econômica Federal, são exemplo nítidos de como a certificação ICP-Brasil está presente na sociedade, convergindo em serviços ao cidadão e otimizando resultados nas gestões dessas entidades.

Quais benefícios a certificação digital trouxe para a administração pública e o cidadão?

Renato Martini: O certificado digital ICP-Brasil não é apenas um documento eletrônico de segurança. Ele é também um documento que confere validade jurídica a qualquer manifestação eletrônica assinada digitalmente e tramitada pela internet. Assim, seus benefícios para a administração pública incluem a celeridade do trâmite processual, a extensa economia de papel, de energia elétrica e

de outros insumos. Incluem-se também benefícios relacionados à disponibilidade dos arquivos, uma vez que eles estão digitalizados e podem ser acessados a qualquer momento com o certificado digital. O cidadão, que ainda não dispõe de muitas aplicações para o acesso a serviços, é beneficiado com a otimização dessas gestões do serviço público. Um processo judicial eletrônico, por exemplo, é julgado em muito menos tempo do que o em papel.

Como você avalia a adoção da certificação digital pelo cidadão comum? Pode-se considerar que ela já está popularizada? Por quê?

Renato Martini: Em 2012, a Receita Federal do Brasil tomou a decisão de exigir dos contribuintes que tiveram renda superior a R$ 10 milhões que seus impostos de renda fossem declarados com a utilização do certificado digital ICP-Brasil. A Receita oferece vantagens para o contribuinte que possui certificação digital. O Centro Virtual de Atendimento da Receita Federal (e-CAC) é prático e seguro. Qualquer procedimento pode ser acompanhado pelo contribuinte. A Receita, quando recebe qualquer demanda assinada com um certificado digital ICP-Brasil, tem certeza de que o contribuinte envia e recebe dados de maneira identificada. Esse é um exemplo de como a tecnologia poderá estar aplicada à vida prática das pessoas em um futuro não muito distante. A tecnologia está popularizada porque ela converge em serviços extremamente importantes no Brasil e alcança, diretamente, o cidadão brasileiro.

Você já afirmou em entrevista que a infraestrutura de chave pública brasileira é um criptossistema civil de uso da sociedade, daí a importância da confiança e da transparência. Fale mais sobre isso.

Renato Martini: A confiança e a transparência conquistadas ao longo dos anos de operação do Sistema Nacional de Certificação Digital no padrão da Infraestrutura de Chaves Públicas Brasileira são fatores determinantes para o êxito da certificação digital no país. Temos uma infraestrutura operada pelo Estado, com dez autoridades certificadoras de 1° nível e que é utilizada pela sociedade civil em aplicações bancárias, fiscais, trabalhistas e outras mais. Significa dizer que esse criptossistema civil de uso da sociedade está pronto para ser a plataforma de governo eletrônico na prestação de serviços, na concessão de benefícios sociais e na fiscalização do Estado como um todo.

Como a certificação digital contribui para a segurança da informação em um mundo hiperconectado como o atual, onde quase todas as informações estão em rede?

Renato Martini: Na prática, o certificado digital funciona como uma carteira de identidade virtual que permite a identificação segura do autor de uma mensagem ou transação feita nos meios virtuais, como a rede mundial de computadores – internet. Tecnicamente, o certificado é um documento eletrônico que, por meio de procedimentos lógicos e matemáticos, asseguraram a integridade das informações e a autoria das transações.

Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

ENTREVISTA

O que se está fazendo para que a tecnologia da certificação digital acompanhe as mudanças e a evolução de fraudes e ameaças virtuais? Como se dá a participação do Executivo e da sociedade civil nesse processo?

Renato Martini: Essa pergunta é muito pertinente. A certificação digital ICP-Brasil é regrada pela medida provisória 2.200-2 que institui a ICP-Brasil e o seu colegiado misto, o Comitê Gestor. Misto porque é composto por membros do governo e da sociedade civil que regularmente realizam reuniões para tratar dos assuntos de interesse dessa infraestrutura. Esse comitê permanente é cioso às mudanças tecnológicas e também às mudanças jurídicas ocorridas no Brasil. As discussões ocorridas nessas reuniões sempre são pautadas pela otimização tecnológica da ICP-Brasil, pelo combate às práticas fraudulentas e pelas possibilidades de inovações.

Uma das inovações é o projeto piloto de AR Biométrica, já implantado em Brasília. Funciona assim: o postulante é convidado a identificar-se mediante seus dados biométricos. Em seguida, ele apresenta seus documentos pessoais e suas impressões digitais são confrontadas com a base de dados do Instituto de Identificação da capital da República. Em segundos, é possível atestar que o portador daquela cédula de identidade é quem ele diz ser. O aproveitamento das consultas é de 97%.

Atualmente, para a emissão do certificado digital ICP-Brasil, o solicitante tem que ir à AR por ele escolhida para confirmar os dados informados durante a solicitação pela internet, devendo apresentar documentos pessoais, como a cédula de identidade, por exemplo. A ideia é que a AR Biométrica, além de verificar se os dados informados conferem com os que o requerente apresenta, realize a consulta aos dados biométricos do requerente que estão disponíveis no banco de dados do Instituto de Identificação.

Quais os próximos passos e desafios da certificação digital?

Renato Martini: Quando falamos de uma infraestrutura regida por normas e padrões tecnológicos internacionais associada à legislação brasileira, os desafios sempre serão enormes. Não temos dúvidas de que o certificado digital ICP-Brasil deva estar nas mãos das pessoas e nosso intuito é o de massificar, ao lado da sociedade civil organizada, a utilização da certificação ICP-Brasil. Sem dúvidas, nosso maior desafio é o de promover a inclusão digital brasileira através de nossa tecnologia ICP, de modo que os grandes serviços que hoje são realizados presencialmente possam, segura e legalmente, ser acessados pela internet.

O **Instituto Nacional de Tecnologia da Informação (ITI)**, criado em 2001, é a autarquia federal responsável por manter a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), seguindo as regras estabelecidas pelo Comitê Gestor da ICP-Brasil. No sistema nacional de certificação digital da ICP-Brasil, o ITI é a Autoridade Certificadora Raiz (AC-Raiz). É ele quem garante a autenticidade, a integridade e a validade jurídica de documentos eletrônicos, aplicações que utilizem certificados digitais ICP-Brasil, bem como a realização de transações eletrônicas seguras. Compete também ao ITI garantir a compatibilidade da ICP-Brasil e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

O ITI também atua na área de P&D, trabalhando para estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital. De acordo com o site da autarquia, “sua principal linha de ação é a popularização da certificação digital ICP-Brasil e a inclusão digital, atuando sobre questões como sistemas criptográficos, hardware compatíveis com padrões abertos e universais, convergência digital de mídias, desmaterialização de processos, entre outras”.

A Lei de Acesso a Informações e a segurança da informação

No dia 16 de maio de 2012, entrou em vigor no Brasil a lei nº 12.527, que regulamenta o direito constitucional de acesso dos cidadãos às informações públicas e vale para os três poderes, Executivo, Legislativo e Judiciário, e todos os níveis de governo, União, estados, Distrito Federal e municípios. O texto ficou conhecido como Lei de Acesso a Informações e estabelece os requisitos mínimos para a divulgação dessas informações e os procedimentos para facilitar e agilizar o seu acesso. O princípio da Lei é: o acesso e a publicidade são a regra e o sigilo, a exceção.

Apesar do que possa parecer à primeira vista, a segurança da informação e a Lei de Acesso a Informações estão em um "acordo de interesses", nas palavras do assessor da Secretaria de Estado de Planejamento e Gestão de Minas Gerais, Marcelo Veloso. Segundo ele, princípios de segurança definidos pela norma ISO 27.002, como preservação da integridade, autenticidade, confidencialidade e disponibilidade, estão presentes também na Lei, que determina a responsabilidade dos órgãos e entidades do poder público de proteger a informação, "garantindo-se sua disponibilidade, autenticidade e integridade"; e ainda prevê a existência de informação sigilosa ("aquela submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado"). Esse, explica Marcelo, é o conceito que a Lei usa para o termo confidencialidade.

O assessor acredita que a Lei fortalecerá a necessidade de implementar políticas, procedimentos e normas que garantam a segurança da informação e o seu pleno cumprimento. "Essa gestão é um desafio e também uma oportunidade que a nova regra proporciona aos órgãos e entidades públicos", diz. Para Marcelo, a (re)avaliação das informações classificadas como ultrassecretas e secretas no prazo de dois anos, estabelecidos pela Lei, é outro desafio, que vai demandar esforço do Estado, devido ao grande volume de informações produzidas – muitas, inclusive, que não são de interesse público.

Além disso, agentes públicos precisarão de treinamento sobre segurança da informação e como cumprir o que a Lei determina, já que ela os torna corresponsáveis pela perda de alguns dos princípios da segurança da informação, como integridade, disponibilidade e confidencialidade. O artigo 32 considera como condutas ilícitas "utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento"; e "divulgar ou permitir a

Divulgação

Marcelo Veloso ministrou palestra sobre segurança da informação e Lei de Acesso a Informações no Secop 2012.

divulgação ou acessar ou permitir o acesso indevido à informação sigilosa ou informação pessoal".

Marcelo cita ainda o que ele considera um desafio e a maior oportunidade trazida pela Lei: o estabelecimento de sistemas de gestão da segurança da informação. "A administração pública ainda é muito carente desse tipo de sistema estabelecido e formalizado, atuando de forma efetiva para garantir os princípios da segurança da informação", conclui.

Transparência e dados abertos

O acesso à informação pública, segundo determina a Lei, pode acontecer de duas formas: solicitação direta do cidadão ao órgão ou publicação de dados e informações na internet (chamada de transparência ativa). Segundo consta no texto, os sítios utilizados para disponibilizar os dados devem permitir o acesso "de forma objetiva, transparente, clara e em linguagem de fácil compreensão"; além disso, deve "possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários; (...) o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina; (...) e garantir a autenticidade e a integridade das informações disponíveis para acesso."

Essa ideia, contida no texto da Lei de Acesso a Informações, é a dos dados abertos governamentais. Segundo a organização sem fins lucrativos Open Knowledge Foundation (Fundação do Conhecimento Aberto, em tradução livre), um dado é considerado aberto quando qualquer pessoa pode livremente usá-lo, reutilizá-lo e redistribui-lo, estando sujeito, no máximo, à exigência de creditar a sua autoria e compartilhar pela mesma licença.

Outros princípios também definem um dado aberto: disponibilização de todo dado que não for considerado sigiloso, para a maior quantidade possível de pessoas, sem necessidade de cadastramento ou identificação; apresentação atualizada do dado tal como ele foi gerado ou coletado e de modo que possa ser processado automaticamente; livre de controle por alguma entidade ou organização e não submetido a copyrights, patentes, marcas registradas ou regulações de segredo industrial. Seguindo essas características, os formatos e recursos mais usados para disponibilizar um dado aberto são CSV, XML, RDF, JSON. Além disso, eles devem ser publicados em sítios na internet.

Quando um dado é realmente aberto, ele propicia a interoperabilidade. Isso significa que pessoas e organizações podem fazer diferentes conjuntos de dados "conversarem", construindo sistemas, produtos e serviços. Além de aplicações desenvolvidas colaborativamente, os dados abertos governamentais aumentam a transparência e a maior participação política do cidadão, trazendo melhorias para a sociedade e para o governo. Na opinião do gerente do Escritório Brasil do Consórcio World Wide Web (W3C), Vagner Diniz, os benefícios mais relevantes do uso de dados abertos são aqueles resultantes da possibilidade de reutilização dos dados disponíveis para produção de novos serviços ou de geração de outras visões, que não as governamentais, sobre o mesmo conjunto de dados.

Ele cita também outros "subprodutos" da utilização de dados abertos: "Melhoria da inclusão digital, porque formatos abertos são mais fáceis de ser reconhecidos por dispositivos especiais de navegação na web para pessoas com deficiência; o intercâmbio de base de dados entre órgãos da mesma administração sem burocracia, e a fácil integração com dispositivos móveis como celular".

O importante é não confundir dados abertos com a abertura indiscriminada das bases de dados utilizadas na gestão pública, o que poderia apresentar riscos à segurança e ameaça à privacidade exigida por determinados tipos de dados. Essa situação é considerada pela Lei de Acesso a Informações: da mesma forma que fala da publicidade, ela afirma que cabe ao órgão público proteger as informações consideradas sigilosas – dados pessoais e aquelas imprescindíveis à segurança da sociedade ou do

Estado – contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados. São exemplos de informações sigilosas assuntos secretos do Estado, temas que possam colocar em risco a segurança nacional ou que comprometam atividades de investigação policial, dados de casos que corram em segredo de justiça e informações pessoais dos agentes públicos ou privados.

"A Lei de Acesso à Informação é bem clara quanto aos procedimentos necessários para se classificar informações públicas como sigilosas. Essa classificação não pode ser arbitrária e discricionária", explica Vagner. Além disso, quando o sigilo for a causa de uma negação ao acesso a determinada informação, ele deve ser justificado. Mesmo assim, a orientação da Controladoria-Geral da União – última instância recursiva no nível federal para casos de negativas – é que o acesso à informação seja liberado, cobrindo-se as partes que afetam a privacidade ou a segurança. "Dados abertos não são incompatíveis com privacidade e sigilo", afirma Vagner.

A Lei também determina prazos para a restrição ao acesso das informações sigilosas. Se elas forem consideradas reservadas, o prazo é de cinco anos; se secretas, de 15 anos; e se ultrassecretas, o limite é 25 anos. A classificação deve levar em conta o interesse público da informação, utilizando o "critério menos restritivo possível".

Compromisso federal

O governo aberto é um compromisso do governo federal brasileiro, que, em setembro de 2011, firmou a Open Government Partnership (OGP), ou Parceria para Governo Aberto, com África do Sul, EUA, Filipinas, Indonésia, México, Noruega e Reino Unido. Na mesma data, foi publicado o decreto que instituiu a Infraestrutura Nacional de Dados Abertos (Inda).

A Inda é a política nacional de dados abertos, criada para "garantir e facilitar o acesso pelos cidadãos, pela sociedade e, em especial, pelas diversas instâncias do setor público aos dados e informações produzidas ou custodiadas pelo poder executivo federal". Segundo o Portal Brasileiro de Dados Abertos (http://dados.gov.br), que centraliza a busca e o acesso dos dados e informações públicas disponibilizados pelos diversos órgãos, a Inda determina os "padrões, tecnologias, procedimentos e mecanismos de controle necessários para atender às condições de disseminação e compartilhamento de dados e informações públicas no modelo de dados abertos".

Vagner Diniz cita ainda outras iniciativas brasileiras do uso de dados abertos: "Os governos do Estado de Pernambuco (http://dados.pe.gov.br) e do Estado do Rio Grande do Sul (http://www.acessoainformacao.rs.gov.br/) também saíram na frente com os seus portais de dados abertos. Muito interessante e pioneiro é o trabalho do Tribunal de Contas dos Municípios do Estado do Ceará (http://www.tcm.ce.gov.br)". Em Minas Gerais, há ainda o trabalho que está sendo realizado pela Assembleia Legislativa de Minas Gerais (http://dadosabertos.almg.gov.br/ws/ajuda/sobre).

No mundo, os países pioneiros no tema de dados abertos são o Reino Unido (http://data.gov.uk/) e os Estados Unidos (http://www.data.gov/). Eles já avançaram muito no assunto e, segundo Vagner, publicam seus dados em formato aberto de maneira consistente, rápida e sustentável. Ele destaca ainda as iniciativas da Austrália (http://data.gov.au/), Nova Zelândia (http://data.govt.nz/), Finlândia (http://www.julkinendata.fi/) e de algumas regiões da Espanha. Para os governos interessados em publicar seus dados abertos, Vagner dá um recado: "Antes de dar o primeiro passo, é da maior importância se ter a firme convicção de que publicar dados abertos é um ato de respeito ao cidadão, pelo direito que ele tem de ter acesso às informações. Mais do que uma atitude volitiva de transparência, é uma ato de garantia de direitos. Da convicção germina-se a vontade política da abertura dos dados, sem a qual nenhum passo será consistente, sustentável e permanente".

Os primeiros meses da Lei de Acesso a Informações

O governo federal faz um balanço positivo dos primeiros meses de vigência da Lei de Acesso a Informações. Nesse período, quase 90% dos pedidos recebidos pela Controladoria-Geral da União – órgão que centraliza o acompanhamento dessas demandas por meio do Sistema Eletrônico do Serviço de Informações ao Cidadão (e-SIC) – foram respondidos. O Sistema também indica que o tempo médio de resposta dos órgãos é de dez dias, sendo que a Lei prevê 20 dias. Os cinco órgãos que receberam o maior número de solicitações são: Superintendência de Seguros Privados, 3.124 (11%); INSS, 2.048 (7,2%); Banco Central, 1.201 (4,2%); Caixa Econômica Federal, 1.050 (3,7%); e Empresa Brasileira de Correios e Telégrafos, 923 (3,21%). Os dados são do dia 28 de agosto de 2012.

Margareth Travessoni

No governo mineiro, as secretarias estaduais de Saúde, Educação e Planejamento e Gestão foram as que mais receberam demandas por informações (cerca de 800 no total, desde a implantação da Lei – dados de outubro de 2012). Segundo a Controladoria-Geral do Estado, após o crescimento registrado nos primeiros meses de vigor da Lei, a média de pedidos semanais recebidos através dos canais disponibilizados (Unidades de Atendimento Integrado, LigMinas e Portal da Transparência) está estabilizada. O acesso ao Portal (sítio por onde é feita também a transparência ativa) é grande e fatos como a divulgação de salários aumenta ainda mais a procura por esse canal.

Para Vagner Diniz, os números são animadores e mostram como alguns governos têm respondido bem às demandas de acesso a informações. "A população e as organizações, particularmente a mídia, têm testado e experimentado se a Lei veio de fato para ficar. O nível de resposta é bastante satisfatório". Ele espera que essa situação chegue também ao nível da gestão municipal: "Ainda temos um caminho a trilhar. Compreender o significado e importância da Lei, preparar-se para o atendimento ao cidadão e organizar as informações para que elas se tornem disponíveis são desafios que ainda se colocam para governos e sociedade."

Para a subcontroladora da Informação Institucional e da Transparência de Minas Gerais, Margareth Travessoni, implantar a Lei de Acesso a Informações está sendo desafiador e instigante: "O governo mineiro já tinha uma política de transparência. O que fizemos foi melhorar a estrutura já existente e prepará-la para o aumento da demanda. Também nos preocupamos com a qualificação dos servidores e, para isso, realizamos capacitações para servidores antes e depois da Lei entrar em vigor". A Controladoria-Geral do Estado está concluindo o levantamento de todas as informações produzidas pelo governo e se prepara para conduzir sua classificação em 2013, determinando quais deverão receber o título de reservada, secreta e ultrassecreta, seguindo os critérios estabelecidos pela Lei.

Margareth ressalta o valor do controle social que a nova legislação permite ao cidadão. Para ela, a sociedade fica mais atenta e se conscientiza para a cultura da transparência na administração pública. "A Lei, inclusive, foi tema de uma das propostas finais da 1ª Conferência Nacional sobre Transparência e Controle Social, realizada em Brasília em maio de 2012. Os delegados entenderam que ela deve ser aplicada com severidade, rigor e eficácia como forma de combater a corrupção e melhorar a gestão pública", conta.

Como obter uma informação pública

"Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado". (artigo 5º da Constituição Federal).

Todas as informações produzidas ou custodiadas pelo poder público e não classificadas como sigilosas são consideradas públicas.

A solicitação de informação na esfera federal pode ser feita pelo Serviço de Informações ao Cidadão (SIC) do órgão ou através do site http://www.acessoainformacao.gov.br. Em Minas Gerais, nas Unidades de Atendimento Integrado (UAIs), pelo LigMinas (telefone 155) e através do Portal da Transparência (http://www.transparencia.mg.gov.br).

Não é preciso justificar o pedido.

O órgão público tem um prazo de 20 dias para fornecer os dados solicitados, prorrogável por mais 10 dias.

Glossário

Bot – tipo de código malicioso que, além de incluir funcionalidades de worms, dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. É capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

Botnet – rede formada por centenas ou milhares de computadores infectados com bots. Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam etc.

Cavalo-de-Troia – programa malicioso que finge ser benigno. Além das funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.

Consumerização – uso de dispositivos móveis pessoais no ambiente de trabalho.

Core – núcleo de processamento do processador.

Cracker – pessoa que tem conhecimento em informática e a utiliza para quebrar sistemas de segurança, de forma ilegal ou sem ética, para furtar informações sigilosas, em proveito próprio ou de outro.

BYOD – sigla para Bring Your Own Device. Movimento no qual as empresas liberam os empregados a levar seus dispositivos móveis pessoais para o ambiente corporativo, utilizando-os para trabalhar.

DDoS – sigla para Distributed

Denial-of-Service, que significa negação de serviço distribuído. É um tipo de ataque que realiza múltiplos acessos simultâneos a um site, excedendo os limites do servidor. Pode causar o travamento total do sistema.

Defacement – ataque que modifica a página de um sítio na internet.

DoS – sigla para Denial-of-Service, que significa negação de serviço. É um tipo de ataque que tornar os recursos de um sistema indisponíveis para seus usuários.

Firewall – dispositivo de uma rede de computadores, cujo objetivo é aplicar uma política de segurança a um determinado ponto da rede.

Flame – programa mais devastador que captura dados, altera configurações de computadores remotamente, liga microfones para gravar conversas, faz capturas de tela e registra trocas de mensagens sem ser percebido pelo usuário da máquina.

Guru – pessoa considerada o mestre dos hackers, tem grande domínio sobre diversos tipos de sistemas.

Hijacker – programa ou script que "sequestra" navegadores de internet. As principais vítimas eram as versões mais antigas do Internet Explorer. Um hijacker pode, por exemplo, alterar a página inicial do browser e impedir o usuário de mudá-la, exibir propagandas em janelas novas, instalar barras de ferramentas e impedir o acesso a determinados sites (páginas de empresas de antivírus, por exemplo). Os navegadores atuais contam com mais recursos de segurança, limitando consideravelmente a ação desse tipo de praga digital.

IPS – sigla em inglês para Sistema de Prevenção de Intrusos. É visto como uma extensão do firewall, pois possibilita decisões de acesso baseadas no conteúdo da aplicação.

Keylogger – pequeno aplicativo que pode vir embutido em vírus, spywares ou softwares de procedência duvidosa. Sua função é capturar tudo o que é digitado pelo usuário. É uma das formas utilizadas para a captura de senhas.

Lammer – pessoa que possui algum conhecimento de informática e quer se tornar um hacker. Iniciante, invade e perturba os sites.

Malware – do inglês malicious software. Nome usado de forma genérica para se referir a códigos ou programas maliciosos.

Oracker – pessoa que acha que sabe, mas não sabe. É considerado um "hacker de araque".

Phishing – tentativa de enganar o usuário para obter suas informações pessoais e financeiras.

Preaker – pessoa que burla os meios de comunicação telefônica para uso próprio, sem o pagamento devido, e instala escutas para facilitar o acesso externo, visando ao ataque a sistemas.

Rootkit – programa malicioso que pode ser utilizado para várias finalidades. O que torna um rootkit ameaçador é a capacidade para dificultar sua detecção por antivírus ou outros softwares de segurança, pois consegue se "camuflar" no sistema. Para isso, desenvolvedores de rootkits podem fazer uso de várias técnicas avançadas, como infiltrar o malware em processos ativos na memória. O rootkit também é de difícil remoção. Pela sua complexidade de desenvolvimento, não é muito numeroso.

SOC – sigla em inglês para Centro de Operações de Segurança.

Spyware – programa malicioso que espiona, coleta e rouba informações pessoais do usuário e as envia pela internet.

Vírus – programa ou código que se dissemina por outras máquinas e provoca efeito prejudicial no computador.

Worm – tipo de vírus mais inteligente que os demais. Pode se espalhar rapidamente para outros computadores – pela internet ou por meio de uma rede local – de maneira automática.

Em uma guerra totalmente científica, contam-se cérebros e não ogivas

Divulgação

Marcelo Bezerra*

Informações confidenciais roubadas dos computadores de engenheiros nucleares por um vírus. Centrífugas nucleares inoperantes ou seriamente afetadas, também por um vírus, este especialmente desenvolvido para tal. Um avião robô desviado pelo inimigo após sua comunicação com a base ser interceptada. Essas poderiam ser cenas de um roteiro de cinema. Mas, como sabemos, aconteceram de verdade e são os exemplos mais recentes do que se convencionou chamar de guerra cibernética. Apesar das opiniões contrárias, não se pode negar que a guerra cibernética já é uma realidade, como atestam os vários centros de defesa cibernética estruturados em vários países, entre eles o Brasil.

Mas não podemos imaginá-la como nos filmes e é bastante improvável que no futuro ocorra uma guerra puramente cibernética. Assim como outras modalidades de guerra, como a química, a biológica e a nuclear, ela se insere dentro de um cenário estratégico maior. A mais famosa definição foi dada por um conselheiro do governo dos Estados Unidos, Richard A. Clarke, autor de um best-seller sobre o tema (Cyber War), publicado em 2010. Ele define guerra cibernética como as ações patrocinadas por um Estado nacional para penetrar em redes ou computadores de outras nações com objetivo de causar dano ou sabotagem. Trata-se, portanto, da expansão dos ataques digitais de hackers e do crime digital a que já estamos acostumados, porém com alvo determinado e criados ou patrocinados por países ou organizações para fins de ataque ou defesa, como parte de uma operação militar em uma guerra deflagrada ou fria.

Sua origem vem do próprio desenvolvimento tecnológico da sociedade. Sistemas computacionais existem hoje na maioria dos equipamentos que usamos em nosso dia a dia. A nova geração de TVs (smart TVs) são na realidade computadores, apenas diferentes fisicamente. Quase tudo o que faz parte de nossa vida leva hoje circuitos eletrônicos e são programáveis. Os serviços que usamos, como bancos e hospitais, funcionam com base em redes de computadores, assim como as maiores indústrias do planeta. Nos Estados Unidos, toda a rede de distribuição de energia está também informatizada. Por definição, todos os sistema e redes de computadores possuem brechas de segurança que podem ser exploradas e, assim, temos o ambiente ideal para um ataque direcionado. Em um mundo estruturado sobre a tecnologia da informação, é óbvio que nações busquem meios de atacar seus inimigos também nessa área.

Da mesma forma, as organizações militares usam pesadamente sistemas informatizados, seja para comunicações, controle de posicionamento de unidades ou como o coração de mísseis e outras armas. Hoje, aviões não tripulados são equipamentos comuns em vários países e em breve o serão no

Brasil, onde há ao menos seis diferentes projetos de empresas brasileiras, associadas ou não a estrangeiros. Um vídeo disponibilizado no You Tube em setembro de 2012 mostrava os testes de um robô "mais rápido que o campeão olímpico Usain Bolt". De acordo com a notícia, era um projeto militar para perseguição de inimigos. E uma das maneiras de se combater a guerra tecnológica é com tecnologia, como bem mostrado pelo Irã ao interceptar o avião robô norte-americano.

Quando conversamos sobre guerra, é necessário falar das armas, e elas, nesse caso, são bem diferentes das tradicionais e das químicas, biológicas e nucleares. A tecnologia empregada na guerra cibernética possui características únicas e até quebra alguns paradigmas. Diferente das armas tradicionais, uma arma cibernética não possui potencial destrutivo. O seu impacto irá depender do sistema atacado e não dela propriamente. Imaginem um programa de ataque capaz de invadir um computador permitindo que esse seja controlado remotamente. Qual o efeito? Se for o de nossas casas, iremos perder algumas centenas de fotos. Mas e se for o computador que controla a operação de uma indústria? E se for uma central nuclear? O efeito de um ataque cibernético é também desconhecido até que ele ocorra, e mesmo assim é possível que a vítima consiga acobertar parte dos impactos. Desse ponto de vista, parece uma arma pouco eficaz, no entanto aí temos o que faz dela algo tão atrativo. Ela é totalmente fria. Não há explosões ou mortes aparentes. Não há cenas emotivas ou soldados mortos. Ela é invisível e pode penetrar em bunkers totalmente a prova de ataques, até mesmo nucleares, em um simples pen drive de um funcionário desatencioso. E, muito importante, pode ser facilmente negada. Dificilmente uma nação poderá retaliar baseada unicamente em um ataque a seus sistemas de computador, já que ataques bem-feitos dificilmente são rastreáveis. Como retaliar se não há certeza absoluta?

"EM UM MUNDO estruturado sobre a tecnologia da informação, é óbvio que nações busquem meios de atacar seus inimigos também nessa área."

Armas cibernéticas também não são estocáveis. Em uma guerra tradicional, leva clara vantagem o adversário que possui maior quantidade de armas e maior poder de destruição. Na guerra cibernética, não há quantidade de armas e, como já comentado, seu potencial de destruição depende do seu alvo. Um arsenal cibernético é também diferente, pois é composto de técnicas e conhecimento. As técnicas são as vulnerabilidades existentes em sistemas e os programas de invasão capazes de explorá-las. Quanto mais desconhecidas, mais valor têm essas vulnerabilidades, chamadas de dia zero. Os programas são geralmente porções de códigos de programação intercambiáveis que podem ser usados em diferentes situações para explorar vulnerabilidades. Há também programas específicos para evadir sistemas de defesa digital, como firewalls. Essas diferentes porções de código são então combinadas em kits de ataque, sistemas de invasão complexos como o Stuxnet, que atacou as centrífugas nucleares iranianas. Para tudo isso, vulnerabilidades dia zero, programas e kits, há a necessidade do conhecimento de especialistas e gênios da computação, os hackers. Esse patrimônio intelectual é a base do "estoque" da guerra cibernética. Sem ele não há ataque nem defesa. Em uma guerra totalmente científica, contam-se cérebros e não ogivas.

***Marcelo Bezerra**

Especialista em segurança de TI com ênfase na proteção de redes, área em que atua há mais de 15 anos. Gerente de Pré-Vendas da Crossbeam Systems para a América Latina. Atuou como diretor técnico da IBM Internet Security Systems também para a América Latina. É colunista da revista *RTI* e palestrante internacional com apresentações realizadas na Argentina, Chile, Colômbia e México, além de alguns dos principais eventos de segurança no Brasil. Mantém também o blog Segurança Digital (segdigital.blogspot.com.br).

Gestão da Segurança de Dados: um processo de gestão de dados do framework DAMA-DMBok®

Divulgação

Fernanda Farinelli*

Parece um clichê, mas quando o assunto é informação vêm à tona as considerações de Drucker (1993) a respeito de essa ser um dos maiores produtores de riqueza da sociedade atual. Em conformidade com Davenport (1998), ele debate que informação são dados dotados de relevância e propósito, selecionados e agrupados seguindo um critério lógico para alcançar um objetivo. Os dados representam um conjunto de fatos distintos sobre eventos do mundo. Enfim, Tom Peters (2001), citado por DMBok (2009, p. 1), contribui para essa análise, afirmando que "as organizações que não entenderem a enorme importância da gestão de dados e informações como ativos tangíveis na nova economia não sobreviverão".

Ao reconhecer seus dados como recurso valioso, as organizações também reconhecem que esses ativos devem ser gerenciados. Segundo o DMBok (2009), o dado, como qualquer outro ativo, possui um ciclo de vida, em que é criado ou adquirido, armazenado, utilizado e destruído. Dessa forma, realizar a gestão de dados é, na verdade, gerenciar o ciclo de vida dos dados. A Data Management Association (Dama) é a principal organização mundial que trata do assunto gestão de dados e propôs o Dama-DMBok (Guide to the Data Management Body of Knowledge) para ser referência a essa função.

Conforme o DMBok (2009), gestão de dados visa a controlar e a alavancar eficazmente o uso dos ativos dados e sua missão e objetivos são atender e exceder às necessidades de informação de todos os interessados da empresa em termos de disponibilidade, segurança e qualidade. É uma responsabilidade tanto da tecnologia da informação de uma empresa quanto de seus clientes internos e externos e envolve desde a alta direção, que utiliza dados na geração de informações estratégicas, até profissionais de nível operacional, que muitas vezes são responsáveis pela coleta e produção dos dados.

O DMBok estabelece um consenso para os processos de gestão de dados, identificando os princípios que a orientam e apresentando uma visão das práticas aceitas, métodos e técnicas que podem ser adotados por uma empresa que deseja gerenciar seus dados, além de servir aos leitores como fonte para um maior entendimento da gestão de dados. O guia está estruturado em dez grupos de interesses descritos por processos e suas atividades: governança de dados; gestão da arquitetura de dados; desenvolvimento de dados; gestão de operações com dados; gestão da segurança de dados; gestão de dados mestre; gestão de data warehousing & business intelligence; gestão de conteúdo e documentação; gestão de meta-dados; e gestão da qualidade de dados.

O foco principal deste artigo é apresentar o processo de Gestão da Segurança de Dados (GSD), que é "o planejamento, desenvolvimento e execução de políticas e procedimentos de segurança para

proporcionar a devida autenticação, autorização, acesso e auditoria nos ativos de dados e informações" (DMBOK, 2009, p. 151).

O objetivo desse processo é proteger os ativos de informação da organização em conformidade com os requisitos de acesso e alteração dos ativos de dados previstos pelo negócio, e as necessidades de privacidade e confidencialidade das partes interessadas e impostas pelos órgãos regulatórios. Entendem-se como requisitos de segurança de dados a autenticação de usuários, controles de autorização e acesso, e auditoria (DMBOK, 2009, p. 151-152).

Para atingir tais objetivos, o DMBok (2009) sugere nove atividades e uma lista de produtos produzidos por essas atividades, destacadas no Quadro 1. Em complemento, o framework recomenda os papéis envolvidos no processo de GSD, seja como fornecedor, consumidor de dados ou participante das atividades, e também cita um conjunto de ferramentas que podem apoiar a execução desse processo.

Quadro 1

Atividades da GSD e seus produtos

ATIVIDADE	PRODUTO
Entender as necessidades de segurança de dados e os requisitos regulatórios	Requisitos de segurança do negócio e dos órgãos regulatórios
Definir políticas de segurança de dados	Documento de política de segurança de dados
Definir padrões de segurança de dados	Documento de padrões de segurança de dados
Definir controles e procedimento de segurança de dados	Documento de procedimentos e controles da segurança
Gerenciar usuários, senhas e grupos de usuários	Controle de contas, senhas, papéis e grupo dos usuários
Gerenciar visões e permissões de acesso aos dados	Controle de acessos e permissão aos recursos de dados
Monitorar e autenticar usuários e comportamento de acesso	Registros de acessos, alertas de notificações de segurança, relatórios de segurança dos dados
Classificar o nível de confidencialidade das informações	Metadados de classificação dos dados Registro de documentos e bancos de dados confidenciais
Auditar a segurança dos dados	Relatórios de auditoria

Uma organização pode optar por terceirizar uma série de funções de TI, inclusive a de execução da segurança, mas não a sua a responsabilidade pelo processo de Gestão da Segurança dos Dados. Nesse caso, torna-se necessário o estabelecimento de contratos que tratem questões como responsabilidades e expectativas de cada papel dentro do processo, acordos de nível de serviço, direitos de autoria, obrigações contratuais, relatórios de acompanhamento.

Dessa discussão, percebe-se que o processo de Gestão da Segurança dos Dados proposto pelo framework Dama-DMBok pode resolver parte dos problemas relacionados à segurança, atribuindo papéis e sugerindo o estabelecimento de políticas, padrões, regras e procedimentos para garantir a segurança das informações organizacionais. Ele estabelece um modelo de referência para a Gestão de Dados e, assim como outros corpos de conhecimentos, deve ser cuidadosamente analisado e adaptado para a realidade da empresa, tendo-se o cuidado de estabelecer uma proposição de gestão de dados que caiba nos recursos e se ajuste aos aspectos culturais e de negócios da empresa.

Referências

DAVENPORT, Thomas H. *Ecologia da informação*: Por que só a tecnologia não basta para o sucesso na era da informação. 2. ed. São Paulo: Futura, 1998.

DMBOK. Mark et al. *The DAMA Guide to The Data Management Body of Knowledge*: DAMA-DMBOK Guide. 1. ed. Estados Unidos: Technics Publications, 2009.

DRUCKER, Peter. *Sociedade pós-capitalista*. São Paulo: Pioneira, 1993.

***Fernanda Farinelli**

Mestre em Administração de Empresas pela Fundação Pedro Leopoldo. Especialista em banco de dados pelo Centro Universitário Belo Horizonte (UNI-BH). Bacharel em Ciência da Computação pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas). Analista de TIC na Prodemge. Professora do Fundação Pedro Leopoldo e da pós-graduação da PUC Minas. Colaboradora da Dama (Data Management Association) Capítulo Brasil.

Lei de Acesso em Minas Gerais

Divulgação

Plínio Salgado*

A Lei de Acesso à Informação (lei n. 12.527/2011) exigiu, para a sua concretização no Estado de Minas Gerais, investimentos em recursos tecnológicos e humanos, além da conscientização dos servidores quanto à sua importância e aplicação em sua atividade diária.

Para assegurar o direito de acesso à informação às pessoas naturais e jurídicas, foi preciso modificar algumas rotinas para adequá-las à Lei e torná-las procedimentos objetivos e ágeis, em linguagem de fácil compreensão.

O principal desafio trazido pela Lei de Acesso à Informação foi estabelecer o respeito à publicidade como preceito geral, sendo o sigilo a exceção. Também, foi preciso reforçar a divulgação de informação de interesse público, independentemente de solicitação, para tanto, atualizaram-se os meios de comunicação oferecidos pela tecnologia da informação. Com a promoção da cultura de transparência na Administração Pública, procurou-se incentivar o controle social da Administração Pública.

O Governador do Estado de Minas Gerais editou o Decreto Estadual n. 45.969, publicado em 24/05/2012. O Decreto regulamentou as diretrizes da Lei n. 12.527/2011, no âmbito do Poder Executivo estadual. Dois artigos se destacam: o art. 37, que fixa a competência da Controladoria-Geral do Estado para orientar a organização das informações do Estado, e o art. 51, que estabelece a obrigação dos órgãos e entidades de ajustarem a sua política de gestão de informações.

Foram realizadas reuniões preparatórias com auditores setoriais e seccionais, com os gestores dos sítios eletrônicos institucionais e com os assessores de Comunicação, antes da entrada em vigor da Lei. Foram feitas melhorias nos canais de atendimento em funcionamento no dia 15/5/2012: Unidades de Atendimento Integrado e LigMinas (155). O Portal de Transparência do Estado de Minas Gerais recebeu atualizações e novas ferramentas. O acesso de visitantes únicos ao Portal, em maio, registrou aumento de 140% em relação ao mesmo mês do ano anterior e, em relação a abril de 2012, o número de visitantes únicos aumentou em 100%.

Foi realizado um trabalho de levantamento das informações produzidas por todos os órgãos e entidades do Poder Executivo, como um primeiro passo na organização da política de gestão de informações. Para isso, foram incluídos quatro relatórios no Acordo de Resultados 2012, instrumento que pontua aqueles que cumprem as obrigações determinadas e refletem no pagamento da gratificação anual.

Em nosso entendimento, o Governo de Minas Gerais cumpre o seu papel e espera que a sociedade use sua capacidade de desenvolver os mecanismos para utilizar as informações, fazendo delas uso legítimo, contribuindo assim com o poder público no aprimoramento do processo de transparência, no controle social e na aplicação adequada dos recursos públicos. Como parceiros da estratégia governamental, a população, antes considerada apenas destinatária das políticas públicas implementadas pelo Estado, passa agora a ocupar também a posição de protagonista na priorização das estratégias governamentais em todos os níveis.

***Plínio Salgado**
Controlador-Geral do Estado de Minas Gerais

Benchmarking

A necessidade de se implantar uma política de segurança da informação para garantir a proteção das informações e a continuidade do negócio já é um conceito consolidado entre dirigentes de organizações, assim como a definição de normas e sua aplicação no seu dia a dia. Para garantir o sucesso dessa ação, o envolvimento dos usuários – todo profissional da empresa, incluindo os cargos de direção – é peça essencial. "O usuário é o elemento no processo da segurança da informação que vai cristalizar, operacionalizar e fazer acontecer a segurança da informação. Ele tem um papel fundamental", afirma o professor e consultor em segurança da informação Edison Fontes.

Nesta edição, conheça o trabalho de comunicação de duas empresas, Companhia Energética de Minas Gerais (Cemig) e Companhia de Tecnologia da Informação do Estado de Minas Gerais (Prodemge), para educar e conscientizar empregados sobre suas políticas de segurança da informação.

Campanha de segurança da informação da Cemig

"Contamos com você". É com esse lema que a Companhia Energética de Minas Gerais (Cemig) vem trabalhando desde 2001 para mostrar aos empregados sua importância dentro do processo de segurança da informação (SI). A frase está presente na logomarca da SI (um círculo verde, com as inscrições "Segurança da informação", "contamos com você" e "Cemig"), usada desde 2005 – e uma das poucas que ainda são utilizadas na empresa após a consultoria contratada para estudar o valor da Cemig.

"Essa logomarca é utilizada em todas as produções da Administração da Segurança da Informação (ASI), garantindo, assim, a imediata associação por parte dos empregados da comunicação com a segurança da informação. E a frase 'contamos com você' é muito importante, por traduzir de forma direta, a mensagem que desejamos passar para os empregados. Nosso intuito é o de que cada pessoa que entre na Cemig, que participe de um de nossos treinamentos, que tenha acesso a algum veículo utilizado por nossa comunicação, seja sensibilizada pela importância do tema e que venha fazer parte do nosso batalhão da segurança da informação", explica o coordenador da ASI, Arlindo Edson Porto Nunes.

O que se busca atingir com as campanhas de segurança da informação na empresa é a adesão e a compreensão dos empregados, fazendo com que eles entendam e também adotem os procedimentos de SI. Para isso, além da logomarca, a ASI frisa em todo trabalho de conscientização que a postura e a participação do empregado são fundamentais para alcançar o sucesso e as metas da segurança da informação. O resultado é que a Cemig, em 2011, superou a meta acordada para o índice de Segurança da Informação em seu *Balanced Score Card* (BSC) – metodologia de medição e gestão de desempenho.

Processo de comunicação

A Cemig formalizou, em 2005, seu processo de comunicação e educação em segurança da informação, que tem o objetivo de disseminar o conhecimento desse tema entre os empregados, terceirizados e fornecedores. Segundo Arlindo, esse processo traz benefícios como a melhoria no resultado do componente "pessoas" que participa do cálculo do índice de segurança da informação; melhoria na adoção dos procedimentos de segurança da informação; redução de incidentes de segurança da informação e uso adequado dos recursos de informática, o que diminui custos, reduz o risco e erro humano e a possibilidade de vazamento de informações estratégicas da empresa.

Duas campanhas são produzidas pela ASI anualmente, pois, segundo Arlindo, essa é a periodicidade mínima para que o conhecimento repassado não se perca. Os temas são definidos a partir dos resultados de uma pesquisa respondida anualmente pelos empregados. "Junto com a área de recursos humanos, selecionamos uma amostra representativa dos empregados que participarão do processo.

Os dados obtidos nela são compilados e analisados para, então, estabelecermos quais temas serão tratados pelas campanhas no próximo ano", explica. A pesquisa também permite à ASI determinar se há necessidade da campanha (que inclui também treinamentos) ser direcionada para alguma cidade, área da empresa ou pessoa específica, dependendo do nível do risco apresentado.

Mudanças na política de segurança da informação da Cemig também podem demandar uma campanha de comunicação: "Se houver alguma alteração legal, tecnológica ou organizacional, que mude substancialmente os critérios e procedimentos que devam ser adotados, ela também pode ser uma demanda". Ainda segundo Arlindo, a identificação de incidentes de segurança da informação, fora da normalidade da empresa, exige um trabalho de comunicação rápido e específico. Nesses casos, a ASI utiliza o informativo digital "Radar" para que os empregados tenham conhecimento do problema, dos procedimentos que devem adotar quando necessário e das ações que estão sendo tomadas visando ao retorno da normalidade.

Guia do Usuário e cartilha para filho dos empregados

Outra fonte de informação é o site da segurança da informação, acessado a partir da página principal da intranet da Cemig. "Para mostrar o apoio da alta gerência da Cemig, temos no site, o pronunciamento do diretor da Diretoria de Gestão Empresarial sobre a importância da adoção da segurança da informação como forma de auxiliar a empresa na realização de sua missão e no alcance de sua visão" enumera Arlindo. Ele diz ainda que tudo que a ASI faz é sempre muito bem explicado, com o intuito de que o empregado entenda as razões pelas quais as medidas estão sendo adotadas.

Linguagem direta e clara, deixando de lado aquele caráter sisudo de uma comunicação corporativa, é outro fator importante para o processo. "O nosso estilo e a nossa forma de comunicar com a empresa são tão característicos que, há alguns anos, fizemos uma campanha sem a nossa marca, como uma brincadeira, e, mesmo assim, as pessoas reconheceram que era nosso trabalho", conta Arlindo. Os novos empregados que a Cemig vem contratando também exigiram da ASI uma nova forma de comunicar. Eles são mais jovens e, com isso, cartuns, treinamentos interativos, textos curtos (ou nenhuma leitura) e filmes passaram a ser utilizados.

O fundamental, afirma Arlindo, é fazer um trabalho contínuo, que esteja alinhado com o público que se quer atingir. Além de utilizar filmes, cartazes, peças teatrais, cartilhas, palestras, artigos, jogos, comunicados, charges, desenhos animados e a intranet da Cemig, a ASI busca aproveitar qualquer outro veículo ou espaço disponibilizados pela área de comunicação da empresa.

Peças gráficas de campanha

Cartazes utilizados em campanha sobre senha segura

A ASI recebe muitas sugestões de empregados sobre temas e assuntos de segurança da informação que podem ser tratados pela área, o que, para Arlindo, é um dos retornos mais importantes, pois comprova o comprometimento do empregado e o sucesso do processo de comunicação. “As pessoas são conscientizadas na empresa, levam este conhecimento para casa, para a família, amigos e, como cidadãos, vão mudando o seu comportamento e passam a ser agentes de mudança comportamental da sociedade. Até chegar ao nível de terem um posicionamento, um questionamento ou sugerirem ações a partir de qualquer assunto que a ASI divulgue. Isso é muito bacana e gratificante”.

Nova realidade

A Cemig está implantando uma estrutura de automação da distribuição de energia, que a torna sujeita a novas ameaças, inclusive das guerras cibernéticas. “Qualquer novidade tecnológica impacta na política de segurança da informação e, a partir daí, você tem que trabalhar a conscientização dos empregados”. Por isso, a preocupação da ASI em preparar e alertar os empregados para este novo cenário e os riscos causados por ele; o que levou o assunto a ser tema de campanha de SI em 2011. Nesse ano, no Dia Internacional da Segurança da informação, autoridades do governo federal, representantes do Exército e da Marinha e especialistas em guerra cibernética foram convidados a palestrar em um evento no auditório da empresa, transmitido para todo o Estado. Na ocasião, também foi mostrado como a guerra cibernética poderá atingir a Cemig, como a empresa está se preparando e quais os próximos passos a serem tomados.

Para chamar a atenção, o convite e a divulgação desse evento tinha que causar impacto. Arlindo conta como foi: “Na manhã do evento, simulamos um ataque a todas as instalações e máquinas da Cemig, com exceção das áreas de controle de energia, de tecnologia da informação e a diretoria. Todos os computadores receberam uma mensagem de alerta, as luzes foram apagadas e, para evitarmos pânico, o sistema de comunicação avisou que se tratava de uma simulação de ataque de guerra cibernética e convidou a todos para o evento. Claro que, com isso, o interesse de todos aumentou consideravelmente”.

Divulgação

Equipe: Giovani Davi Silva, William Resende Gonçalves, Telma Elisa da Silva e Arlindo Edson Porto Nunes

Campanha de segurança da informação da Prodemge

A implantação do sistema de controle de acesso físico marcou o lançamento da primeira campanha de segurança da informação na Prodemge. Para isso, um evento foi realizado no pátio da empresa, em 2006, e contou com a entrega de novos crachás aos empregados, além de uma cartilha de segurança da informação que continha os principais pontos que garantem a segurança da informação e instruções sobre senha e confidencialidade. Durante a solenidade, o então presidente da Prodemge, Maurício Dias Costa, também assinou as principais normas relacionadas ao tema.

"A identidade visual e o slogan dessa campanha, 'Adote essa ideia, foram elaborados por uma consultoria externa contratada para elaborar um plano corporativo de segurança para a Prodemge e as secretarias de Fazenda e de Planejamento e Gestão", explica a analista de comunicação da Prodemge, Lívia Mafra. Segundo ela, as peças gráficas que apoiaram a implantação do projeto de segurança da Prodemge foram adaptadas para a realidade da empresa pela área de comunicação da Companhia. Com a equipe de SI, a área também foi responsável pela criação de um hotsite na intranet, em que eram divulgadas as notícias de interesse dos empregados. Outra ação para atingir e conscientizar a comunidade Prodemge foram palestras ministradas por especialistas da área. Eles trataram de temas como segurança da informação, política de segurança, segurança física e continuidade, segurança no dia a dia, pessoas, classificação da informação e ameaças.

Após dois anos de trabalho, marcados pela reestruturação da área de Segurança da Informação (SI) e revisão dos instrumentos normativos, teve início uma nova etapa da comunicação sobre segurança da informação da Prodemge. Sua principal característica: uma mascote criada para ser a porta-voz da SI. "Ele foi pensado para ter um perfil agradável, sem se mostrar como inimigo ou um cão de guarda", conta a gerente de Segurança da Informação da Prodemge, Carine Carvalho. Uma pesquisa conceitual revelou que o suricato tinha o perfil mais adequado à mascote: esse animal anda em bando, faz revezamento para tomar conta da toca e emite sinais sonoros de alerta.

Lívia lembra que, buscando envolver os empregados na nova etapa da campanha, foi realizado um concurso para escolher o nome da mascote. "Zé Loso foi o vencedor e o empregado que o sugeriu ganhou uma assinatura de revista", conta. A partir desse momento, o Zé Loso esteve e está presente em todas as ações e peças de comunicação da segurança da informação na Prodemge. Na avaliação de Carine, a utilização da mascote tem se mostrado positiva, propiciando o reconhecimento imediato das pessoas do assunto de SI e, por isso, é usada até hoje.

O tema dessa segunda etapa, e que durou até 2012, foi "Segurança da Informação: seja parte dela". O objetivo era ser um convite às pessoas para participar do projeto, alertando para a importância que elas têm no processo. Lívia ressalta o dia do

lançamento da campanha: “A empresa recebeu uma decoração diferente e personalizada. Havia cartazes nos quadros de aviso, *banner*, faixa, cartazes e lembretes sobre hábitos seguros nas estações de trabalho. Os empregados receberam um e-mail especial sobre o lançamento, que também apresentava o Zé Loso. Também distribuímos um porta-crachá retrátil e fizemos um *quizz* premiado sobre segurança da informação”.

Durante os quatro anos de duração dessa segunda etapa, diversas atividades foram elaboradas constantemente para envolver os empregados e informar sobre as normas e instruções relacionadas ao projeto de SI. Além delas, duas ações especiais foram programadas: a *Semana de Segurança da Informação* e o *Um Dia na Prodemge*.

A primeira aconteceu em novembro de 2009. De acordo com Lívia, na abertura, a coordenadora da Promotoria Estadual de Combate aos Crimes Cibernéticos do Ministério Público do Estado de Minas Geras, Vanessa Fusco, falou sobre os limites e as possibilidades de enfrentamento dos crimes cibernéticos no Brasil; e os outros dias foram dedicados ao debate do assunto por parte de diversos especialistas.

O evento *Um Dia na Prodemge* foi uma sugestão de uma empregada da Prodemge, durante outro evento, denominado *Bate Papo com a GIS* – um espaço no qual os empregados podiam tirar dúvidas e dar sugestões à equipe de segurança da informação da Prodemge. Nas férias de julho 2009, 90 filhos de empregados visitaram a sede da empresa (então localizada no bairro de Lourdes, em Belo Horizonte); assistiram a uma palestra sobre navegação segura na internet; praticaram ginástica laboral (assim como os pais o fazem periodicamente); e conheceram o Palácio da Liberdade (antiga sede do governo mineiro). “O sucesso foi

Peças gráficas da primeira campanha

Cartazes da segunda campanha

tanto que planejamos uma nova tarde, com mais 70 crianças", relembra Lívia.

Terceira campanha

No segundo semestre de 2012, teve início a terceira campanha de segurança da informação da Prodemge. Após um período de adaptação ao novo cenário vivido pela empresa (em junho de 2010, a sede foi transferida para a Cidade Administrativa Tancredo Neves, nova sede do governo mineiro), as equipes de segurança da informação e de comunicação elaboraram uma campanha que tem um novo tema "Segurança da Informação: a gente cuida". Lívia explica que, após seis anos, os empregados já têm uma maior consciência e maturidade do que deve ser feito para proteger as informações corporativas e dos riscos envolvidos. Por isso, o objetivo é promover uma reflexão coletiva sobre a importância e os cuidados com a informação e relembrar diretrizes e normativos.

Nesse sentido, a campanha foi estruturada em cima de três pilares da segurança da informação: confidencialidade, integridade e disponibilidade. Serão abordados temas como classificação da informação, descarte de documentos e mídias, acesso lógico, senhas, redes sociais, malware e backup.

"A comunicação é importante, pois temos que constantemente lembrar as regras, os riscos e os fatores envolvidos com a segurança da informação. Para além das campanhas, a *newsletter* tem surtido efeito nesse sentido. Os assuntos são definidos a partir da necessidade do dia a dia e surgem também de perguntas dos empregados, mudanças nas normas, legislação", conclui Carine.

Cartazes da terceira campanha

O usuário faz

a diferença em segurança da informação

Divulgação

Edison Fontes*

Segurança da informação é um processo organizacional que tem como objetivo garantir a realização do negócio no que depende da informação e dos recursos de informação. Um recurso de informação é qualquer elemento que armazene, transmita, reproduza ou apresente uma informação. Pode ser um computador ou uma simples folha de papel.

Em um processo de segurança da informação, são desenvolvidos regulamentos, elaborados controles de acesso físico e lógico, criados planos de continuidade, realizadas análises de riscos e implantadas outras ações que estruturam esse processo. É um trabalho de grandes proporções e de uma variedade de ações.

Nesse conjunto de ações, existe um elemento que faz a diferença entre o sucesso e o insucesso da proteção da informação: o usuário! Isto é: você.

A pessoa humana é fator crítico de sucesso. Melhor dizendo, a pessoa humana é o fator decisivo para o sucesso. Mas, para que isso aconteça, o que é necessário? Podemos elencar algumas características que precisam ser consideradas para que o usuário faça a diferença.

a) A organização precisa definir políticas e normas

É necessário que regulamentos de segurança da informação existam e sejam explicitados para os usuários. A organização precisa dizer como ela deseja que o usuário se comporte em relação ao uso da informação. O usuário precisa saber suas responsabilidades, o que é permitido, o que é proibido, o que fazer em situações de exceção e a quem recorrer quando não souber o que fazer diante de uma determinada situação.

b) A alta direção precisa cumprir as políticas e normas

Os regulamentos de segurança da informação são obrigatórios para todos. Caso existam situações diferentes, elas devem ser descritas nas políticas e normas. Transparência, seriedade e exemplo da alta administração são fundamentais para o sucesso da segurança da informação.

c) Abordagem profissional para a segurança da informação

O usuário precisa ser ensinado, treinado e continuamente lembrado que o processo de segurança da informação exige um comportamento profissional para todos. As regras são definidas para a proteção da informação da organização. Não existe nada pessoal contra qualquer usuário. Caso um usuário não necessite de um determinado acesso a uma informação para o desempenho das suas funções na organização, ele não deve ter esse acesso. O usuário precisa entender que a organização não está perdendo a confiança nele. A organização está agindo profissionalmente.

d) A segurança da informação vai impactar as atividades do usuário

Existe uma relação inversamente proporcional: segurança e facilidade de uso. Quanto mais segurança, menos facilidade de uso. Quanto mais facilidade de uso, menos segurança. É um fato! A organização precisa ser transparente com esse fato e dizer para o usuário que algumas vezes a facilidade de uso vai ser impactada, porque o tipo de negócio da organização exige uma proteção rígida para a informação.

e) Clima organizacional envolve a segurança

Um bom clima organizacional é bom para a organização como um todo. A segurança será beneficiada se a organização possuir um bom clima organizacional. Quem trabalhou ou trabalha em organizações com um clima organizacional agradável sabe muito bem que camaradagem, transparência e trabalhos em grupo podem conviver com hierarquia, regras e responsabilidades. Esse conjunto contribui para o sucesso da organização.

"TRANSPARÊNCIA, seriedade e exemplo da alta administração são fundamentais para o sucesso da segurança da informação."

f) O usuário pode discordar das regras, mas tem que segui-las

Quando uma organização explicita suas regras e explica o porquê delas, facilita o entendimento pelos usuários. Isso não quer dizer que os usuários vão concordar com tudo, mas eles precisam entender tudo. Com essa abordagem, os usuários vão ter uma atitude profissional em seguir as regras. Ou, se essa diferença for muito grande, o usuário vai buscar outra organização em que ele se sinta adequado.

g) Mundo virtual

O mundo virtual cada vez mais faz parte da vida das pessoas. O mundo virtual e o mundo físico compõem o ambiente de vida do usuário. A organização precisa definir para o usuário como, ele sendo um colaborador, deve se comportar em relação às informações da organização. Sem nenhuma má-fé, o usuário pode compartilhar informações da organização que são confidenciais e deveriam ficar restritas internamente.

h) A segurança da informação pessoal do usuário

A organização tem responsabilidade em tratar com responsabilidade e sigilo os dados dos seus usuários. Mas, muitas vezes, o próprio usuário não tem esse cuidado. O usuário compartilha suas informações pessoais no mundo virtual. Na maioria das vezes, disponibiliza muitas informações suas nas redes sociais. Essa é uma decisão do usuário, mas ele precisa estar atento que os amigos dos amigos, e os amigos dos amigos dos amigos tomarão conhecimento dos comentários do usuário. Sejam comentários de que está em tal aeroporto, que está no curso de inglês, que odeia o seu chefe ou que não queria estar trabalhando naquela segunda-feira. Principalmente se depois ele mudar de ideia ou ficar constrangido diante do chefe.

Muitas vezes é dito que a pessoa humana é o elo mais fraco da corrente de segurança da informação. Entendo que se a organização tiver uma atitude profissional e honesta no processo de segurança da informação, a pessoa humana também será o elo mais forte na corrente da proteção da informação.

Para que isso aconteça, o usuário precisa estar comprometido com a organização. Algumas pessoas querem apenas estar envolvidas. Não dá! Estar comprometido é mais do que estar envolvido. Não sabe a diferença? Quando comemos ovos com bacon no café da manhã, a galinha está envolvida, mas o porquinho está comprometido.

Boa segurança para todos!

***Edison Fontes**
Mestre em Tecnologia, certificado CISM, CISA, CRISC (Isaca-USA), professor e consultor em segurança da informação. É autor de cinco livros sobre proteção da informação na organização.
edison@pobox.com.

Arquitetura empresarial e segurança de informação: uma profícua sinergia

Divulgação

Marcello Bax*

1. Introdução

Além de comentar aqui a respeito do desafio enfrentado pelas empresas e órgãos públicos no esforço para lidar com seu legado informacional de forma segura, pretende-se argumentar sobre como um processo de elaboração de uma Arquitetura Empresarial (AE) pode apoiar tal esforço.

Com efeito, as ameaças à segurança dos negócios de um órgão público e seu ambiente operacional de tecnologia podem advir das mais variadas fontes. Isso inclui ataques de hackers, uso inadequado de novas tecnologias, manutenção precária dos sistemas, funcionários descontentes, desastres naturais, e até mesmo erros não intencionais, entre outros.

Como o uso das Tecnologias de Informação e Comunicação (TIC) continua a acelerar, as agências governamentais estão cada vez mais expostas a ameaças diárias quanto à confidencialidade, integridade e disponibilidade das informações que gerenciam. Por isso, elas investem uma quantidade crescente de recursos em soluções de segurança e privacidade de dados e informações a fim de cumprirem sua missão e atenderem as exigências legais de proteção de informações em face de ameaças cada vez mais sofisticadas.

A Arquitetura Empresarial (AE) é uma disciplina emergente que fornece um contexto ao mesmo tempo amplo e expressivo sobre como se estrutura o alinhamento entre tecnologia e negócios em uma organização. Esse contexto pode servir também para se projetar e implementar controles de segurança de informação eficazes e que abarcam toda a organização. Assim, existem metodologias de AE que incluem o domínio segurança de forma integrada, permitindo análises que ultrapassam perspectivas pontuais no nível de sistemas de informação isolados e promovem, assim, uma visão de segurança e privacidade de toda a empresa. A partir de uma visão global da organização, tais metodologias guiam a implantação de controles de privacidade que vão assegurar a confidencialidade, integridade e disponibilidade de dados e informações. Essas metodologias são conhecidas como Arquiteturas de Segurança de Informação Empresarial (ASIE) e são explicadas mais adiante no texto.

2. Arquitetura empresarial e segurança de informação

A gestão apoiada pela elaboração da Arquitetura Empresarial (AE) ou Corporativa (uma prática emergente) fornece um contexto interessante para o desenvolvimento de controles de segurança e privacidade. A AE estabelece o quadro geral, corporativo, das relações entre estratégia, negócio e tecnologia nas organizações. Nesse contexto, a estrutura de segurança pode ser considerada uma subarquitetura

que permeia todos os níveis da AE e inclui, nesta última, camadas que contêm requisitos de segurança e privacidade. As camadas de tal subarquitetura podem englobar, por exemplo: governança da segurança da informação; operações de segurança, segurança pessoal; segurança da informação/fluxo de dados; segurança de sistemas, segurança de infraestrutura e até a segurança física.

É importante, entretanto, destacar o fato de que controles de segurança e privacidade totalmente à prova de falhas não existem. Isso porque os componentes da AE e soluções de segurança são concebidos e geridos por membros da organização ou agentes contratados, e o acesso privilegiado é uma ameaça que não pode ser completamente superada, devido a relações de confiança e privilégios inerentes.

Contudo, com base no panorama amplo fornecido pela AE, uma agência governamental pode alcançar uma solução bem-ajustada aos riscos que corre efetivamente, nem excessiva nem frouxa demais. Como vimos, tal solução permite uma abordagem completa das ameaças internas e requisitos de segurança da informação englobando a organização como um todo. Uma solução desse tipo é geralmente denominada de Arquitetura de Segurança de Informação Empresarial (ASIE).

"A ARQUITETURA Empresarial fornece um contexto amplo e expressivo sobre como se estrutura o alinhamento entre tecnologia e negócios em uma organização."

3. Arquitetura de segurança de informação empresarial

Arquitetura de Segurança de Informação Empresarial (ASIE) é uma parte da AE que tem foco na segurança da informação como um todo. Trata-se de aplicar um método abrangente e rigoroso para descrever a estrutura e o comportamento atual e/ou futuro dos processos de segurança de uma organização e seus sistemas de informação de modo que eles se alinhem com os objetivos estratégicos centrais da organização que são dados pela alta direção.

Embora muitas vezes associadas à área de tecnologia (de segurança da informação), a arquitetura se relaciona de forma mais ampla às práticas de segurança do negócio e não apenas à tecnologia, na medida em que aborda informação, negócios, produtos e processos também.

4. ASIE como proposta de solução integrada e global

Como dissemos acima, ao considerar o aspecto "segurança" de forma incorporada à AE, a ASIE fornece uma visão ampla e integrada, bem superior àquela caracterizada por configurações localizadas em silos de sistemas e redes específicos. Trata-se de uma proposta de solução empresarial que incorpora informações de negócios, sistemas de informação e tecnologia e adiciona o domínio "Segurança". Alguns artefatos adicionais se agregam então à AE, tais como roadmaps de negócios, requisitos legais, roadmaps de tecnologia, tendências da indústria, análises de riscos etc.

Como metas, a ASIE buscará dar coerência, estrutura e coesão à organização, e permitir o alinhamento do negócio com a tecnologia, sem descuidar da segurança. Trata-se de um processo de modelagem que fornece abstração de modo que fatores complicadores, como de tecnologia e software, sejam removidos e recolocados em diferentes níveis de detalhes somente quando necessário. Além disso, uma das metas mais importantes talvez seja a de estabelecer uma "linguagem" comum para o tratamento da segurança da informação dentro da organização.

5. Ferramentas e guias conceituais: frameworks

A prática de ASIE envolve o uso de algum framework que fornece os elementos conceituais necessários à elaboração de uma série de arquiteturas de referência: arquitetura "atual", "intermediária" e "alvo", bem como de sua aplicação para negociar e alinhar os projetos de mudança preconizados pelas partes interessadas no negócio (stakeholders).

Tais frameworks definem conceitos que servem para descrever em detalhes a organização, os papéis dos atores, as entidades e os relacionamentos que existem ou devem existir para executar um conjunto de processos de negócios. Eles fornecem uma taxonomia rigorosa e formal (uma ontologia) que identifica claramente que processos uma empresa executa, e relacionam que informações detalhadas sobre como esses processos são executados de forma segura.

O produto final é um conjunto de artefatos (diagramas) que descrevem, em diferentes graus de detalhe, exatamente o que e como a organização opera e quais controles de segurança já existem ou são necessários. Esses artefatos são muitas vezes gráficos, como diagramas visuais, mas não são meros desenhos ilustrativos, pois podem ter sua validade verificada por software.

Dadas essas descrições, cujos níveis de detalhe irão variar de acordo com o ponto de vista de cada um dos stakeholders com que se busca comunicar, "decisores" podem melhor fundar suas decisões sobre onde investir recursos, onde realinhar objetivos organizacionais e processos e que políticas e procedimentos apoiarão a missão ou as funções de negócios da organização.

"O OBJETIVO DE criar uma arquitetura na organização é garantir que a estratégia de negócios e tecnologias estejam alinhadas também com as preocupações de SI"

No framework utilizado como guia conceitual de elaboração da arquitetura, junto com os modelos e diagramas sugeridos, vai também um conjunto de melhores práticas que visam a garantir a adaptabilidade, escalabilidade e gerenciamento dos modelos criados. Essas melhores práticas não são exclusivas da ASIE, mas são essenciais para o seu sucesso. Elas envolvem princípios como a componentização, a comunicação assíncrona entre os componentes principais, identificadores e assim por diante.

6. Metodologia

A implementação da ASIE começa por documentar a estratégia da organização e outros detalhes necessários, tais como: onde (em que mercado) e de que forma ela opera o seu negócio. O processo então segue em cascata para baixo, com vistas a documentar as competências essenciais dos atores, os processos de negócios e como a organização interage com ela mesma e com as partes externas, como clientes, fornecedores e governo.

Tendo documentado a estratégia da organização e sua estrutura, o processo de arquitetura, então, flui para dentro dos componentes de tecnologia de informação, tais como: (1) organogramas, atividades e fluxos de processo de como a organização opera; (2) fornecedores de hardware, software e serviços; (3) inventários de aplicações, softwares e modelos; (4) interfaces entre aplicações: eventos e fluxos de dados; (5) intranet, extranet, internet, comércio eletrônico, links EDI com as partes, dentro e fora da organização; (6) classificações de dados, bancos de dados e modelos de suporte de dados; (7) hardware, plataformas de hospedagem: servidores, componentes de rede e dispositivos de segurança e onde eles são mantidos; (8) redes locais e metropolitanas, diagramas de conexão à internet etc.

Sempre que possível, todos os itens acima devem ser explicitamente relacionados com a estratégia da organização, objetivos e operações. A ASIE irá documentar o estado atual dos componentes técnicos de segurança listados acima, bem como um estado futuro "desejado", ideal (Arquitetura de Referência), e, finalmente, um estado futuro "alvo", que é o resultado da negociação dos compromissos entre o cenário possível versus o cenário ideal. Essencialmente, o resultado é um conjunto de modelos relacionados, e normalmente mantido por software especializado, disponível no mercado.

Vale notar que tal mapeamento exaustivo da ASIE pode sobrepor outras iniciativas já em andamento na organização, como o mapeamento de metadados, ou com o conceito Itil do Banco de Dados do Gerenciamento de Configuração, além

de outras. Assim, quando esse for o caso, manter a consistência das informações pode ser um desafio significativo.

7. Resultados e manutenção do esforço de arquitetura

Um resultado intermediário de um processo de arquitetura é um inventário da estratégia de segurança do negócio que se compõe de elementos como: os processos de segurança da empresa, organogramas, interfaces entre sistemas e topologias de rede e as relações explícitas entre eles. Os inventários e os diagramas são ferramentas que apoiam a tomada de decisão. Mas eles por si só não bastam, pois é ainda preciso manter o processo vivo e em constante revisão. A organização deve elaborar e implementar um processo que garanta o movimento contínuo do estado atual para o estado futuro planejado. No curso desse processo, busca-se preencher as lacunas existentes entre a estratégia atual da organização e a segurança de TI para apoiá-la. É importante também para determinar as atualizações necessárias e substituições que devem ser feitas na arquitetura de segurança de TI com base na idade, viabilidade e desempenho de hardware e software, problemas de capacidade conhecidos ou previstos e outras questões.

Regularmente, o estado atual e futuro são redefinidos para ilustrar e explicar a evolução da arquitetura, tais como: mudanças na estratégia organizacional e em fatores externos como evolução na tecnologia, alterações em clientes/fornecedores/governo, além de alterações internas e externas que ameaçam a organização ao longo do tempo.

8. Considerações finais

A literatura especializada revela que a prática da ASIE está se tornando comum, sobretudo em instituições governamentais e financeiras ao redor do globo. O objetivo de criar uma arquitetura na organização é garantir que a estratégia de negócios e tecnologias estejam alinhadas também com as preocupações de segurança da informação. Ela permite a rastreabilidade dos aspectos de segurança, desde a estratégia de negócio até a camada de infraestrutura de tecnologia subjacente.

Um projeto de ASIE bem-conduzido ajuda a responder a perguntas importantes, tais como: (1) Qual é a postura de risco de segurança da informação da organização?; (2) Está a arquitetura atual agregando valor à segurança da organização?; (3) Como uma ASIE pode ser modificada para que acrescente mais valor à organização?; (4) Com base no que se sabe sobre o que a organização quer realizar no futuro, a atual arquitetura de segurança será um apoio ou está-se assumindo riscos exagerados?; (5) Que riscos são esses?

Assim, a prática da ASIE permite uma abordagem completa das ameaças internas e requisitos de segurança da informação, englobando a organização como um todo.

***Marcello Peixoto Bax**

Doutor em Informática pela Universidade de Montpellier II, França. Possui diploma de Estudos Aprofundados (DEA) em Matemática e Computação e diploma de Estudos Especializados (DESS) em Informática pela Université d'Aix Marseille II, França. Bacharel em Ciência da Computação pela Pontifícia Universidade Católica de Minas Gerais (PUC-Minas). Atualmente é professor associado da Escola de Ciência de Informação da Universidade Federal de Minas Gerais (UFMG). Tem experiência nas áreas de Ciência da Informação e da Computação, com ênfase em Sistemas de Informação, atuando principalmente nos temas: gestão de conhecimento e informação com uso de tecnologias semânticas; sistemas de informação em saúde; inteligência artificial (ontologias) e filosofia da informação; bibliotecas digitais e gestão de conteúdo.

Login e senha x Autenticação do usuário com Certificado Digital

Júlia Magalhães

Luiz Morato Júnior*

Quase todo dia, a imprensa especializada em Tecnologia de Informação e Comunicação (TIC) divulga notícias sobre quebra de segurança de sistemas e aplicações, de hackers e crackers que se apoderaram de cadastros de usuários e senhas, listas de e-mails ou CPFs para uso ilícito e acesso indevido.

Quando você faz um cadastro na internet, é comum que lhe seja solicitado o CPF, um e-mail ou os dois. Um deles será utilizado como o código de usuário. Portanto, é muito fácil se passar por alguém quando se utiliza tais dados como códigos de usuário.

Depois, vem a questão da senha. Alguns aplicativos não dão um tratamento apropriado à senha informada e confirmada pelo usuário. Permitem o cadastramento de qualquer sequência de números simples, como "1234". É verdade que outros aplicativos possuem algoritmos de análise dos caracteres digitados, exigem ao menos um caractere especial, letras, números etc. Mas boa parte dos usuários, por comodidade ou para não esquecer suas senhas, apela para data de nascimento, sequências simples de números, placa de carro e outros elementos de fácil memorização. Ocorre que tal expediente também facilita as coisas para crackers e hackers, os quais já possuem diversos artifícios eficientes para quebrar senhas.

Nesse caso, é importante que as aplicações tenham mecanismos que impeçam ações do tipo "força bruta".

Entretanto, o problema maior em questão é o fato dessa senha trafegar muitas vezes de forma não criptografada – e ser armazenada nos servidores de bancos de dados do mesmo modo.

Para que todas essas fragilidades sejam superadas ou diminuídas, a tecnologia da certificação digital se apresenta como provedora de soluções que garantem:

a) autenticidade: as partes envolvidas na transação podem se identificar mutuamente;

b) privacidade: somente as partes designadas têm acesso às informações da transação;

c) integridade: as informações das transações entre as partes são protegidas contra adulterações;

d) não repúdio: as partes não podem negar os atos por elas praticados com relação à transação;

e) validade jurídica: o uso de certificação digital confere às transações eletrônicas a mesma validade jurídica de transações em papel.

O governo brasileiro institucionalizou a certificação digital como tecnologia para autenticar e identificar os usuários com quem suas aplicações estão interagindo. A Receita Federal e a Caixa Econômica Federal forçaram, no bom sentido, a massificação da certificação digital para as pessoas ju-

rídicas. Quem faz declarações de imposto de renda há mais de 20 anos, como eu, notou a diferença em termos de agilidade e segurança.

No âmbito do governo de Minas Gerais, a autenticação de usuários através de certificação digital é utilizada, por exemplo, pelo Departamento Estadual de Trânsito de Minas Gerais (Detran-MG) desde 2006! Mais recentemente, a Secretaria de Estado de Saúde (SES) implantou o Geicom, sistema de prestação de contas de prefeituras para os recursos disponibilizados pela SES. Prefeitos, secretários municipais de saúde e coordenadores da SES se autenticam com seus certificados digitais.

Mas, afinal, por que e como essa modalidade de autenticação consegue ser tão vantajosa?

Primeiramente, um pouco de teoria e conceitos. O certificado digital é um documento de identidade, um passaporte para realizar transações eletrônicas, visto que uma Autoridade Certificadora garante a identidade do seu titular. Ele fica armazenado em dispositivos criptográficos, que podem ser cartão criptográfico, smart card, token ou arquivo, no caso dos certificados do tipo A1. Além dos dados de identificação do titular do certificado, são armazenadas as chaves pública e privada e a senha individual que dá acesso a esses dados. Todos esses dados são armazenados e trafegados de forma criptográfica, aumentando ainda mais a segurança.

Portanto, quando um sistema ou aplicação está perguntando "Quem é você?", o certificado digital vai garantir as características de autenticidade, integridade e não repúdio. No caso de login e senha, o sistema não tem essas garantias.

Outra grande vantagem é que a senha não trafega na internet. Ela permanece no dispositivo e não em servidores. Esses dispositivos, inclusive, possuem mecanismos de destruição da identidade e da senha, caso sofram uma tentativa de invasão.

Na Engenharia de Software, os fatores que viabilizam uma autenticação e uma identificação segura de determinado sistema são "O que sou?", "O que tenho?" e "O que sei?". A Tabela 1 abaixo mostra a diferença desses fatores entre as modalidades de autenticação:

Tabela 1

Fatores que viabilizam autenticação e identificação segura

FATOR	LOGIN E SENHA	CERTIFICAÇÃO DIGITAL
O que sou?	e-mai, CPF, Masp, etc.	Certificado digital
O que tenho?	–	Dispositivo criptográfico
O que sei?	Senha em arquivo ou no banco de dados, muitas vezes não criptografada	Senha armazenada no dispositivo e criptografada

Fonte: Elaborado pelo autor.

Pode-se concluir, portanto, que o uso da certificação digital como modalidade para autenticação e identificação de usuários apresenta muitas vantagens quando comparado com a utilização de login e senha. Tanto analistas de requisitos e arquitetos de soluções, quanto executivos de negócio devem ter consciência dessas vantagens, de modo a sempre considerar prioritariamente o uso do certificado digital, como fator de segurança e garantia de autenticidade, integridade, privacidade, não repúdio e validade jurídica.

Após a autenticação e identificação do usuário, vem a parte da autorização de acesso e perfis. Interessante dizer que há sites, como o Portal e-CAC do governo federal, que dá acesso a vários serviços se você tem certificação digital e lhe oferece um rol bastante reduzido de serviços se você não possui. Mas isso já é tema para outro artigo.

***Luiz Morato Jr.**

Analista de Sistemas da Prodemge, especialista em Gestão em TI pela UFMG (Universidade Federal de Minas Gerais), gerente de Operações da Autoridade Certificadora Prodemge.

Referências

WIKIPÉDIA. *Autenticação de usuários*. Disponível em: <http://pt.wikipedia.org/wiki/Autentica%C3%A7%C3%A3o>. Acesso em: 9 set. 2012.

ITI. Press release de 30/8/2012. *Certificação digital versus login e senha*: como funcionam e quais os cuidados. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Noticias/PressRelease2012Aug30_231146>. Acesso em: 3 set. 2012.

PRODEMGE. *Apresentação institucional sobre Certificação Digital*. Arquivo em Power Point baixado da Intranet em 30 ago. 2012.

Política de segurança, uma ferramenta eficaz para a segurança da informação de uma organização

Divulgação

Ricardo Cruz*

A Governança Corporativa ganhou força nos últimos anos devido à necessidade de transparência das organizações perante autoridades reguladoras e legislativas. Essa necessidade tem aumentado a importância da implementação de gestão da segurança da informação, gestão de riscos, gestão de crises e outras mais, que, sem o apoio da alta gestão e de uma política de segurança forte, não alcançam a eficiência e a eficácia necessárias para apoiar a estratégia da organização.

Para entendermos em que a Política de Segurança da Informação pode apoiar a estratégia da organização, é preciso explanar sobre estratégia. Embora tenha muitos conceitos, gosto, particularmente, do conceito de Porter, que assim a define: "[...] conceito firmemente integrado, claramente coerente e altamente deliberado, que coloca a empresa em posição de obter vantagem competitiva".

A Política de Segurança é uma ferramenta eficaz para que a organização alcance a segurança da informação, desde que seja vista como tal, não somente para adequação a exigências de mercado, e sim como item essencial para a estratégia organizacional, sendo contribuição importante para que a organização tenha um diferencial competitivo.

As equipes de Governança, Risco e Compliance (GRC), comuns nas organizações que estão preocupadas com as exigências de mercado, com a necessidade de gerir os riscos, de forma a identificar falhas antes que essas aconteçam, devem implementar em seus processos treinamentos e capacitação de todos os colaboradores nas diretrizes de sua Política de Segurança, de forma a inserir na cultura empresarial a importância de se preocupar com a informação.

Ao inserir a segurança da informação na cultura empresarial, apoiada na Política de Segurança, a organização consegue utilizar dessa ferramenta como diferencial competitivo perante o mercado, posicionando-se entre os principais provedores de segurança da informação para seus clientes, trazendo confiança e disponibilidade para os serviços prestados, e agregando valor aos processos do negócio, independentemente de área de atuação: tecnologia, saúde, governo etc.

***Ricardo Cruz**
Bacharel em Gestão Empresarial pelo UNI-BH e pós-graduando em Gestão da Segurança da Tecnologia da Informação. Certificado ISO 27.002, ISO 20.000, Itil, Cobit e Microsoft. Coordenador de GRC na Montreal.

UNIVERSIDADE
CORPORATIVA
PRODEMGE

A segurança da informação discutida em artigos inéditos que abordam a disponibilidade de serviços de rede, computação em nuvem, privacidade, segurança cibernética na América Latina, gestão e informação documental e legado informacional.

UNIVERSIDADE
CORPORATIVA
PRODEMGE

Legado informacional: um desafio dos órgãos públicos

Divulgação

Vanessa Fusco Nogueira Simões

Especialista em Ciências Penais pela Universidade Gama Filho, Rio de Janeiro. Doutora em Direito pela Universitat de Barcelona, Espanha. Coordenadora da Promotoria Estadual de Combate aos Crimes Cibernéticos do MPMG. Representante do MPMG no Grupo Persecução Penal da Estratégia Nacional de Segurança Pública (Enasp).

RESUMO

O incremento da eficiência e da efetividade do setor público aliado ao crescimento da responsabilização dos gestores e dos órgãos ante as demandas sociais e a redução do gasto público com custeio foram importantes mudanças trazidas neste século. A administração pública cada vez mais investe nas Tecnologias de Informação e Comunicação (TICs) e essa modernização trouxe inegáveis benefícios, mas também possibilitou o incremento de condutas ilícitas através das redes ou sistema informatizados da administração pública. A ausência de regulamentação de formas de acesso aos dados que estão nos servidores e que são necessários à investigação criminal é um tema que merece reflexão, bem como a conservação e fornecimento de logs na iniciativa privada.

1. Introdução

Um dos maiores desafios da administração pública atual é justamente como manejar, guardar e proteger a enormidade de informações que circulam diariamente em seus servidores de correios eletrônicos, expostas em suas homepages ou armazenadas em seus servidores. Sobre a questão do armazenamento, outra pergunta vem logo a seguir: pode a administração pública utilizar-se da cloud computing para guardar seus dados?

Primeiramente é preciso ressaltar que, apesar dos órgãos públicos, de maneira geral, já estarem informatizados há bastante tempo, não raramente ainda nos deparamos com a total ausência de regulamento de utilização dos recursos informacionais no serviço público, tanto quanto surgem situações não previstas e até impensadas nos regulamentos existentes.

Segundo Bresser Pereira (1998), esse processo de reforma administrativa e modernização do Estado é uma tarefa de grande importância e os governos no mundo e, em especial, na América Latina e no Brasil, têm dedicado bastante atenção nas duas últimas décadas do século XX.[1]

A modernização dos mecanismos de gestão pública é um objetivo que vem sendo buscado pelas instituições neste século XXI. Através da reforma da gestão pública, os Estados nacionais procuram tornar seus estados mais eficientes e mais voltados para o atendimento das demandas da sociedade, forçados que são pela acirrada competitividade na economia global. Nessa reforma se criam novas instituições e se definem novas práticas, objetivando transformar os burocratas clássicos em gestores públicos focados na reconstrução da capacidade do Estado, no ponto de vista fiscal e de legitimidade democrática.

Paralelamente à necessidade de modernização e movido pelos conceitos de transparência, eficiência no atendimento e acessibilidade, o Estado brasileiro viu-se impelido a investir cada dia mais nas chamadas TICs.

Compilando vários conceitos sobre as TIC, Alexandre Mendes resumiu:

"TIC é um conjunto de recursos tecnológicos que, se estive-

1 BRESSER-PEREIRA, Luiz Carlos. *Reforma da nova gestão pública: agora na agenda da América Latina*. Revista do Serviço Público. Brasília: Fundação Escola Nacional de Administração Pública, jan./mar. 2002.

rem integrados entre si, podem proporcionar a automação e/ou a comunicação de vários tipos de processos existentes nos negócios, no ensino e na pesquisa científica, na área bancária e financeira etc. Ou seja, são tecnologias usadas para reunir, distribuir e compartilhar informações, como exemplo: sites da Web, equipamentos de informática (hardware e software), telefonia, quiosques de informação e balcões de serviços automatizados."[2]

Como uma verdadeira política pública, surgiu o Governo Eletrônico, sinalizando com a possibilidade de serem adotadas plataformas abertas e softwares livres, que por princípio, privilegiam o caráter público do conhecimento, facilitando o compartilhamento de informações, reduzindo ou impedindo a duplicação de esforços e gerando mais conhecimento. Como parte dessa política pública, os governos federal e estadual brasileiro lançaram portais, basicamente com os seguintes objetivos:

"O desenvolvimento de programas de Governo Eletrônico tem como princípio a utilização das modernas tecnologias de informação e comunicação (TICs) para democratizar o acesso à informação, ampliar discussões e dinamizar a prestação de serviços públicos com foco na eficiência e efetividade das funções governamentais. No Brasil, a política de Governo Eletrônico segue um conjunto de diretrizes que atuam em três frentes fundamentais:

1. Junto ao cidadão;
2. Na melhoria da sua própria gestão interna;
3. Na integração com parceiros e fornecedores."[3]

O conjunto das TICs tem acenado com a perspectiva de facilitar a criação de redes de informações e ambientes de interação governo/governo, governo/fornecedores e governo/sociedade, constituindo o que chamamos de governo eletrônico. O maior objetivo das estratégias de governo eletrônico é acelerar processos, facilitar a prestação de serviços e garantir a transparência da coisa pública para todos os cidadãos.

Nesse sentido, a fim de que se possam prestar bons serviços à comunidade, seja pela via do ciberespaço ou pela via presencial, é necessário, antes de tudo, planejar-se no sentido de implantar um processo de modernização com efetividade, ou seja, uma modernização elaborada sobre uma política integrada de desenvolvimento das instituições do Estado, não necessariamente restrita apenas ao período de um governo

O desenvolvimento das TIC no âmbito governamental trouxe vantagens e desafios. Vantagens com uma maior aproximação do governo da sociedade em geral, mais capilaridade, monitoramento de aplicação de recursos públicos e democratização da informação através de programas, como por exemplo, o de inclusão digital. Mas os desafios também estão presentes: segurança da informação, modificação constante nas tecnologias, privacidade *versus* interesse público, investimentos e capacitação e regulamentação do setor.

O reconhecimento do direito à privacidade ocorre dentro dos chamados direitos da personalidade, que têm como característica serem absolutos, indisponíveis, intransmissíveis, irrenunciáveis e não patrimoniais.

Aplicam-se aos dados pessoais, assim, as normas constitucionais que protegem o direito à privacidade, em especial os incisos X, XII e XIV do art. 5º da Constituição Federal.

Recentemente, em 18 de novembro de 2011, foi editada a lei nº 12.527/2011, regulamentando o acesso à informação, que estabelece "os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal".

Referiremos-nos a seguir sobre a questão da quebra da privacidade de dados, ou seja, quando é necessária a preservação e informação de dados – aqueles que são armazenados pelos provedores – quando esses servirem de um meio de prova na investigação criminal, a serem fornecidos por provedores "empresa privada", diante da prática de um crime pela rede mundial de computadores. E, finalmente, iremos abordar a nossa percepção sobre a necessidade de disciplina da guarda de logs no serviço público.

2. Crimes cibernéticos e produção de prova

São puníveis no Brasil aqueles crimes já previstos na legislação penal – Código Penal e leis esparsas – em que o computador ou a rede são o instrumento. Esses crimes, apesar de não se tratarem de crimes cibernéticos "puros", quando praticados pela internet, dependem de que a in-

2 MENDES, Alexandre. Disponível em: <http://imasters.com.br/artigo/8278/gerencia-de-ti/tic-muita-gente-esta-comentando-mas-voce-sabe-o-que-e>. Acesso em: 11 out. 2012.
3 Disponível em: <http://www.governoeletronico.gov.br/o-gov.br>. Acesso em: 11 out. 2012.

vestigação criminal obtenha elementos de prova que estão em poder dos provedores de serviço e provedores de acesso. Assim é que a maioria dos dados necessários não só à produção da prova, bem como à identificação do local do crime[4] para fins de fixação de competência, está em poder da iniciativa privada. Falamos não só de logs de acesso e dados de cadastro, mas também dados de conteúdo, como dados de tráfego, conteúdo de comunicação, a prova material muitas vezes da prática de um crime, tudo está em poder dos provedores.

Inicialmente, faremos uma breve exposição da questão da produção de prova que depende dos provedores em nosso país, para, em seguida, adentrar na questão da guarda de logs no serviço público.

Segundo Fernando Capez (2005):

> [...] a prova destina-se à formação da convicção do juiz acerca dos elementos essenciais para o deslinde da causa... O objeto da prova é toda circunstância, fato ou alegação referente ao litígio sobre os quais pesa incerteza, e que precisam ser demonstrados perante o juiz para o deslinde da causa.[5]

Em se tratando de crimes cometidos pela rede e a volatilidade e velocidade dessa, imprescindível se torna a preservação dos dados de que necessita a Polícia Judiciária e o Ministério Público para realizar a investigação de um crime nessa modalidade. O pedido de preservação da prova de que tanto necessita o investigador é feito tanto aos provedores de conteúdo, quanto aos provedores de acesso.

Nem a conceituação do que são provedores de conteúdo e de acesso está pacificada em nossa doutrina. Vejamos:

Segundo Patrícia Peck Pinheiro (2010):

> Os provedores de acesso não são apenas empresas prestadoras de serviço. São grandes aglutinadores do mundo virtual, responsáveis pela abertura das portas de entrada dos usuários na rede (seja ela pública ou privada). Quanto a estes provedores, existem duas posições jurídicas bem determinadas. A primeira deve a sua atuação como Operadora de Telecomunicações responsáveis pela transmissão de mensagens e conteúdos por meio da rede. A segunda, de Editores, responsáveis pela hospedagem, publicação e até produção de conteúdo na Internet.[6]

Em outra classificação, Marcel Leonardi assevera:

> Provedor de serviços de Internet é o gênero do qual as demais categorias (provedor de backbone, provedor de acesso, provedor de correio eletrônico, provedor de hospedagem e provedor de conteúdo) são espécies. O provedor de backbone é a pessoa jurídica que efetivamente detém as estruturas de rede capazes de manipular grandes volumes de informações, constituídas, basicamente, por roteadores de tráfego interligados por circuitos de alta velocidade. O provedor de acesso é a pessoa jurídica fornecedora de serviços que consistem em possibilitar o acesso de seus consumidores à Internet. O provedor de correio eletrônico é a pessoa jurídica fornecedora de serviços que consistem em possibilitar o envio de mensagens do usuário a seus destinatários, armazenar as mensagens enviadas a seu endereço eletrônico até o limite de espaço disponibilizado no disco rígido de acesso remoto e permitir somente ao contratante do serviço o acesso ao sistema e às mensagens, mediante o uso de um nome de usuário e senha exclusivos. O provedor de hospedagem é a pessoa jurídica fornecedora de serviços que consistem em possibilitar o armazenamento de dados em servidores próprios de acesso remoto, permitindo o acesso de terceiros a esses dados, de acordo com as condições estabelecidas com o contratante do serviço. O provedor de conteúdo é toda pessoa natural ou jurídica que disponibiliza na Internet as informações criadas ou desenvolvidas pelos provedores de informação, utilizando servidores próprios ou os serviços de um provedor de hospedagem para armazená-las. Não se confunde com o provedor de informação, que é toda pessoa natural ou jurídica responsável pela criação das informações divulgadas através da Internet, ou seja, o efetivo autor da informação disponibilizada por um provedor de conteúdo".[7]

O Comitê Gestor da Internet no Brasil, através do site "registro.br" define o que para fins daquela instituição, é considerado provedor de acesso, provedor de serviços e provedor de hospedagem:

As organizações que recebem

4 Através da identificação do usuário do IP (Internet Protocol).
5 CAPEZ, Fernando. *Curso de Processo Penal*. 12. ed. São Paulo: Editora Saraiva, 2005.
6 PINHEIRO, Patrícia Peck. *Direito Digital*. 4. ed. São Paulo: Editora Saraiva. 2010.
7 Disponível em: <http://jus.uol.com.br/revista/autor/marcel-leonardi>. Acesso em: 26 ago. 2011.

endereços IP do Registro.br são classificadas como "ISP" (provedores de serviços e acesso à Internet) ou como "Usuário Final". Tal classificação é de uso exclusivo junto ao Registro.br e não tem por objetivo determinar o tipo de serviço prestado pela organização[8].

Um Provedor de Serviços é uma empresa previamente homologada e certificada através de um contrato firmado com o Registro.br, para que o registro e a manutenção dos domínios e entidades possam ser feitas através de uma interface específica. Os Provedores de Serviços podem ou não oferecer serviços agregados ao registro de domínios. Os clientes dos Provedores de Serviços só podem cadastrar novos domínios ou alterar os dados de domínios e entidades existentes através do seu Provedor de Serviços, sendo que nestes casos o sistema do Registro.br somente permitirá a visualização dos dados de seus domínios e/ou entidades, caso sejam contatos destes.

Já o Provedor de Hospedagem é uma empresa que oferece serviços de hospedagem de sites na Internet e também pode oferecer aos seus clientes o registro de domínio agregado aos seus serviços. Tal provedor não tem nenhum vínculo formalizado com o Registro.br e seus clientes podem interagir diretamente com o sistema do Registro.br, para atualizar dados dos seus domínios e entidades, desde que sejam contatos destes. Estas duas definições são utilizadas somente como nomenclatura na documentação relativa aos serviços do Registro.br.[9]

Para efeitos deste artigo, consideraremos as definições apresentadas pelo CGI acima, tendo em vista se tratar do órgão gestor da internet no Brasil cujos regulamentos são seguidos pelas empresas brasileiras.

Entretanto, consultando site da Anatel, verificamos pela normativa vigente daquela concessionária de serviço público que a sigla ISP (Internet Service Provider) equivale a SCM (Serviço de Comunicação Multimídia)[10]. No Brasil, provedor de acesso é aquele que fornece serviços de valor adicionado (SVA)[11] que referem-se aos serviços presentes na internet e que o diferencia de uma rede comum. O SVA é regido pelo Comitê Gestor de Internet.

Evidentemente, a internet considerada na categoria "meio de telecomunicação" se submete às regras a ela inerentes, como verdadeiro serviço de utilidade pública. Vejamos o que o jurista Fernando Botelho assevera a respeito:

> Particulares prestarão o serviço publico de que é incumbido o Estado e o farão em concurso com o próprio Estado – isto é – com a administração pública central , ou ainda, em nome próprio e em caráter privado, aliás, com a percepção, até, de receitas privadas, por mero arbitramento estatal dos respectivos preços públicos (sistema de tarifamento público)[12].

Em que categoria deverão ser então enquadrados os serviços de telecomunicações – que hoje são prestados, ou executados, e postos, na ponta final de utilização comunitária, pela via do regime particular de contratação? A resposta estará em que constituem as atividades de telecomunicações, basicamente, atividades não-essenciais, mas indisputavelmente úteis aos interesses comunitários, assumindo por isso, conditio de serviços de utilidade pública, na medida em que, o define a Lei (art.60, §1º, da Lei 9472/97), a atuação material representa-se por transmissão, emissão ou recepção for fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos,

8 Disponível em: <http://registro.br/provedor/numeracao/custos.html>. Acesso em: 26 ago. 2011.

9 Disponível em: <http://registro.br/suporte/faq/faq7.html>. Acesso em 26 ago. 2011.

10 Anexo à resolução nº 272, de 9 de agosto de 2001. Regulamento do serviço de comunicação multimídia. "Art. 1º Este Regulamento tem por objetivo disciplinar as condições de prestação e fruição do Serviço de Comunicação Multimídia (SCM). Art. 2º A prestação do Serviço de Comunicação Multimídia é regida pela Lei n.º 9.472, de 16 de julho de 1997, pelo Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução n.º 73, de 25 de novembro de 1998, por outros regulamentos, normas e planos aplicáveis ao serviço, pelos termos de autorização celebrados entre as prestadoras e a Agência Nacional de Telecomunicações (Anatel) e, particularmente, por este Regulamento. Art. 3º O Serviço de Comunicação Multimídia é um serviço fixo de telecomunicações de interesse coletivo, prestado em âmbito nacional e internacional, no regime privado, que possibilita a oferta de capacidade de transmissão, emissão e recepção de informações multimídia, utilizando quaisquer meios, a assinantes dentro de uma área de prestação de serviço".

11 SVA é o PSCI, o provedor de internet propriamente dito e toda a sua edificação, seus servidores, seus roteadores, o seu link de saída para a internet, independente se ela seja uma Lan House ou seja um servidor de jogos, ou tenha um link para uso próprio. O Serviço de Comunicação Multimídia é um serviço fixo de telecomunicações de interesse coletivo, prestado em âmbito nacional e internacional, no regime privado, que possibilita a oferta de capacidade de transmissão, emissão e recepção de informações multimídia, utilizando quaisquer meios, a assinantes dentro de uma área de prestação de serviço, ou seja, pode ser rádio, cabo, tudo que vai do ponto de acesso até o assinante, o meio legal de levar tudo isso até o assinante.

12 Botelho, Fernando Neto. *As telecomunicações e o FUST*. Belo Horizonte: Editora Saraiva. 2001. p.18.

caracteres, sinais, escritos, imagens sons ou informações de qualquer natureza". A cibernética, como ciência-meio, e suas mais atualizadas derivações aplicativas (como a extraordinária telemática) foram, então, assimiladas pelo Estado brasileiro como integrantes da atividade-fim pública denominada telecomunicações, dado o próprio tratamento formal que sobre o tema fornece, antes de qualquer outro, a própria Constituição Federal do país.[13]

Assim é que o Serviço de Comunicação Multimídia (SCM) é um autêntico serviço de utilidade pública e como deve estar sujeito à atuação da agência controladora, ou seja, a Anatel.

Em se tratando de telecomunicações – o que se aplica a SCM conforme dito acima – e com relação especificamente ao auxílio às autoridades na investigação, o Regulamento dos Serviços de Telecomunicações[14] estabelece:

> Art. 26. A Prestadora observará o dever de zelar estritamente pelo sigilo inerente aos serviços de telecomunicações e pela confidencialidade quanto aos dados e informações, empregando todos os meios e tecnologia necessárias para assegurar este direito dos usuários.
>
> Parágrafo único. A Prestadora tornará disponíveis os recursos tecnológicos necessários à suspensão de sigilo de telecomunicações determinada por autoridade judiciária ou legalmente investida desses poderes e manterá controle permanente de todos os casos, acompanhando a efetivação destas determinações e zelando para que elas sejam cumpridas dentro dos estritos limites autorizados.

3. Normativa sobre conservação de dados: o exemplo da União Europeia.

A diretiva relativa à conservação de dados em vigor no âmbito da União Europeia (diretiva 2006/24/CE) exige que os Estados-Membros obriguem os prestadores de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações (a seguir designados por «operadores») a conservarem os dados relativos ao tráfego e os dados de localização durante um período que pode ir de seis meses a dois anos, para efeitos de investigação, detecção e repressão de crimes graves.

A referida diretiva estabelece seu objeto e âmbito de aplicação:

> Objecto e âmbito de aplicação
>
> 1. A presente directiva visa harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro 2. A presente directiva é aplicável aos dados de tráfego e aos dados de localização relativos quer a pessoas singulares quer a pessoas colectivas, bem como aos dados conexos necessários para identificar o assinante ou o utilizador registado. A presente directiva não é aplicável ao conteúdo das comunicações electrónicas, incluindo as informações consultadas utilizando uma rede de comunicações electrónicas[15].

A diretiva prevê que a conceituação de "dados de tráfego", "utilizador", "serviço telefônico", "código de identificação de utilizador" etc., procurando uniformizar o entendimento para que a aplicação da diretiva se adeque aos termos em que foi proposta.

Recentemente, a referida diretiva foi avaliada por uma comissão instituída no âmbito do Conselho e Parlamento Europeu, resultando em relatório contendo as conclusões do grupo de expertos.

A diretiva é aplicável aos "fornecedores de serviços de comunicações eletrônicas publicamente disponíveis ou a uma rede pública de comunicações" (artigo 1º, nº 1). Dois Estados-Membros (Finlândia e Reino Unido) não exigem aos pequenos operadores que conservem os dados, porque, segundo argumentam, os custos tanto para o prestador do serviço como para o Estado seriam superiores aos benefícios retirados em matéria de aplicação da lei e da justiça penal. Quatro Estados-Membros (Letônia, Luxemburgo, Países Baixos e Polônia) indicaram que haviam adotado regimes administrativos alternativos. Embora os grandes operadores presentes em vários Estados-Membros beneficiem de economias de escala em termos de custos, os operadores

13 Botelho, Fernando Neto. *As telecomunicações e o FUST*. Belo Horizonte: Editora Saraiva. 2001. p. 22.
14 Alterado pela resolução nº 234, de 06/09/00 e pela resolução nº 343, de 17 de julho de 2003.
15 Disponível em: < http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:PT:PDF>. Acesso em: 30 ago. 2011.

de menor dimensão de alguns Estados-Membros criam normalmente empresas comuns ou externalizam essas funções para empresas especializadas em programas de conservação e de extração de dados, a fim de reduzirem os seus custos.

A diretiva também diferencia o que é conservação de dados do que é preservação de dados:

> A conservação de dados é distinta da preservação de dados (também conhecida por «congelamento rápido» ou «quick freeze») através da qual os operadores, por ordem de um tribunal, são obrigados a conservar os dados relativos exclusivamente a determinados indivíduos suspeitos de actividades criminosas, a partir da data da ordem de preservação. A preservação de dados é um dos instrumentos de investigação previstos e utilizados pelos Estados participantes na Convenção do Conselho da Europa sobre a Cibercriminalidade.[16]

Há que se ressaltar, todavia, que a diretiva em comento foi proposta e aprovada após os atentados de Madrid e Londres (2004 e 2005), quando a pressão por investigações ágeis em matéria de terrorismo era latente.

Nesse momento, retoma-se a discussão se a referida diretiva viola direitos fundamentais.

Convém ressaltar que vivemos neste momento uma crescente internacionalização dos serviços de tratamento de dados e a externalização do seu armazenamento – a computação na nuvem (cloudy computing) – e se busca analisar as possibilidades de harmonizar os períodos de conservação de dados em toda a UE. Há uma diversidade de prazos para tal conservação.

A comissão que analisa a diretiva irá estudar a partir de agora a possibilidade de definir períodos distintos em função das diferentes categorias de dados ou das categorias de crimes graves, ou de uma combinação de ambos.[17]

Interessa para nós ressaltar que a experiência da União Europeia, que já possui a diretiva de conservação/preservação de dados há mais de cinco anos, uma vez que tal experiência poderá auxiliar o Brasil na construção de instrumento semelhante. Ainda tratando da referida diretiva, a comissão que a analisou estabeleceu também o valor dos dados conservados em investigações penais ou em processos-crime. Vejamos:

> Foi referido que os dados de tráfego conservados são necessários para contactar testemunhas que, de outro modo, não poderiam ser identificadas, e para fornecer elementos de prova ou pistas para se apurar a cumplicidade na prática de um crime. Alguns Estados-Membros alegaram ainda que a utilização dos dados conservados permitiu ilibar pessoas suspeitas da prática de crimes, sem ter sido necessário recorrer a outros métodos de vigilância, como as escutas telefônicas ou as buscas domiciliárias, considerados mais intrusivos.[18]

4. A preservação de dados e a investigação criminal no Brasil

Atualmente, dois projetos de lei em tramitação no Congresso Nacional tratam do assunto guarda de registros: o PL 84/99 e aquele chamado como Marco Civil da Internet PL 2126/2011.[19] Ambos preveem que somente mediante ordem judicial a guarda dos registros se dará.

A necessidade de obtenção de ordem judicial para a guarda dos registros está na contramão do que na prática ocorre em uma investigação criminal em que há a necessidade de obtenção de logs de acesso, posto que em inúmeros casos, a requisição policial ou ministerial já é suficiente à preservação destes por alguns provedores.

Com relação aos provedores de acesso (SCM) situados no Brasil, não há normativa que estabeleça quem pode requisitar a preservação de dados e nem por quanto tempo esses dados devem ser guardados.

É, em nosso entendimento, perfeitamente possível que o regulamento do SCM também preveja o prazo para a conservação dos dados, uma vez que os projetos de lei atualmente no Congresso Nacional não têm prazo para apreciação. O art. 61 do Regulamento do Serviço de Comunicação Multimídia poderia incluir dispositivo específico com relação ao tema, bem como o prazo em que as SCM devem responder às autoridades quando de posse da requisição ou ordem judicial. Não se trata a disciplina de conservação/preservação dos dados de matéria que atinge a privacidade ou sigilo das comunicações, mas ato meramente regulatório que está no âmbito das atribuições da agência controladora. O aludido art.

16 Disponível em: < http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:PT:PDF>. Acesso em: 30 ago. 2011. p. 5.
17 A proposta de diretiva relativa à conservação de dados apresentada pela comissão em 2005 previa períodos de conservação de dados de um ano para os dados telefônicos e de seis meses para os dados da internet.
18 Ibidem, p. 26.
19 O PL 84/99 determina a guarda dos registros de conexão pelos provedores durante três anos. Já o projeto de marco civil do governo estabelece prazo de apenas um ano, embora ressalte que a Justiça pode determinar o armazenamento por mais tempo.

61 do regulamento já contém dispositivo que remete ao atendimento prioritário a autoridades.

> CAPÍTULO V
>
> Dos Serviços Públicos e de Emergência
>
> Art. 61. As prestadoras de SCM deverão, nos termos do Regulamento dos Serviços de Telecomunicações, atender com prioridade o Presidente da República, seus representantes protocolares, sua comitiva e pessoal de apoio, bem como os Chefes de Estado estrangeiros, quando em visitas ou deslocamentos oficiais pelo território brasileiro, tornando disponíveis os meios necessários para a adequada comunicação destas autoridades.

Recentemente, a Anatel colocou em consulta pública o estabelecimento de regras para a guarda de logs:

> CONSULTA PÚBLICA Nº 46, DE 9 AGOSTO DE 2011
>
> Também coloca em discussão a regulamentação da neutralidade de redes, com vedação ao bloqueio e tratamento discriminatório de tráfego, excetuados os procedimentos que se mostrarem indispensáveis à segurança e à estabilidade do serviço e das redes que lhe dão suporte. Também fica estabelecida a obrigação de guarda dos logs de acesso por três anos (dois anos para os prestadores de pequeno porte), conforme recomendação do Ministério Público Federal. (g.n)[20]

A questão do prazo para o armazenamento dos dados pelos provedores ainda permanece sem solução. Pensamos que ainda no ano de 2012 tal normatização no Congresso Nacional não terá chance de ser votada, restando à própria Anatel avançar, conforme sugerido pelo Ministério Público Federal, regulamentando essa guarda através de resolução, independentemente de previsão legislativa.

5. Condutas típicas e elementos de prova em poder da administração pública

Como dissemos, a necessidade de modernização da administração pública passou obrigatoriamente pela adoção das TICs na sua rotina diária. Cada dia mais os webmails são utilizados para se estabelecer comunicação entre os servidores, entre o público e o prestador de serviço público, aumentando assim o tráfego de informações nas redes das instituições.

Esses dados que trafegam pela rede dos servidores das instituições do poder público, vez ou outra, também podem servir de prova para a elucidação de um crime e comumente, o fornecimento desses dados à autoridade que investiga o delito, esbarra em uma série de dificuldades, que vão desde a não preservação de dados até a falta de regulamentação de como fornecê-los.

Concretamente, citamos o exemplo de um crime que vem se tornando comum: a denunciação caluniosa, que está prevista no art. 339 do CP.[21] Em tempos de proliferação das ouvidorias, diversos são os casos que vemos em que ao servidor público é imputada conduta ilícita, dando início à instauração de investigação administrativa ou investigação policial em face desse mesmo servidor. Ocorre que muitas vezes, a informação/logs de quem enviou e-mail trazendo a imputação ao servidor público, está protegida pelo anonimato (muitas ouvidorias têm a opção de manter os dados do "denunciante" em sigilo) ou quando não se faz a opção pelo sigilo das informações, esses logs simplesmente não são guardadas pelo servidor da instituição do poder público. E, se são guardados, não há regulamentação de para quem devem ser fornecidos, de que maneira e por que prazo devem ser guardados.

Outro exemplo de crime praticado pela web contra os sistemas da administração pública são aquelas condutas previstas nos artigos 313-A e 313-B.

Os primeiros crimes cibernéticos ditos "puros ou próprios" que foram tipificados na legislação brasileira visam à proteção dos sistemas informatizados da administração pública. São aqueles previstos nos artigos 313-A e 313-B do Código Penal.[22] O incremento da ocorrência destes crimes – de inserção, modificação, exclusão de dados falsos em sistemas informatizados em bancos de dados da administração pública – começa a preocupar as autoridades encarrega-

20 Disponível em: <http://www.anatel.gov.br/ >. Acesso em: 12 out. 2012.

21 Art. 339. Dar causa à instauração de investigação policial, de processo judicial, instauração de investigação administrativa, inquérito civil ou ação de improbidade administrativa contra alguém, imputando-lhe crime de que o sabe inocente: (Redação dada pela lei nº 10.028, de 2000) Pena - reclusão, de dois a oito anos, e multa.§ 1º - A pena é aumentada de sexta parte, se o agente se serve de anonimato ou de nome suposto.§ 2º - A pena é diminuída de metade, se a imputação é de prática de contravenção.

22 Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000))Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Incluído pela Lei nº 9.983, de 2000). Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000)Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa (Incluído pela Lei nº 9.983, de 2000).

das na persecução penal, justamente porque não será possível a identificação e comprovação da autoria desse crime se não for fornecido ao investigador – pelo próprio administrador da rede ou do sistema violado – os logs de acesso que permitiram a ocorrência da modificação ilícita.

6. Considerações finais

Neste ensaio nosso objetivo foi o de trazer à discussão questões que envolvem legado informacional da administração pública. O recorte escolhido foi a questão da guarda de logs que servirão de prova para elucidar a autoria da prática de crimes. Primeiramente, há que se reafirmar a necessidade de se disciplinar o prazo para a guarda de logs para a garantia das investigações criminais que envolvem, de qualquer forma, condutas pela internet ou sistemas informatizados. O crescimento de atividades como o comércio eletrônico, a implantação do sistema de Nota Fiscal Eletrônica, os cursos on-line, a rede bancária, as polícias, para citar somente alguns são atividades que acabam servindo, cedo ou tarde, cenário para a prática de condutas criminosas. Daí a urgência da disciplina da matéria.

No que tange ao serviço público, verifica-se que há um verdadeiro tabu em se tratar do tema guarda de logs. Aparentemente, a possibilidade de se obter logs de acesso de atividade ocorrida em um servidor (de rede) da administração pública soa como uma verdadeira possibilidade de estabelecimento de certa "vigilância", o que é, claro, rechaçado por todo cidadão. Assim é que urgente que a administração pública atente para essas questões, mesmo porque os investigadores – que também são servidores públicos – são aqueles que justamente sabem da importância da obtenção do dado informático para elucidar um crime. E essa disciplina não se deve resumir apenas na previsão do prazo e forma de guarda desses logs, mas, sobretudo, a maneira que esta se dará, em quais hipóteses e para quais autoridades, mediante simples requisição para quem tiver o poder de requisitar ou mediante ordem judicial.

Acreditamos que a partir dessa normatização, a administração pública estará dando o exemplo à iniciativa privada e mais, trazendo a possibilidade de ser transparente, observados os parâmetros legais – quer dizer, sem receio de ferir o direito constitucional à privacidade.

Referências

BRESSER-PEREIRA, Luiz Carlos. *Reforma da nova gestão pública: agora na agenda da América Latina*. Revista do Serviço Público. Brasília: Fundação Escola Nacional de Administração Pública, jan./mar. 2002.

CAPEZ, Fernando. *Curso de Processo Penal*. 12. ed. São Paulo: Editora Saraiva, 2005.

CORRÊA, Gustavo Testa. *Aspectos jurídicos da internet*. São Paulo: Saraiva, 2000.

FERREIRA, apud Ivett e Senise. *A criminalidade informática,* Direito e Internet - Aspectos jurídicos relevantes. Editora Edipro, 2001.

GOMES, Luiz Flávio. *Atualidades criminais*. Disponível em www.direitocriminal.com.br.

GRECO, Rogério. *Curso de Direito Penal* - Parte Especial. Ed. Impetus, 2006.

INELLAS, Gabriel César Zaccaria de. *Crimes na internet*. São Paulo: Juarez de Oliveira, 2004, p. 80.

JÚNIOR, Jose Calda Gois. *O Direito na Era das Redes – A Liberdade e o delito no Ciberespaço*. Ed. Edipro, 2001.

LIMA DE LA LUZ, Maria. *Delitos informáticos*. México DF: Criminalia. Academina Mexicana de Ciencias penales. Ed. Porrua, 1984.

LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. Ed. Milenium, 2005. p. 36, 51, 105.

NETO, Marcílio José da Cunha. *Manual de Informática Jurídica*. Ed. Destaque, 2002. p. 200.

PINHEIRO, Patrícia Peck. *Direito Digital*. 4. ed. São Paulo: Editora Saraiva, 2010.

ROHRMANN, Carlos Alberto. *Curso de Direito Virtual*. Ed. Del Rey, 2005. p. 120, 137, 181, 199 e 215.

ROSA, Fabrizio. *Crimes de Informática*. Ed. BookSeller, 2002. p. 49 e 63.

ROSSINI, Augusto Eduardo de Souza. *Brevíssimas considerações sobre delitos informáticos*. Caderno Jurídico Direito e Internet. São Paulo: Imprensa Oficial do Estado. Escola Superior do Ministério Público. 2002.

Fortalecimento de segurança cibernética: uma das prioridades da OEA e da América Latina

Divulgação

Belisario Contreras

Administrador de empresas pela Universidade Francisco de Paula Santander (UFPS), na Colômbia, e mestre em Estudos Latino-Americanos pela Escola de Serviço Exterior Edmund A. Walsh da Universidade de Georgetown, em Washington DC, EUA. Atualmente é gerente do Programa de Segurança Cibernética na Secretaria do Comitê Interamericano contra o Terrorismo (CICTE), pertencente à Organização dos Estados Americanos (OEA).

RESUMO

O uso da internet cresceu exponencialmente nos últimos dez anos, o que trouxe todo tipo de oportunidades para o mundo inteiro, especialmente para as comunidades da América Latina e do Caribe. Se por um lado a internet facilita a difusão da informação e a conectividade entre as pessoas, por outro ela põe em evidência as vulnerabilidades e as ameaças que esse tipo de conectividade traz, tanto em nível nacional como internacional.

O perigo que se corre com a massificação da internet fez com que os Estados-Membros da Organização dos Estados Americanos (OEA) começassem a desenvolver políticas e estratégias para combater essas ameaças, conforme o que foi acordado na Estratégia Interamericana de Segurança Cibernética adotada em 2004.

Nos últimos dez anos, os países da América Latina e do Caribe têm experimentado uma das maiores taxas de crescimento de usuários de internet em todo o mundo. Se olharmos para a maioria dos países da América Central e do Sul, percebemos uma taxa de crescimento de 1.000% e, ainda em dívida, uma taxa de crescimento de quase 1.400% na região do Caribe, enquanto outras regiões do mundo, como a Ásia e a Europa estão crescendo a taxas de 400% e 700%, respectivamente.[1]

O aumento de usuários de internet, e especialmente o benefício que obtemos dessa ferramenta, tem produzido um rápido aumento nas oportunidades na região e transformou a "Rede" em uma das plataformas que tornou possível dar um grande salto para o governo eletrônico, a interação social, a educação a distância, o comércio eletrônico e, até mesmo, podemos ousar dizer que aumentou a qualidade de vida dos cidadãos de ambas as Américas e ao redor do mundo. Desde os cybercafés até os smartphones, o uso da internet está sendo modificado e massificado para todo tipo de usuários no hemisfério. Especificamente no caso dos smatphones, a média do uso entre os usuários é de 17%, enquanto a média global de uso de smartphones é de 27%, o que sugere que esse tipo de tecnologia tem potencial de crescimento na região. Apesar de que uma maior penetração da internet tem trazido muitos benefícios para a nossa sociedade, esse desenvolvimento também trouxe vulnerabilidades e ameaças que podem comprometer as boas intenções do desenvolvimento da Tecnologia da Informação e Comunicação (TIC).

A evolução de ameaças cibernéticas para os governos, o setor privado e a sociedade civil, e, acima de tudo, o seu potencial para criminosos e até mesmo terroristas, provocou uma reação dos desenvolvedores de políticas estatais e outras partes interessadas relevantes na América Latina e Caribe, considerando a necessidade de desenvolver novos mecanismos, estratégias e políticas públicas para combater essas ameaças. Por esse motivo, há cerca de dez anos, os Estados-Membros da Organização dos Estados Americanos (OEA) decidiram começar a discutir, no seio desses mecanismos, ações

1 Cf. http://www.coha.org/the-internet-and-latin-america-the-rise-of-the-virtual-world-and-emerging-cyber-security-issues.

que permitiriam à região estar mais bem preparada para responder a novos desafios cibernéticos.

Uma das principais respostas dos Estados-Membros da OEA foi a aprovação, em 2004, da "Estratégia Integral Interamericana de Segurança Cibernética", com uma abordagem multidimensional e multidisciplinar para a criação de uma cultura de segurança cibernética no hemisfério[2]. A adoção dessa "estratégia" é talvez um dos êxitos políticos – e de consensos – mais significativos que a região tem em relação ao ciberespaço. É importante notar que até agora nenhuma outra região do mundo tem um instrumento dessa natureza, até a Europa ainda está desenvolvendo uma estratégia cibernética para a região[3]. Em termos gerais, a estratégia de segurança cibernética interamericana tem três objetivos principais:

a) a formação de um observatório interamericano de aviso para a divulgação rápida de informações sobre segurança cibernética e a resposta a crises, incidentes e ameaças à segurança, para a qual é necessária a criação da Equipe de Resposta para Incidentes de Seguridade Cibernética (CSIRTs, na sigla em inglês) em cada país da região;
b) identificação e adoção de normas técnicas para arquitetura da internet segura;
c) certificar que os Estados-Membros da OEA tenham os instrumentos jurídicos necessários para proteger os usuários de internet e redes de informação.

Poderíamos dizer que, como resultado dessa estratégia, a maioria dos países das Américas começou a tomar consciência das necessidades de cada um em se tratando de segurança cibernética. Nós podemos ver com muita satisfação como em 2004 tínhamos formalmente constituído apenas quatro CSIRTs. Em 2012, o número que os Estados-Membros têm relatado é de 17 CSIRTs, com perspectivas de aumentar, especialmente na região da América Central. É importante notar que não podemos padronizar e medir todas essas equipes de resposta na região da mesma forma, dado que, pelo menos em cibernética, cada um dos nossos Estados teve (e terá) que viver processos de maturidade e desenvolvimento completamente diferentes. Por exemplo, em um país como o Brasil, por um lado, nós podemos encontrar pelo menos 35 CSIRTs[4] que estão espalhadas por todo o país, abrangendo várias áreas do Estado, desde o setor de governo, passando pela academia, até o setor financeiro. Essa presença reflete claramente o alto nível de avanço e de conscientização sobre a importância de proteger as redes não apenas do governo, mas também do setor privado e da sociedade civil. Por outro lado, podemos ver que há outros países da região em que só nos últimos anos começaram a dar maior prioridade a essa questão, e ainda que haja um desejo, eles não têm uma estrutura robusta para prevenir e dar uma resposta eficaz aos incidentes cibernéticos que enfrentamos todos os dias.

É importante observar que, embora a criação e o desenvolvimento de CSIRTs permitam responder de forma mais eficaz aos incidentes cibernéticos, de qualquer forma não podemos dizer que com essas organizações os riscos aos quais nossa sociedade está exposta com o uso da internet vão desaparecer. Paradoxalmente, a maioria dos especialistas na região reconhece que tais estruturas implementadas dentro de um país, ou mesmo dentro de uma organização, são mais uma prova do grande número de riscos e vulnerabilidades aos quais os governos, empresas e utilizadores estão expostos. Por exemplo, a Symantec publicou no seu relatório anual desse ano que "o número de vulnerabilidades diminuiu 20 por cento, (mas que) a quantidade de ataques maliciosos incrementou 81 por cento".[5] Esse resultado mostra que os esforços dos diferentes atores da segurança cibernética estão fazendo um bom trabalho, mas não podem baixar a guarda, porque mais ameaças são detectadas e outras ameaças novas emergem, requerendo um esforço contínuo da parte dos usuários.

A fim de continuar com o posicionamento da segurança cibernética como um dos principais problemas da região, no dia 7 de março passado, todos os Estados-Membros da OEA reafirmaram seu compromisso de reforçar a sua capacidade para enfrentar essas ameaças novas e decidiram adotar (de maneira consensual) a declaração "Reforço de Segurança Cibernética nas Américas",[6] por meio da qual se reafirma e se reconhece o impacto potencial das ameaças à segurança cibernética e as vulnerabilidades para os Estados-Membros da OEA. Da mesma forma, todos os Estados-Membros do Comitê Interamericano contra o Terrorismo (Cicte) reconheceram a importância

2 Cf. http://oas.org/cyber/documents/AG-RES.%202004%20Cyber%20Security%20Strategy%20 (complete).pdf.
3 Cf. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper.
4 Cf. http://www.cert.br/csirts/brazil/.
5 Cf. http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20120503_01.
6 Cf. http://oas.org/cyber/documents/Declaration.pdf

de promover a cooperação do setor público com o setor privado e acadêmico para fortalecer a salvaguarda e proteção da infraestrutura crítica de informação e comunicações. Esse último reconhecimento é fundamental, porque ele destaca que até certo ponto todos os jogadores participantes na internet têm uma responsabilidade partilhada e isso é essencial para compartilhar e coordenar os vários esforços.

Sem minimizar o grande valor que tem a Estratégia de 2004, bem como a Declaração de 2012, gostaria de deixar claro que esses instrumentos são úteis, desde que cada um dos nossos países assim os considerem. Nos últimos anos, tornou-se muito claro que sempre que exista vontade será possível encontrar uma alternativa para desenvolver as habilidades necessárias para cumprir os compromissos assumidos por cada um dos Estados. É importante ter em mente que o primeiro passo é sempre a parte mais difícil de toda a estrada, mas uma vez que a ideia exista, haverá vários recursos e iniciativas para promover e sustentar esses esforços. A OEA é um desses recursos. Para dar um exemplo, na legislação, o "Grupo de Crime Cibernético" (Remja) vem usando um modelo colaborativo, no qual o conselho é dado a diferentes países na região, possibilitando o desenvolvimento e a adoção de legislações que permitam processar os crimes cibernéticos de maneira mais fácil, tanto nacional como internacionalmente. Além disso, esse grupo tem fornecido treinamento para juízes, procuradores e policiais sobre como lidar com esses tipos de crimes e conduzir o que o processo requer. Esforços similares são conduzidos através do Comitê Consultivo Permanente I (CCP) da Comissão Interamericana de Telecomunicações (Citel), em que a discussão e as recomendações promovem o debate e o desenvolvimento de novas tecnologias, a fim de compreender como os países da região estão criando quadros normativos para estimular a infraestrutura e a inovação, de modo que eles recebam novos serviços em um ambiente de segurança jurídica, concorrência saudável e condições tecnológicas em evolução.

Como mencionado acima, a Secretaria do Cicte, através do seu programa de segurança cibernética, teve, talvez, um dos papéis mais ativos no hemisfério em termos de promoção desses recursos. Embora o desenvolvimento de CSIRTs na região tenha sido um dos pilares desse programa, o trabalho que vem se desenvolvendo na região deixou claro que, assim como era necessário ter uma estratégia regional sobre segurança cibernética, é necessário que os nossos países tenham políticas, estratégias ou uma visão completamente clara sobre quais são os passos a serem seguidos nacionalmente. Portanto, nos últimos anos, a OEA/Cicte vem atuando em alguns países, promovendo o desenvolvimento de políticas e estratégias nacionais de segurança cibernética. Esse processo já foi iniciado em países como Antígua e Barbados, Colômbia, Chile, México, Panamá e Trinidade e Tobago, entre outros.

Tomando a Colômbia como um exemplo, mostramos como esse país, além de ver a necessidade de desenvolver o seu CSIRT nacional, reconheceu a necessidade de estabelecer uma estratégia ou "Política Nacional de Segurança e Defesa Cibernéticas".[7] Sendo assim, delineou a criação do Grupo de Resposta a Emergências Cibernéticas da Colômbia (Colcert) e um Comando Conjunto Cibernético (CCOC), o qual é responsável pela defesa cibernética do Estado colombiano. A parte mais interessante deste trabalho é que, além de reconhecer que há carência em "institucionalidade" adequada, centra-se na necessidade de reforçar os instrumentos legislativos e de cooperação internacional e promover a pesquisa e a formação adequada para o país frente a essas ameaças.

Embora as estratégias nacionais sejam um veículo muito importante para promover a coordenação através de um país, eu acho muito importante notar que os riscos estão mudando e precisam ser revistos, se necessário atualizando essas estratégias e políticas cibernéticas. Mais uma vez, é claro que as estratégias ou políticas nacionais não são as soluções definitivas para os nossos "problemas cibernéticos", mas ajudam a ter uma boa definição dos papéis de cada um dos atores, e, acima de tudo, ter uma melhor organização, característica fundamental das pessoas que apresentam nossas maiores ameaças. Se observarmos alguns dos incidentes cibernéticos ocorridos durante a última década, como, por exemplo, o cyber ataque à Estônia em abril de 2007[8], o ataque à SK Communications na Coréia do Sul em julho do 2011[9] e o recente ataque aos bancos estadunidenses em setembro deste ano[10], podemos facilmente mostrar que, para eles terem sido capazes de existir, é essen-

7 Cf. http://www.dnp.gov.co/LinkClick.aspx?fileticket=-lf5n8mSOuM%3D&tabid=1260
8 Cf. http://www.guardian.co.uk/technology/2007/may/18/news.russia?INTCMP=ILCNETTXT3487.
9 Cf. http://www.commandfive.com/papers/C5_APT_SKHack.pdf.
10 Cf. http://newyork.newsday.com/business/pnc-bank-wells-fargo-u-s-bank-hacker-attacks-planned-for-weeks-experts-say-1.4051463.

cial ter uma organização e, acima de tudo, um suporte intelectual e econômico que permita o seu acionar. Um dos grandes desafios que têm, tanto os governos como o setor privado, é a habilidade de contra-atacar o desenvolvimento de agrupações dedicadas a obstruir os fins de conectividade e, acima de tudo, evitar que os cidadãos com qualidades e habilidades excepcionais no uso da tecnologia acabem do lado errado.

É claro que, a fim de lidar com qualquer tipo de crime, é necessário contar com uma institucionalidade e um quadro normativo adequado, permitindo uma ação correspondente. Não obstante, mais importante ainda é desenvolver iniciativas para prevenir e antecipar as ameaças cibernéticas. Para isso, é essencial investir no desenvolvimento de programas de treinamento para os usuários finais, na criação de mecanismos de avaliação de vulnerabilidade, no trabalho coordenado com as empresas prestadoras de serviços de internet e nas ferramentas para criar mecanismos eficazes de coordenação entre diferentes atores. Em nosso hemisfério, estamos mostrando que essas iniciativas estão começando a dar resultados bastante alentadores.

Na prevenção de usuários finais da internet, países como Argentina, Brasil, Canadá, Chile, Colômbia, Estados Unidos, México, Uruguai e Venezuela, para citar alguns, começaram a desenvolver campanhas, com o apoio do setor privado, a fim de alertar os cidadãos de todas as idades os riscos e as ameaças que correm se não usarem as TICs de forma responsável. Uma proposta interessante a esse respeito é a iniciativa do "Pare. Pense. Conecte-se",[11] a qual procura unificar as diferentes mensagens de prevenção que os usuários estão recebendo diariamente. Além dessa, o Fórum Econômico Mundial (WEF) está promovendo uma iniciativa chamada "Parcerias para Resiliência Cibernética",[12] o que é certamente notável, considerando que essa organização é composta por líderes importantes tanto do setor privado quanto do Governo.

Poderíamos dizer que a América Latina e o Caribe estão no momento certo para realizar os ajustes necessários para reforçar as infraestruturas críticas de informação de nossos países. Todos os dias há mais serviços, instituições e dispositivos que começam a se interligar e, se não agir como esperado, nós nos encontraremos diante de uma grande rede que pode em breve se tornar uma bolha. O ciberespaço não está respeitando os limites e barreiras da realidade virtual. Apenas alguns anos atrás, pensávamos que os sistemas de controle industrial (ICS) eram talvez os mais seguros e impenetráveis. No entanto, a evidência de incidentes cibernéticos com esse tipo de infraestrutura conseguiu chamar a atenção das empresas prestadoras de energia, serviços de água, transporte de massa, entre muitas outras organizações que permitem que nosso dia a dia seja completamente normal e calmo. Dado o desenvolvimento de ameaças virtuais sofisticadas, bem como o crescente número de ameaças avançadas persistentes (APT), é evidente e necessário que os setores identificados como "infraestrutura crítica" tenham que prestar atenção especial aos problemas do ciberespaço, não apenas pelo impacto financeiro que um incidente de grande escala poderia ter em cada uma dessas instituições, porém, mais importantes ainda, pela dependência que a sociedade tem desses serviços, os quais poderíamos denominar como vitais.

É claro que nossos Estados estão começando a tomar as medidas adequadas para alcançar as metas de segurança cibernética descritos na Estratégia de 2004 e na Declaração de 2012. Ao longo dos últimos anos, a maioria dos países do hemisfério ocidental tem tomado medidas concretas para melhorar as capacidades cibernéticas, seja estabelecer um CSIRT, adotar uma política cibernética nacional, ou talvez uma avaliação modesta, mas importante, sobre as capacidades atuais. A internet tem sido um veículo importante para a inovação e o crescimento econômico, tendo um impacto positivo em todos os cidadãos das Américas. Para ser capaz de continuar aproveitando as oportunidades que a internet apresenta, devemos nos manter na vanguarda da luta para proteger as redes hemisféricas. Para isso, os Estados-Membros da OEA devem estar atualizados nas mais recentes ameaças cibernéticas e desenvolvimentos relacionados. Temos de aceitar que o caminho para redes seguras nunca termina. Nós não vamos estar completamente seguros, mesmo com as CSIRTs em vigor ou as estratégias nacionais aprovadas. Novas ameaças estão sempre surgindo, criando a necessidade de novas formações, novas políticas e partilha permanente de informações e melhores práticas. O momento é perfeito para os governos fazerem um balanço das capacidades existentes, coordenarem esforços e avançarem juntos. A partir do trabalho em conjunto e da reunião do nosso conhecimento, os cidadãos e as empresas vão colher os frutos de nossos esforços coletivos.

11 Cf. http://stopthinkconnect.org/.
12 Cf. http://www.weforum.org/issues/partnering-cyber-resilience-pcr.

Alta disponibilidade de serviços de redes baseada na utilização de cluster implementado por meio de software livre


Divulgação

Evandro Nicomedes Araujo

Mestre em Administração Pública com ênfase em Gestão da Informação pela Fundação João Pinheiro (FJP) e especialista em Redes de Telecomunicações pela UFMG. Atua como analista de suporte a redes de comunicação de dados da Prodemge desde 1994. Professor dos cursos de Ciência da Computação e de Gestão da Tecnologia da Informação no UNI-BH.


Divulgação

Alberone Rodrigues de Lima

Formado em Gestão da Tecnologia da Informação pelo Centro Universitário de Belo Horizonte (UNI-BH). Gestor da área de TI do escritório Pinto & Soares Advogados Associados.

RESUMO

O objetivo deste artigo é fazer um estudo prático (técnico) a respeito do comportamento da continuidade do fluxo de transferência de dados executada por serviços de rede em uma solução de cluster de alta disponibilidade. Para se alcançar o objetivo proposto, será implementado um cluster de alta disponibilidade com dois computadores e se disponibilizará um terceiro computador, que servirá como cliente para se executar as transferências de arquivos que estão disponíveis nos servidores do cluster, usando protocolos de rede HTTP e FTP. Uma ferramenta de escuta de rede (sniffer/Wireshark) será utilizada para se verificar o fluxo de informações durante a transferência dos arquivos, quando da comutação entre as máquinas que compõem o cluster. Verificou-se que a solução de alta disponibilidade de cluster não apresentou continuidade no fluxo de informações, tendo em vista que, no caso de falha do servidor primário, o processo de transferência de dados executada via HTTP ou FTP no momento da falha se perde e, após a falha, o processo de transferência deve ser iniciado novamente, pelo controle do protocolo de transporte Transmission Control Protocol (TCP).

1. Introdução

As soluções de cluster de alta disponibilidade se mostram atraentes devido ao seu bom desempenho aliado ao seu baixo custo, principalmente para empresas com recursos financeiros escassos. Denomina-se cluster o agrupamento de dois ou mais computadores trabalhando em conjunto, executando tarefas, aplicações ou disponibilizando serviços, que se apresenta para o usuário como um único computador de forma individual (PITANGA, 2003).

Clusters podem ser utilizados em aplicações para sondagem de petróleo em águas profundas, na área da medicina, biologia, processamento de imagens, etc., tudo que exija grande poder de processamento, apresentando um custo bem inferior se comparado ao uso de supercomputadores. Podem ser de processamen-

to dedicado (cluster Beowulf[1]) e não dedicado, em que o processamento é realizado de acordo com a ociosidade das estações de trabalho (cluster Openmosix[2]) (PITANGA, 2004).

Segundo Pitanga (2004), as soluções de clusters de alta disponibilidade, balanceamento de carga e de processamento distribuído têm em suas características conceitos, aplicação, implementação e vantagens frente aos supercomputadores. Algumas das características elencadas são: baixo custo, flexibilidade, escalabilidade, fácil manutenção e substituição de componentes, independência de fornecedores. Em Pereira (2005), pode-se examinar uma proposta de solução de cluster de alta disponibilidade utilizando-se sistema GNU/Linux e ferramentas livres Drbd e Heartbeat, o que corrobora a crescente utilização de software livre para implementações de soluções de cluster de alta disponibilidade. Importante ressaltar que há diferentes tipos de abordagem para soluções de cluster, por exemplo: alta disponibilidade, balanceamento de carga e processamento distribuído. Entretanto, este artigo se deterá na solução de cluster de alta disponibilidade conforme proposta por Pereira (2005).

Diante desse contexto, este artigo tem como objetivo geral fazer um estudo prático (técnico) a respeito do comportamento da continuidade de serviços de rede em uma solução de cluster de alta disponibilidade. Entende-se por continuidade de serviços de rede a não interrupção do fluxo de informação durante as transferências de dados entre um computador cliente e outro servidor.

Especificamente, pretende-se:

a) implementar um laboratório de informática composto por três computadores, uma rede fast-ethernet[3], que servirá de infraestrutura de rede para o funcionamento de uma solução de cluster de alta disponibilidade, que disponibilizará dois serviços de rede: hipertext transfer procolol (HTTP[4]) e file transfer protocolol (FTP[5]) configurados e implementados a partir de ferramentas livres;

b) verificar (observar) o comportamento do fluxo das informações transferidas por esses serviços de rede, quando da comutação dos hosts[6] que fazem parte do cluster de alta disponibilidade. Entende-se, aqui, como fluxo de informações, todos os dados ou informações transferidas fim a fim entre dois hosts de uma rede através do uso de qualquer dos serviços elencados, no caso deste estudo, a transferência entre uma estação de trabalho/cliente e o cluster implementado.

Cabe ainda ressaltar que se acredita que não há interrupção do fluxo de informações desses serviços, caso haja uma interrupção de uma dos hosts que fazem parte do cluster de alta disponibilidade. Este artigo parte da hipótese de que a alta disponibilidade das soluções livres de cluster ocorre em todos os níveis inclusive no nível de protocolos de redes, não ocasionando a descontinuidade do fluxo de informações nas transferências de dados entre hosts da rede e os hosts do cluster, quando da comutação do mesmo. Para efeitos deste artigo, entende-se como comutação dos hosts do cluster a interrupção, por quaisquer motivos e em qualquer nível, do funcionamento do host principal do cluster, de forma que todos os serviços oferecidos por este host tenham que ser comutados ou transferidos para o outro host que compõe a solução de cluster.

2. Metodologia

Quanto ao tipo de abordagem, esta pesquisa pode ser compreendida como uma pesquisa de natureza experimental, de campo. Por acreditar que a solução de clusters de alta disponibilidade mantém o fluxo de informações dos arquivos transferidos por serviços de redes, a exemplo de FTP, HTTP, funcionando sem nenhum grau de interrupção durante a comutação entre os hosts que fazem parte do cluster, optou-se por montar um laboratório de informática para se fazer as observações e análises necessárias com a finalidade de corroborar ou refutar tal hipótese.

Esses serviços de rede foram escolhidos estrategicamente, a partir do tipo de protocolo de rede que utilizam, e são capazes de promover transferência de arquivos de tamanhos maiores, possibilitando, dessa forma, condições para que se possa observar, através de ferramentas de escuta na rede Wireshark[7] (*sniffers*), o comportamento do fluxo de informações ou a transferência das informações durante a comutação entre os hosts que compõem o cluster.

As ferramentas de escuta de rede são amplamente utilizadas com ob-

1 Cluster constituído de vários nós escravos e um nó controlador (PITANGA, 2004).
2 Projeto de código aberto baseado no Mosix (Multicomputer Operating System Unix) (PITANGA, 2004).
3 Especificação para rede ethernet com transmissão de dados de cem megabits (MORIMOTO, 2004).
4 Protocolo utilizado para acesso a páginas web (MORIMOTO, 2004).
5 Protocolo usado para transferir dados através de redes TCP/IP (MORIMOTO, 2004).
6 Máquinas que pertencem a uma rede.
7 Cf. http://www.wireshark.org/.

jetivo de se verificar o tráfego nas redes de computadores. Com elas é possível capturar todos os pacotes[8] que trafegam na rede, de forma a poder analisá-los, verificando, assim, o comportamento do fluxo de informações nas redes. O Wireshark é uma ferramenta de análise de protocolos de rede, conhecida anteriormente pelo nome Ethereal.

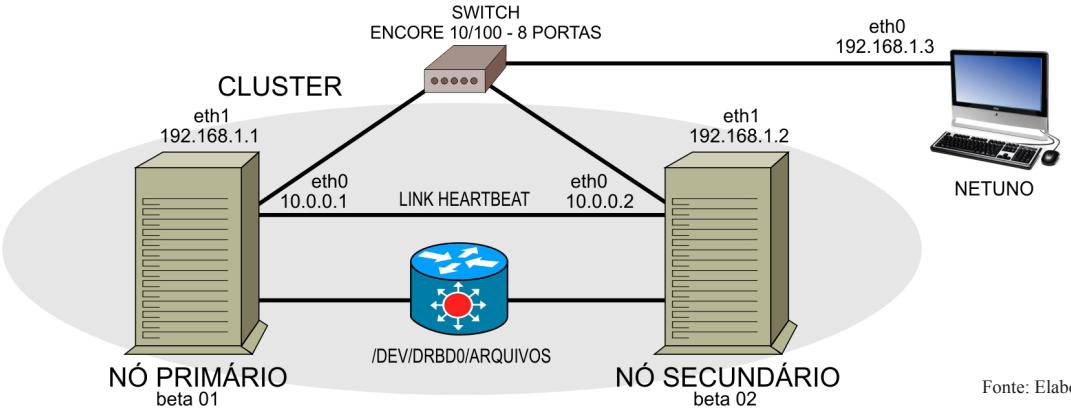
Para tal constatação, foi montado um laboratório de informática, composto por três computadores interligados por uma rede fast-ethernet:

Configuração das máquinas do cluster:

- servidor primário (ativo) do cluster (beta01);
  - endereço IP 192.168.1.1 (interface eth0[9]);
  - endereço IP 10.0.0.1 (interface eth1[10]) link[11] Heartbeat;
  - processador AMD Athon 850 Mhz;
  - memória 128 MB, sendo 8 compartilhada para vídeo disco rígido de 20GB Seagate;
  - placa de vídeo PCI Nvidia Vanta 16MB;
  - placa mãe ASUS A7S-VM (som, vídeo e rede onboard);
  - placa de rede onboard Realtek 8139 (nomeada no Linux como eth0);
  - placa de rede Encore – chipset Realtek 8139 (nomeada no Linux como eth1);
  - sistema operacional Ubuntu Server 6.06.1 LTS.
- servidor secundário (passivo) do cluster (beta02)
  - endereço IP 192.168.1.2 (interface eth0);
  - endereço IP 10.0.0.2 (interface eth1) link Heartbeat;
  - processador AMD Athon 850 Mhz;
  - memória128 MB, sendo 8 compartilhada para vídeo;
  - disco rígido de 20GB Seagate;
  - placa de vídeo PCI Nvidia Vanta 16MB;
  - placa mãe ASUS A7S-VM (som, vídeo e rede onboard);
  - eth0 placa de rede onboard Realtek 8139;
  - eth1 placa de rede Encore – chipset Realtek 8139;
  - sistema operacional Linux Ubuntu Server 6.06.1 LTS.

Configuração da máquina de onde se fizeram os testes:

- Máquina cliente:
  - processador AMD Sempron 2600+;
  - memória 512 DDR 266;
  - Ubuntu 7.10 Gutsy;
  - placa mãe Pcchips A31G;
  - vídeo onboard Silicon Integrated Systems [SiS] 661/741/760 PCI/AGP;
  - eth0 placa de rede onboard Via-Rhine ;
  - eth1 Silicon Integrated Systems [SiS] 190 Gigabit Ethernet Adapter;
  - endereço IP 192.168.1.3;
  sistema operacional Linux Ubuntu 7.10 Gutsy Gibbon.
- Configuração da rede:
  - switch[13] 10/100 Encore ENH 908-NWY;
  - cabos UTP[14] categoria 5[15].
- Ferramentas de software utiliza-



Fonte: Elaborada pelos autores

Figura 1 - Sistema de alta disponibilidade com dois servidores sendo acessados por um cliente[12]

8 Informações enviadas em uma rede podem ser divididas em partes de tamanho definido, sendo cada parte um pacote (MORIMOTO, 2004).
9 Forma como é referenciada a primeira interface de rede no Linux.
10 Forma como é referenciada a segunda interface de rede no Linux.
11 Neste caso é canal de interligação entre os computadores.
12 Um dos servidores é primário (ativo) host beta01 e outro secundário (passivo) host beta02.
13 Dispositivo concentrador em que são ligados os computadores da rede.
14 Cabo par trançado sem blindagem. (MORIMOTO, 2004).
15 Qualificação quanto à qualidade e capacidade de transmissão de dados, podem ser usados em redes ethernet de dez e cem megabits. (MORIMOTO, 2004).

das: (mais detalhes serão expostos adiante)

- Heartbeat-2 2.0.2-5, instalado no cluster;
- DRBD 0.7, instalado no cluster;
- Proftpd 1.2.10-27Ubuntu, instalado no cluster;
- Wireshark Version 0.99.6, instalado na máquina cliente (netuno);
- Ping, instalado na máquina cliente (netuno).

3. O conceito de cluster

A tecnologia de cluster surgiu com o projeto Sage[16] (Semi-Automatic Ground Environment), construído pela IBM[17] (International Business Machines) para o Norad[18] (Nort American Air Defense), começando a operar em 1962, formado por diversos sistemas separados que trabalhavam de forma cooperativa com intuito de monitorar invasões aéreas no continente norte-americano. Em 1994, é criado o cluster Beowulf, desenvolvido pela Nasa[19] (National Aeronautics and Space Administration), construído com computadores comuns disponíveis no mercado (16 máquinas Intel 486 – 100 MHZ), atingindo a marca de 70 megaflops[20], com um valor total de construção de US$ 40.000,00, ou seja, 10% do preço de uma máquina comercial com desempenho equivalente (PITANGA, 2004).

Os clusters podem ser de processamento dedicado, a exemplo o cluster Beowulf, e de processamento não dedicado, que é realizado de acordo com a ociosidade das estações de trabalho, nesse caso temos o exemplo do Openmosix.

Como exemplo de sucesso no uso de cluster de alta disponibilidade, podemos citar o Google, que é uma ferramenta de busca na internet, que mantém cluster de servidores em suas centrais. A solução que utilizam agrega alta disponibilidade e balanceamento de carga.

4. Principais tipos de cluster

a) alta disponibilidade – caracteriza-se por um sistema com funcionamento desejável de 24 horas por dia, sete dias por semana, garantindo a continuidade dos serviços, ainda que haja falhas em um ou mais dispositivos, tanto em termos de hardware[21] como de software[22]. Esse tipo de solução utiliza técnicas de replicação de arquivos e serviços, e redundância de hardware e software. Segundo Pitanga (2004, p. 24), "um servidor de boa qualidade apresenta uma disponibilidade de 99,5%, enquanto uma solução através de clusters de computadores apresenta uma disponibilidade de 99,99%".

b) cluster de alta performance de computação – envolve as condições de processamento paralelo e processamento distribuído, provendo um processamento de alto desempenho para solução de problemas computacionais em diversas áreas. Um cluster de processamento paralelo tem como principal característica a de que a cada novo processo inicializado, o cluster o divide entre os computadores. Utilizando essa tecnologia, o tempo de término de processamento torna-se consideravelmente menor do que se fosse realizado em um único computador.

c) cluster de balanceamento de carga – tem como principal finalidade distribuir de forma equilibrada a carga de informações (tarefas) entre servidores para que, no grupo de servidores, um único servidor não fique sobrecarregado e outros sem carga, tornando as respostas de requisições mais rápidas e proporcionando um melhor uso do hardware.

5. Funções das ferramentas livres DRBD, Heartbeat

Distributed Replicated Block Device (DRBD) responsável pela replicação dos dados gravados no disco rígido entre os nós/nodos[23] do cluster. A sincronização dos dados é feita bit[24] a bit, tudo que for escrito no dispositivo de bloco virtual que é criado pelo DRBD será escrito no disco rígido do servidor primário/ativo e servidor secundário/passivo.

A funcionalidade Heartbeat é responsável pela verificação do funcionamento dos nós/nodos e pela

16 Em português: ambiente terreno semiautomático.
17 Empresa norte-americana.
18 Em português: Departamento de Defesa Aérea Norte-Americano.
19 Em português: Administração Nacional Aeronáutica e Espacial.
20 Um milhão de operações de ponto flutuante por segundo.
21 Partes físicas do computador (placas, processador, disco rígido etc.).
22 Parte lógica, conjunto de instruções e dados (sistema operacional, programas etc.).
23 Forma como é identificado cada computador interligado ao cluster.
24 Dígito binário, menor unidade de informação (pode ter os valores 0 ou 1)(MORIMOTO, 2004).

comutação dos serviços entre os servidores que compõem o cluster. Trabalha com envio de pacotes para verificação do funcionamento das máquinas do cluster. Conforme seu desenvolvedor, Alan Robertson, o mesmo "traz tecnologias e funções que se igualam ou mesmo superam as de muitos sistemas comerciais de HA (High Availability)[25]".

6. Vantagens e desvantagens de uma solução de cluster de alta disponibilidade

A um custo razoavelmente baixo (em torno 10% de uma solução comercial), tanto na implementação quanto na sua manutenção, pode-se prover um sistema de alta disponibilidade de uma forma simples e de desempenho que pode ser comparado ao das soluções proprietárias, seja ele um servidor de arquivos, banco de dados, servidor web, servidor de e-mail, servidor de DHCP[26], servidor de DNS[27], Servidores de Proxy Caching[28], aplicações de ERP[29] (Enterprise Resource Planning) etc. Pode-se reaproveitar o hardware já existente na empresa, mesmo que sejam computadores heterogêneos, ou comprando-se microcomputadores genéricos, os quais possuem preços mais acessíveis e são facilmente encontrados no mercado. As empresas podem até comprar um equipamento robusto para tarefas de missão crítica, mas caso não seja adquirido hardware específico, como produtos ofertados para o seguimento corporativo, voltados para aplicações de missão crítica, ainda existirá a lacuna da redundância. O cluster de alta disponibilidade pode prover a redundância de hardware e software, garantindo o funcionamento do serviço em caso de indisponibilidade do equipamento, seja por falha do hardware ou do software (PITANGA, 2004).

Para demonstrar a vantagem do cluster de alta disponibilidade, pode-se considerar a solução baseada em ferramentas livres e gratuitas, o que desobriga a organização da compra de licenças de software.

Uma desvantagem da solução de cluster está na necessidade de um link dedicado para o Heartbeat, e uma falha neste link pode fazer com que as duas máquinas do cluster montem o sistema de arquivos[30] do cluster, levando a uma inconsistência dos dados.

Outra desvantagem está na perda de dados de download[31]/upload[32] que estiverem sendo executados durante uma falha do servidor primário do cluster.

O que é despendido com a área de tecnologia da informação (TI) não pode ser visto como gasto, mas sim como investimento, e muitas empresas estão mudando sua visão com relação a isso, uma vez que há uma grande dependência de sistemas computacionais. Nesse contexto, a solução de cluster torna-se ainda mais atraente, principalmente para empresas que dispõem de poucos recursos financeiros.

Para algumas organizações, como por exemplo as que utilizam comércio eletrônico, um pequeno tempo de indisponibilidade do sistema pode afetar o negócio da empresa, causando prejuízos financeiros significativos. Qualquer empresa está sujeita a ser surpreendida com falhas de hardware ou de software, o que indisponibiliza acesso aos arquivos pelos usuários. Como proposta a esse tipo de falha, podemos implementar uma solução de cluster de alta disponibilidade, provendo acesso aos arquivos vitais ao funcionamento da empresa. Essa solução se baseia na redundância de hardware e reconfiguração via software.

Uma solução de sistema de arquivos baseado em cluster, tanto o do tipo Beowulf quanto o tipo Openmosix, mostra-se ineficaz em razão da necessidade de um nó controlador, pois caso haja falha nesse nó/nodo, o serviço ficará indisponível. Já a solução de cluster focada na alta disponibilidade, baseada na utilização das ferramentas livres Heartbeat[33] (batimento cardíaco) responsável pelo gerenciamento do cluster realizando a verificação de funcionamento dos nós/nodos e tomada de decisão (caso necessário) e DRBD (Distributed Replicated Block Device) responsável pela replicação dos dados entre os nós/nodos primário e secundário, ambos os nós/nodos podem responder pelo nó primário, a falha de um nó/nodo não compromete o funcio-

25 Em português: alta disponibilidade.
26 Servidor que fornece endereços IP (protocolo de internet) dinâmicos para outros computadores da rede (MORIMOTO, 2004).
27 DNS (Sistema de Nomes de Domínio) faz a tradução de nome para endereço IP (MORIMOTO, 2004).
28 Servidor que guarda as páginas acessadas em cache (no disco rígido do servidor) (MORIMOTO, 2004).
29 Sistema integrado de gestão empresarial (MORIMOTO, 2004).
30 "É um conjunto de estruturas lógicas e de rotinas, que permitem ao sistema operacional controlar o acesso ao disco rígido." (MORIMOTO, 2004, p. 337).
21 Baixar arquivo através de uma rede ou internet (MORIMOTO, 2004).
32 Enviar arquivo através de uma rede ou internet.
33 Aplicativo do projeto High Availability Linux – http://www.linux-ha.org/pt_BR/HomePage_pt_BR.

namento do outro, de forma a garantir a alta disponibilidade do sistema de arquivos.

Nessa solução, a capacidade de processamento é atribuída apenas a uma das máquinas (cluster ativo/passivo), sendo que a segunda só será acionada em caso de falha do servidor principal (servidor primário); esse processo é conhecido como failover e o retorno à atividade do servidor que sofreu a falha é conhecido como failback; de acordo com a configuração escolhida, o servidor primário que sofreu falha assume a posição de secundário, só retornando à condição de servidor primário em caso de falha do outro servidor, processo conhecido como nice failback. Dentre as configurações necessárias, a solução deve ser configurada de forma a garantir o sincronismo dos servidores, para que a informação seja idêntica, independente de qual máquina esteja atendendo às requisições dos usuários no momento (servidor primário ou secundário). (SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO, 2006).

O exemplo concreto da arquitetura de cluster proposta é mostrado na FIG. 2, em que os computadores dos clientes têm acesso ininterrupto aos arquivos que são providos pelo servidor primário, e no caso de eventual falha deste computador, o servidor secundário assume a posição de servidor primário. Essa troca de papéis é viabilizada pela ação do software DRBD, responsável pela replicação dos dados entre o servidor primário e secundário. O Heartbeat é responsável pela monitoração do funcionamento dos servidores e o acionamento de tarefas em caso de falha do cluster.

Os componentes envolvidos na solução de cluster de alta disponibilidade podem ser classificados em dois grupos:

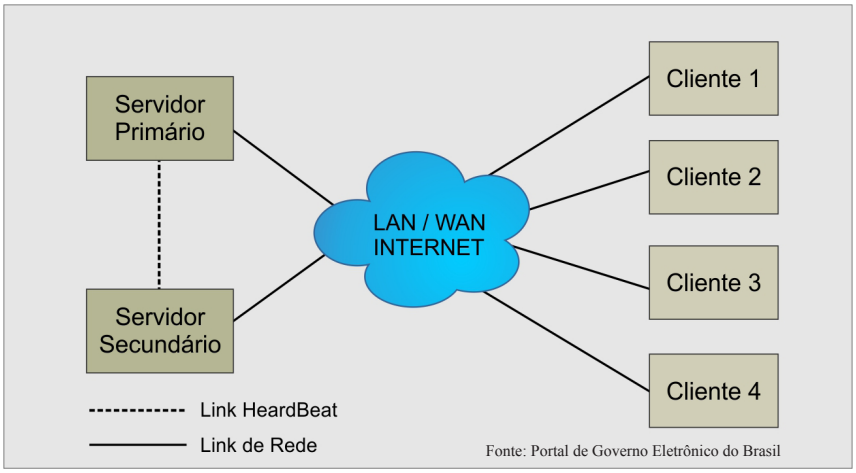


Figura 2 - Sistema de alta disponibilidade com dois servidores sendo acessados por quatro clientes

Hardware (computadores e ativos de rede):

Dois computadores que serão o nó/nodo primário e o secundário, o switch que fará a interligação dos computadores do cluster de alta disponibilidade com o restante da rede. Para tanto, cada um dos computadores do cluster terão duas placas de rede, ou seja, uma para o link do Heartbeat e a outra para interligação com a rede onde a solução será provida, sendo a rede, nessa proposta, uma rede fast-ethernet, que fornece uma largura de banda de 100Mbps. Com relação à interligação com a rede e o link do Heartbeat, visando à maior confiabilidade, deve-se considerar a utilização de redundância visando a aumentar a tolerância a falhas, principalmente do link do Heartbeat que pode ser feito com um canal fast-ethernet e um canal serial.

Softwares, já descritos anteriormente:

DRBD, Heartbeat e o sistema operacional Linux.

Utilizando-se computadores comuns, podendo esses serem heterogêneos em termos de hardware, o que torna a solução bastante flexível, considerando o uso de dois computadores apenas, em que os dois respondem ora como primário, ora como secundário no caso de eventual falha/indisponibilidade de um deles. Nesse cenário, em caso de uma das máquinas apresentar algum tipo de defeito, ela poderá ser substituída por outra, sem que o serviço fique indisponível aos usuários. Pode-se ainda considerar a utilização de um terceiro computador para realização de backup dos dados guardados no cluster.

7. Análise de resultados

Abaixo, apresentamos partes que foram exportadas do arquivo gerado com a captura de pacotes realizada com o Wireshark, durante o download de um arquivo via HTTP.

Após o início do download, o servidor primário do cluster foi desligado de forma abrupta e a máquina secundária assumiu a condição de servidor primário do cluster, passando a responder pelo endereço IP 192.168.1.1. A distinção das máquinas é demonstrada pelo endereço mac address das placas de rede, beta01 (00:40:a7:04:0f:da) e beta02 (00:40:a7:04:9a:2d).

A captura de pacotes no Quadro 1 demonstra a última comunicação

com o servidor que respondia pelo nó/nodo primário do cluster (beta01), endereço IP 192.168.1.1.

A captura de pacotes no Quadro 2 demonstra o momento em que máquina beta02 faz um broadcast na rede (request), passando a responder pelo nó/nodo primário do cluster.

No caso dos testes com download via FTP, o Quadro 3 demonstra, respectivamente, a falha do servidor primário beta01 (desligamento forçado) e o início de atividade da máquina beta02, iniciando os procedimentos para passar a responder pelo cluster.

O processo de download com a utilização do FTP falhou da mesma forma que o download feito via HTTP.

Nos testes realizados com o ping, feito o desligamento do servidor primário do cluster durante execução do ping (flag -c count), dos 50 pacotes transmitidos, 44 foram recebidos e seis foram perdidos, permitindo afirmar que o tempo de comutação do cluster foi de seis segundos.

Observou-se que, apesar do time do ping ser de seis segundos, na análise de resultados percebeu-se um time de 80.025205 segundos no caso da captura de pacotes no download via HTTP e 22.436709 segundos no download via FTP. Acredita-se que as diferenças entre os times se devem pelas diferenças entre o funcionamento do protocolo HTTP e FTP.

8. Considerações finais

Acredita-se que os objetivos geral e específico tenham sido atingidos, considerando que o laboratório foi montado e configurado com sucesso, possibilitando a coleta de dados para posterior análise.

Com base na análise da coleta dos dados realizada no laboratório piloto, utilizando-se a ferramenta de análise de rede Wireshark, verificou-se que a solução de alta disponibilidade de cluster não apresentou continuidade no fluxo de informações, tendo em vista que no caso de falha do servidor primário, o processo de transferência de dados executada via HTTP ou FTP no momento da falha se perde, e após a falha o processo de transferência

Quadro 1

```
No.     Time        Source          Destination     Protocol    Info
44825   17.500556   192.168.1.3     192.168.1.1     TCP         52285 > www [ACK] Seq=916 Ack=64710207
Win=663264 Len=0 TSV=4508257 TSER=1746
Frame 44825 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: AsoundEl_d3:a0:0a (00:02:2a:d3:a0:0a), Dst: beta01 (00:40:a7:04:0f:da)
Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.1 (192.168.1.1)
Transmission Control Protocol, Src Port: 52285 (52285), Dst Port: www (80), Seq: 916, Ack: 64710207, Len: 0
```

Fonte: Software de captura de pacotes de rede Wireshark

Quadro 2

```
No.     Time        Source          Destination     Protocol    Info
44826   97.525761   beta01          Broadcast       ARP         Gratuitous ARP for 192.168.1.1 (Request)
Frame 44826 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: beta01 (00:40:a7:04:9a:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request/gratuitous ARP)
```

Fonte: Software de captura de pacotes de rede Wireshark

Quadro 3

```
No.     Time        Source          Destination     Protocol    Info
45      68.203370   192.168.1.1     192.168.1.3     TCP         ftp > 44322 [ACK] Seq=292 Ack=118
Win=5792 Len=0 TSV=246472 TSER=1007229
Frame 45 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: ItautecP_04:0f:da (00:40:a7:04:0f:da), Dst: AsoundEl_d3:a0:0a (00:02:2a:d3:a0:0a)
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.3 (192.168.1.3)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 44322 (44322), Seq: 292, Ack: 118, Len: 0

No.     Time        Source          Destination     Protocol    Info
46      90.640079   ItautecP_04:9a:2d   Broadcast   ARP         Gratuitous ARP for 192.168.1.1 (Request)
Frame 46 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: ItautecP_04:9a:2d (00:40:a7:04:9a:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request/gratuitous ARP)

No.     Time        Source          Destination     Protocol    Info
47      91.158532   ItautecP_04:9a:2d   Broadcast   ARP         Gratuitous ARP for 192.168.1.1 (Reply)
Frame 47 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: ItautecP_04:9a:2d (00:40:a7:04:9a:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (reply/gratuitous ARP)

No.     Time        Source          Destination     Protocol    Info
48      91.678614   ItautecP_04:9a:2d   Broadcast   ARP         Gratuitous ARP for 192.168.1.1 (Request)
Frame 48 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: ItautecP_04:9a:2d (00:40:a7:04:9a:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request/gratuitous ARP)

No.     Time        Source          Destination     Protocol    Info
49      92.198630   ItautecP_04:9a:2d   Broadcast   ARP         Gratuitous ARP for 192.168.1.1 (Reply)
Frame 49 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: ItautecP_04:9a:2d (00:40:a7:04:9a:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (reply/gratuitous ARP)

No.     Time        Source          Destination     Protocol    Info
50      92.656815   192.168.1.1     192.168.1.255   NBNS        Registration NB BETA02<20>
Frame 50 (110 bytes on wire, 110 bytes captured)
Ethernet II, Src: ItautecP_04:9a:2d (00:40:a7:04:9a:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
NetBIOS Name Service
```

Fonte: Software de captura de pacotes de rede Wireshark

deve ser iniciado novamente.

Concluiu-se ainda que o tempo de comutação entre as máquinas do cluster (servidor primário/secundário) pode ser reduzido para um tempo de seis segundos, não se considerando a disponibilidade de serviços dentro desse tempo, ou seja, em um tempo de seis segundos, de acordo com os testes de laboratório, a máquina secundária assumiu o endereço IP da máquina primária, respondendo às consultas endereçadas ao IP 192.168.1.1 (IP do cluster).

Referências

ALVARENGA, Fabiano Veira de. *Uma proposta de aplicação para a solução do problema da árvore geradora de custo mínimo com grupamentos utilizando cluster em Linux*. 2007. Monografia (Especialização) – Departamento de Ciência da Computação da Universidade Federal de Lavras, Lavras, 2007. Disponível em <http://www.ginux.ufla.br/files/mono-FabianoAlvarenga.pdf>. Acesso em: 01 out. 2007.

BECHER, Marcelo Renan. *Montagem de um ambiente de cluster usando software livre: uma abordagem aos clusters de alta disponibilidade*. 2007. Disponível em <http://ist.sociesc.com.br/cursos/bsi/TrabalhoDeDiplomacao/TD-MarceloBecher-2007-1.pdf>. Acesso em: 30 set. 2007.

BORTOLIN, Elcio Luiz Pagani. *Alta Disponibilidade usando CODA e LVS*. 2005. Monografia (Especialização) – Departamento de Ciência da Computação, Universidade Federal de Lavras, 2005. Disponível em: <http://www.ginux.ufla.br/files/mono-ElcioBortolin.pdf>. Acesso em: 30 set. 2007.

CALDEIRA, Bruno Pêsso. *Alta Disponibilidade* – replicação de Dados Via Mysql, com Ênfase em Identificação e Recuperação de Falhas. 2006. Monografia (Especialização) – Departamento de Ciência da Computação, Universidade Federal de Lavras, 2006. Disponível em <http://www.ginux.ufla.br/files/mono-BrunoCaldeira.pdf>. Acesso em: 30 set. 2007.

DANTAS, Mario. *Ambientes Distribuídos de Alto Desempenho*: clusters e grades Computacionais. [S.1:Portal Brasileiro sobre computação de alto desempenho, 2006. Disponível em: <http://www.gridcomputing.com.br/tiki-index.php?page=Getting% 20Started>. Acesso em: 26 abr. 2006.

FERREIRA, Roberta Ribeiro. *Caracterização de desempenho de uma aplicação paralela do método dos elementos finitos em ambientes heterogêneos de PCs*. 2006. Dissertação (Mestrado em Ciência da Computação) – Instituto de Ciências Exatas, Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2006. Disponível em: <http://monografias.cic.unb.br/dspace/bitstream/123456789/81/1/Dissertacao_RobertaRibeiroFerreira.pdf>. Acesso em: 13 set. 2007.

JÚNIOR, Esli Pereira Faustino; FREITAS, Reinaldo Borges. *Construindo Supercomputadores com Linux*: Cluster Beowulf. Goiânia: 2005. Monografia – Departamento de Telecomunicações, Cefet-GO, Goiânia, 2005.

JÚNIOR, Raimundo Viégas. *Estudo de viabilidade da implementação de técnicas de cluster para a criação de laboratórios de Informática em instituições de ensino públicas voltada à programação nos cursos de Engenharia e Ciência da Computação*. São Paulo, 2006. World Congress on Computer Science, Engineering and Technology Education. Disponível em: <http://www.dca.ufrn.br/~rviegasjr/wccset2006.pdf>. Acesso em: 30 set. 2007.

MORIMOTO, Carlos E. *Dicionário de Termos Técnicos de Informática*. 3. ed. Disponível em: <http://www.dominiopublico.gov.br/pesquisa/DetalheObraForm.do?select_action=&co_obra=4783>. Acesso em: 21 dez. 2007.

PEREIRA, Roberto Benedito de Oliveira. *Alta Disponibilidade em Sistemas GNU/LINUX utilizando as ferramentas Drbd, Heartbeat e Mon*. 2005. Monografia (Especialização em Administração em Redes Linux) Departamento de Ciência da Computação, Universidade Federal de Lavras, Lavras, 2005. Disponível em: <http://www.ginux.ufla.br/node/120>. Acesso em: 30 set. 2007.

PINTO, Hudson de Jesus Lamounier. *Técnicas baseadas em clusters para um melhor aproveitamento do poder computacional*. Formiga, 2006. Universidade de Formiga Departamento de Ciência da Computação Instituto de Ciências Sociais Aplicadas e Exatas. Disponível em: <http://comp.uniformg.edu.br/~hlamounier/artigo.pdf>. Acesso em: 13 set. 2007.

PITANGA, Marcos. *Computação em cluster*: o estado da arte da computação. Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2003.

_____. *Construindo supercomputadores com Linux*. 2. ed. Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2004.

SLTI – Secretaria de Logística e Tecnologia da Informação. *Guia de Estruturação e Administração do Ambiente de Cluster e Grid*. Brasília, 2006. Disponível em: <http://guialivre.governoeletronico.gov.br/guiaonline/downloads/guiacluster.pdf>. Acesso em: 03 nov. 2007.

ZACARIAS, Daniel Constantino. *Funcionamento de um cluster Linux*. 2004. Disponível em: <http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=733>. Acesso em: 23 ago. 2007.

ZACARIAS, Daniel Constantino. *Funcionamento de um cluster Linux*: parte II – a revanche. 2004. Disponível em: <http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=840>. Acesso em: 23 ago. 2007.

Reflexões sobre a segurança de arquivos e de documentos arquivísticos: impactos das novas tecnologias e das mídias digitais


Divulgação

Leandro Ribeiro Negreiros

Mestre em Ciência da Informação, bibliotecário da Assembleia Legislativa do Estado de Minas Gerais (ALMG), professor do curso de Arquivologia da Universidade Federal de Minas Gerais (UFMG), coordenador e professor do curso de especialização em Gestão de Arquivos e Documentos da Pontifícia Universidade Católica de Minas Gerais (PUC-Minas).


Divulgação

Welder Antônio Silva

Mestre em Ciência da Informação, arquivista da ALMG, professor do curso de Arquivologia da UFMG e professor do curso de especialização em Gestão de Arquivos e Documentos da PUC-Minas.

RESUMO

Este artigo reflete de maneira crítica sobre as concepções e elementos necessários à segurança de arquivos e de documentos arquivísticos (digitais e tradicionais), principalmente em função do uso das novas tecnologias de informação e comunicação nas atividades de registro, gerenciamento, acesso e disseminação. Defende-se a necessidade de os arquivistas entenderem o termo segurança em sentido amplo, e não restrito, que considera tão somente a preservação dos suportes em que estão registrados os documentos. Aponta que as medidas de segurança em relação aos documentos arquivísticos devem ser entendidas e tratadas como ações e diretrizes proativas, que envolvem todas as rotinas e procedimentos arquivísticos, tendo em vista a necessidade de proporcionar um acesso confiável quando, onde e a quem for necessário.

1. Introdução: concepções e pontos de vista

Se procurarmos a definição de segurança em dicionários, podemos destacar quatro acepções (HOUAISS; VILLAR, 2009; FERREIRA, 1999):

a) ação ou efeito de assegurar e garantir alguma coisa: estado em que a satisfação de necessidades e desejos se encontra garantida;
b) situação em que não há nada a temer: estado, qualidade ou condição de estar livre de perigos, de incertezas, de danos e de riscos;
c) certeza, infalibilidade, convicção, evidência: estado, condição ou caráter daquilo que é inabalável, ou que se pode confiar;

d) conjunto de processos, dispositivos e medidas de precaução que asseguram o sucesso de um empreendimento, do funcionamento de algo ou do cumprimento de algum plano.

É importante destacar que, na maioria das vezes, fala-se de segurança em Arquivologia quando se pretende discutir e apresentar ações que visem à preservação e à conservação dos documentos. Todavia, medidas de segurança que contemplem essas quatro acepções devem ser consideradas na execução de todas as rotinas e procedimentos arquivísticos, e não estritamente naquelas cujo foco é a preservação dos suportes que compõem os conjuntos documentais.

Os arquivistas precisam entender a segurança em sentido amplo, e não restrito, ou seja, contemplando a proteção, a estabilidade, a inviolabilidade, a cautela, a prudência, o compromisso, a certeza, a eficácia, a eficiência, a confiança e a garantia de resultados satisfatórios em todos os serviços, rotinas e procedimentos que compõem as três fases do ciclo de vida dos documentos (corrente, intermediária e permanente), seja no contexto tradicional ou no digital.

É necessário que todas as rotinas e procedimentos arquivísticos sejam executados mediante diretrizes e orientações que não só exprimam segurança *stricto sensu* aos suportes dos documentos, sejam eles tradicionais ou digitais, mas, e principalmente, ao objetivo maior de um arquivo, que é a disponibilização e o acesso garantido aos documentos arquivísticos e às informações neles registradas.

Produzem-se, protocolam-se, controlam-se a tramitação, classificam-se, ordenam-se, avaliam-se, transferem-se, recolhem-se, acondicionam-se, armazenam-se, preservam-se e se descrevem os conjuntos documentais arquivísticos com o objetivo maior de proporcionar acesso confiável, ou seja, seguro e garantido, quando, onde e a quem for necessário.

Todavia, não se pode negar que a segurança dos arquivos e documentos arquivísticos merece, atualmente, ainda mais visibilidade e importância, tendo em vista a ascensão do uso das novas tecnologias de informação e comunicação nas atividades de gerenciamento, utilização e acesso. Além disso, é preciso destacar também, como causa dessa projeção, o surgimento dos documentos digitais, como forma de registro e fonte de informação. Tais circunstâncias trazem à tona a necessidade de se garantir a funcionabilidade e a utilidade dos documentos arquivísticos diante dos riscos, ameaças e vulnerabilidades que apresentam os sistemas informatizados, as mídias digitais e seus usuários.

As ameaças são concebidas, neste artigo, como os agentes causadores ou as condições favoráveis (internas ou externas) capazes de explorar as vulnerabilidades, gerando riscos. Por vulnerabilidades, compreendem-se as fragilidades presentes ou associadas aos serviços, rotinas, procedimentos, sistemas e conjuntos documentais arquivísticos. E por riscos, entendem-se as possibilidades de exploração das vulnerabilidades pelas ameaças, podendo causar algum dano ou incerteza e comprometer o sucesso de um empreendimento, do funcionamento de algo ou do cumprimento de algum plano[1].

As vulnerabilidades por si só não provocam incidentes ou ações negativas (riscos), uma vez que necessitam de agentes causadores ou de condições favoráveis (ameaças) para tanto. Dessa forma, medidas de segurança que protejam a instituição, o serviço de arquivo, as rotinas/procedimentos, os sistemas de gerenciamento e, por fim, os conjuntos documentais arquivísticos (todos dotados de vulnerabilidades e sujeitos a ameaças) devem ser previstas e implementadas (FIG. 1).

A garantia de qualidade arquivística, com o advento das novas tecnologias e das mídias digitais, está sujeita a vários riscos, que são proporcionados por diversos fatores, agentes e condições, ora provenientes do ambiente interno (serviço de arquivo e/ou instituição); ora provenientes do ambiente externo; ora relacionados aos aspectos humanos ou tecnológicos; ora aos processos, rotinas e procedimentos arquivísticos; e, é claro, ora relacionados aos próprios conjuntos documentais.

Como se percebe, sempre haverá riscos, que devem, na medida do possível, ser previstos e medidas de segurança precisam ser planejadas e implementadas. Se antes do advento das novas tecnologias e das mídias digitais, as ameaças e vulnerabilidades precisavam ser mapeadas e administradas, agora, diante de tais fenômenos, merecem cada vez mais esforços.

2. Elementos que sustentam a segurança de documentos arquivísticos

Para a Arquivologia, é importante determinar alguns elementos que asseguram a existência e a eficácia do documento arquivístico. De ma-

1 Sêmola (2003) trabalha os conceitos de vulnerabilidade, ameaça e risco ao abordar a segurança da informação direcionada aos gestores de tecnologia da informação e considerando uma visão executiva. Neste artigo, procurou-se utilizar esses termos adaptados à temática da segurança no bojo da Arquivologia.

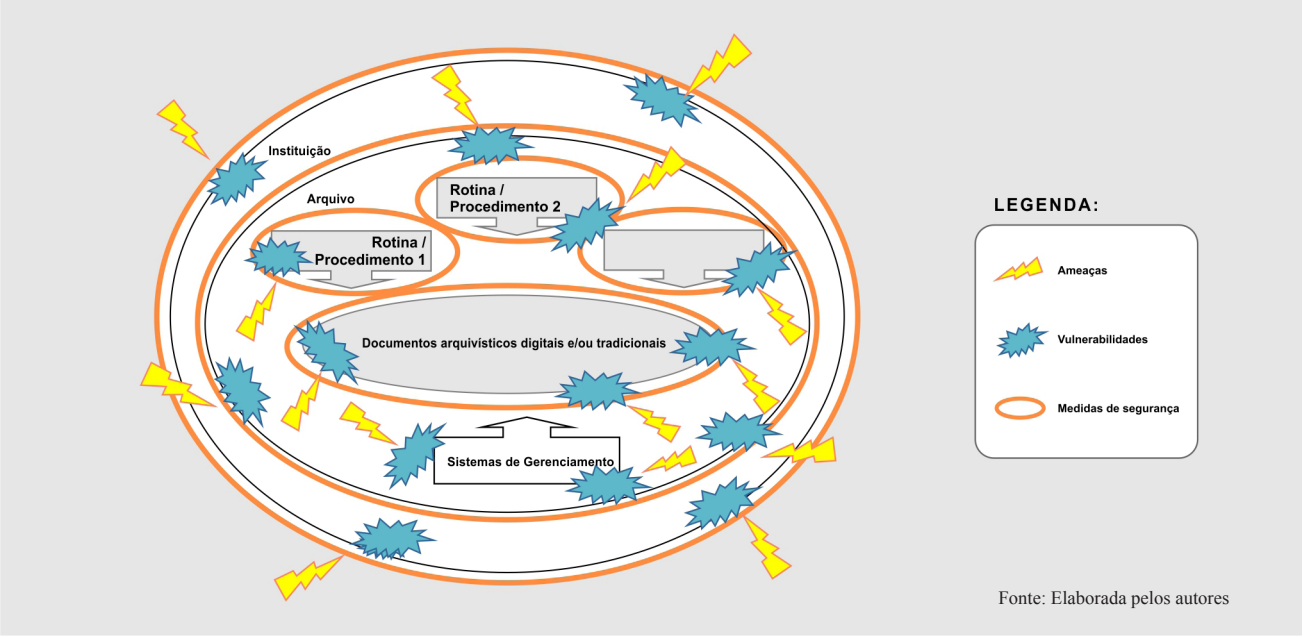


Figura 1 – Ameaças, vulnerabilidades, riscos e medidas de segurança

neira geral, a teoria arquivística apresenta quatro elementos que orientam a discussão sobre a segurança dos documentos arquivísticos: autenticidade, integridade, confiabilidade e acessibilidade.

A autenticidade, segundo a definição da Câmara Técnica de Documentos Eletrônicos (CTDE), é a "credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e que está livre de adulteração ou qualquer outro tipo de corrupção" (BRASIL, 2009, p. 5). De acordo com Rondinelli (2005), a autenticidade está ligada ao processo de produção, utilização e preservação de documentos. Assim, os documentos arquivísticos são produto de rotinas processuais que visam à execução de alguma atividade, sendo autênticos quando criados e conservados de acordo com procedimentos regulares, que podem ser comprovados em espaço e tempo determinados, a partir de rotinas estabelecidas.

A integridade é o "estado dos documentos que se encontram completos e que não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada" (BRASIL, 2009, p. 17). Para que as ações sejam representadas de maneira efetiva pelos documentos, é preciso que eles estejam completos e que não tenham sido alterados. Esse elemento possui estreita relação com a autenticidade, pois a inexistência de um compromete a percepção do outro. O documento arquivístico original, ou sua reprodução autorizada e validada, é, portanto, a melhor evidência da ação. Um documento arquivístico íntegro é, portanto, aquele que: possui todos os elementos que lhe conferem autenticidade; é caracterizado por categoria, espécie e tipo bem definidos; tem grau informacional adequado; define todas as relações com seus anexos; e não foi alterado, a não ser de maneira legítima, ao longo de sua existência.

A confiabilidade é um atributo do documento arquivístico que o torna o melhor representante de uma ação. Esse atributo "existe quando um documento arquivístico pode sustentar o fato ao qual se refere, e é estabelecido pelo exame da completeza da forma do documento e do grau de controle exercido no processo de sua criação" (BRASIL, 2009, p. 9). A definição da CTDE cria um elo teórico entre o termo confiabilidade e os demais explicitados (autenticidade e integridade). Além disso, aponta a relação coerente e necessária para a garantia de segurança do documento arquivístico.

A confiabilidade também pode ser concebida como sinônimo de fidedignidade; assim, um documento arquivístico confiável ou fidedigno, independente de seu suporte, é aquele digno de fé e confiança e, por isso, é possível apontá-lo como a melhor evidência de uma ação. Não se pode negar que a confiabilidade do documento arquivístico é inerente ao seu produtor e aos demais envolvidos nos seus processos de utilização e preservação. Por isso, fica clara a importância da ética e da

imparcialidade nesses momentos.

A acessibilidade, por sua vez, é traduzida como a "facilidade no acesso ao conteúdo e ao significado de um objeto digital" (BRASIL, 2009, p. 3). Embora seja notória a importância do acesso como função da Arquivologia, a acessibilidade, nesse contexto, mais que isso, é a preocupação com a garantia de disponibilidade da informação registrada no documento arquivístico. Importa também no cuidado com os registros dos contextos administrativo, fiscal, legal, tecnológico, de preservação e outros, como garantia para o entendimento da informação e como facilitador da compreensão do documento arquivístico na estrutura organizacional à qual pertence. Embora a acessibilidade seja mais evidente em documentos digitais, esse aspecto deve também contemplar os documentos tradicionais.

A confluência desses quatro elementos será capaz de garantir segurança administrativa, fiscal, legal e probatória ao documento arquivístico. Eles devem ser considerados, mantidos e tratados no planejamento e na execução dos serviços, rotinas e procedimentos arquivísticos, independentemente da fase do ciclo de vida em que se encontram os documentos.

Sempre haverá riscos humanos, tecnológicos ou processuais. Cabe ao profissional da informação planejar, agir, avaliar e, como em um ciclo, reiniciar todas essas ações. A segurança é, portanto, algo a se administrar, tanto em relação aos documentos digitais quanto aos convencionais.

3. Documentos arquivísticos digitais e a segurança

A já complicada atividade de manutenção de segurança dos arquivos, de suas rotinas/procedimentos e dos documentos arquivísticos tradicionais tornou-se ainda mais complexa com a utilização de documentos digitais. À Arquivologia não é fundamental determinar em qual suporte está o documento, e sim, por outro lado, se as características que o consolidam como um documento arquivístico foram mantidas. Assim, o documento arquivístico em suporte digital pode manter as mesmas características arquivísticas que os documentos tradicionais. A diferença está no suporte, nas formas de acesso e na preservação. O grande desafio, portanto, é garantir que o documento digital seja efetivamente um documento arquivístico e acessível ao longo do tempo.

Há, no entanto, uma série de questões que envolvem a segurança desses documentos arquivísticos eletrônicos, ou seja, que dizem respeito à garantia de que estejam acessíveis ao longo do tempo. Até o surgimento do suporte digital, estando o suporte físico preservado, assim também estaria a informação. Com o complexo de segurança que se formou a partir do surgimento dos documentos digitais, outras considerações merecem ser feitas.

Primeiramente, o documento arquivístico digital tem que preservar seu conteúdo, ou seja, a informação arquivística nele inscrita. No momento de sua criação, o produtor escolhe o melhor formato e estrutura para representá-lo e, portanto, essas determinações devem ser mantidas em curto, médio e longo prazos. Qualquer variação do formato e da estrutura adotadas invalidaria o documento arquivístico digital em questão.

Outro aspecto importante de segurança está relacionado ao hardware e ao software utilizados na produção do documento. Tanto o equipamento quanto os aplicativos utilizados no processo de criação documental devem ser mantidos para a promoção do acesso e consulta. Ainda que não seja o mesmo hardware ou software, um esforço constante deve ser efetuado para que o acesso ao documento não seja prejudicado. O estabelecimento de uma política de segurança de documentos arquivísticos digitais deve ser uma iniciativa para todas as instituições que decidem realizar a gestão de documentos digitais. A atividade de transferência de mídia, ou seja, a substituição de suportes digitais defasados por outros que suportem o mesmo documento e promovam o seu acesso de forma semelhante à do momento de sua criação deve ser extremamente calculada e planejada, dado o seu alto custo.

A realização de cópias de segurança é também mais um cuidado que o surgimento dos documentos digitais impôs às instituições. Comumente conhecidas como backup, as cópias de segurança são reproduções feitas com vistas a preservar as informações no caso de perda ou destruição do original.

Acrescenta-se a esses desafios de segurança, o empreendimento de manutenção das características dos documentos arquivísticos. No contexto eletrônico, seja ele um sistema informatizado de gestão arquivística de documentos, ou até mesmo um servidor, o documento tem que manter em longo prazo as suas propriedades. Além disso, os quatro elementos apresentados na seção anterior também devem ser conservados.

Todas as iniciativas de preservação e de segurança, dado o atual contexto jurídico, esforçam-se para manter os documentos digitais pre-

servados para consultas futuras, mas o país ainda carece de legislação que reconheça o documento arquivístico eletrônico como um documento original.

4. Considerações finais

Diante das concepções, argumentos e pontos de vista apresentados, acredita-se que as medidas de segurança, sejam elas relacionadas à instituição, ao serviço de arquivo, às rotinas/procedimentos, aos sistemas de gerenciamento ou aos conjuntos documentais, devem compreender diretrizes, orientações, práticas, procedimentos e mecanismos que:

a) identifiquem e monitorem as vulnerabilidades e as condições e/ou agentes que representam ameaças;
b) reduzam, eliminem, corrijam ou adaptem as vulnerabilidades e ameaças;
c) impeçam que as ameaças explorem as vulnerabilidades presentes e mapeadas;
d) limitem ou minimizem os impactos causados pelos riscos, caso seja inevitável a possibilidade de exploração das vulnerabilidades pelas ameaças;
e) visem a manter as práticas, procedimentos e mecanismos implementados.

Também se entende que é necessário modificar alguns comportamentos institucionais e profissionais relacionados à segurança dos arquivos e documentos arquivísticos, a saber:

a) as medidas de segurança devem ser ações corporativas, holísticas e globais, envolvendo todas as rotinas e procedimentos arquivísticos, e não somente aquelas relacionadas à preservação dos suportes documentais;
b) os arquivistas devem estar inseridos nas discussões sobre segurança, pois esta não é área exclusiva da Tecnologia da Informação;
c) os planos de segurança devem ser proativos e não reativos, defensivos e/ou paliativos;
d) as medidas de segurança são investimentos e não despesas;
e) as medidas de segurança devem ser tratadas como processos (ações coordenadas e sistematizadas), e não como um projeto pontual;
f) os problemas de segurança devem ser discutidos no nível estratégico da estrutura hierárquica institucional, e não somente nos níveis táticos e operacionais;
g) as medidas de segurança devem ser dinâmicas e não estáticas.

Em síntese, defende-se que as medidas de segurança, junto aos documentos arquivísticos (tradicionais ou digitais), devem ser entendidas e tratadas como ações e diretrizes proativas e preventivas, que assegurem que todas as rotinas e procedimentos arquivísticos a serem executados estejam livres de perigos, incertezas, danos e riscos. Tais medidas objetivam garantir infalibilidade e sucesso, tendo em vista a necessidade de proporcionar um acesso confiável, eficiente, eficaz e autêntico, quando, onde e para quem for necessário.

Referências

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos (CTDE). *Glossário*. 2009. Disponível em: <http://www.documentoseletronicos.arquivonacional.gov.br/media/2008ctdeglossariov5.pdf>. Acesso em: 30 ago. 2012.

FERREIRA, A. B. H. *Novo Aurélio Século XXI*: o dicionário da língua portuguesa. 3. ed. totalmente revista e ampliada. Rio de Janeiro: Nova Fronteira, 1999.

HOUAISS, A.; VILLAR, M. *Dicionário Houaiss da língua portuguesa*. Rio de Janeiro: Objetiva, 2009.

RONDINELLI, R. C. *Gerenciamento arquivístico de documentos eletrônicos*: uma abordagem teórica da diplomática arquivística contemporânea. Rio de Janeiro: FGV, 2005

SÊMOLA, M. *Gestão da segurança da informação*: visão executiva da segurança da informação: aplicada ao Security Officer. Rio de Janeiro: Campus, 2003.

A segurança da informação documental nos órgãos públicos

Nelson Spangler de Andrade

Engenheiro, mestre em Administração Pública, Sistemas de Informação e Gestão pela Fundação João Pinheiro/Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (FJP/DCC-UFMG). MBA pela FJP em Gestão Empresarial. Analista de Conteúdo Digital na Companhia de Tecnologia da Informação do Estado de Minas Gerais (Prodemge).

Gabriel Sales

Gabriel Sales

Sândalo Salgado Ribeiro

Especialista em Gestão de Projetos Educacionais pelo Centro Universitário UNA. Analista de Conteúdo Digital na Prodemge. Bibliotecário, CRB6 – n° 2.656.

RESUMO

Com o avanço exponencial da Tecnologia da Informação e Comunicação, as organizações devem intensificar os cuidados para manter íntegro, disponível e seguro o seu ativo de informações. O artigo aborda a segurança dos documentos criados e geridos pelas organizações, com o foco no setor público, contrapondo seus principais suportes, o papel e a mídia eletrônica. A adoção de acervos de documentos digitais, com claras vantagens com relação aos acervos em papel, traz desafios com relação à segurança. A tecnologia permite a disseminação de grandes volumes de informações em diferentes suportes digitais. Falhas e vulnerabilidades, além da obsolescência, devem ser tratadas e corrigidas. Aspectos legais referentes à documentação eletrônica também são considerados.

1. O valor da informação nas organizações

Quais são as informações vitais para uma organização executar seus processos de negócios sem gerar impactos e prejuízos? Onde essas informações são armazenadas? Como podem ser acessadas? Estão seguras? Estão íntegras? Respondendo a essas indagações, serão determinadas as áreas críticas que apresentam riscos, ameaças e vulnerabilidades na organização.

Em decorrência disso, um ambiente para a prevenção contra falhas e crimes nos meios informacionais deve ser instalado com a preocupação de evitá-los e na medida do possível não permitir a sua manifestação. A segurança da informação tornou-se um processo indispensável e rotineiro em todas as empresas. Segundo Jamil (2001, p. 43):

Encontrar e disponibilizar informações: toda organização tem informações que precisarão ser acessadas a partir de um ponto qualquer, para poucas ou muitas pessoas, como: metas empresariais, volumes de vendas, políticas empresariais, dados de inventários, orçamentos e planos de curto, médio e longo prazos. Alguns tipos de informações, como linhas mestras da

administração da empresa, raramente se alteram. Outras como dados de vendas mudam o tempo todo, sendo constantemente atualizadas. Tudo isto pode afetar não só a forma como as pessoas trabalham, mas também a qualidade do trabalho que elas executam.

Essa afirmação ilustra a importância que toda empresa deve ter com a segurança da informação, pois a informação disponível é sempre o foco por parte de alguém com segundas intenções, por constituir-se em um dos ativos principais das organizações e por conter um alto valor agregado.

Entre os diversos tipos de incidentes contra a segurança da informação, podem-se destacar: a quebra de sigilo; a invasão de privacidade; o roubo de informações de acervos físicos e digitais, por meio de tecnologias móveis, e a indisponibilidade de diversos tipos de serviços essenciais. Todas as empresas estão suscetíveis a essas ocorrências, uma vez que possuem em seus ativos o principal alvo dessas ações: a informação.

2. O suporte papel

O papel tem sido o principal suporte para armazenar e divulgar criações e informações geradas pela humanidade. Nas últimas décadas, entretanto, o suporte digital tem se colocado como alternativa mais evoluída e vantajosa na maioria dos nichos em que o papel era dominante.

A administração pública no Brasil acumula centenas de milhões de páginas documentais que retratam as ações das diversas esferas de governo. São documentos necessários para estabelecimento de valor probatório, decisões em processos administrativos e questões legais, preservação da história e demonstração da transparência das instituições. A quase totalidade desses acervos ainda utiliza o papel como suporte para os documentos.

Essa mesma administração pública tem investido no uso das tecnologias de informação para racionalizar seus processos e prestar serviços para a sociedade. Entretanto, o uso do ferramental que a tecnologia de informação e comunicação dispõe para a gestão de documentos públicos ainda é incipiente.

Apesar de alguns órgãos e instituições arquivísticas públicas manterem seus acervos seguros, íntegros e organizados, observa-se a dificuldade para convencer os responsáveis pelos diversos setores públicos a adotarem políticas para investimentos nos órgãos que possuem acervos documentais, definindo medidas para mitigar os riscos e as deficiências de segurança proporcionada pelo acesso aos documentos.

O uso do papel como suporte para os arquivos documentais gerados e geridos pelos órgãos públicos vem enfrentando restrições e problemas de várias ordens.

a) a dificuldade crescente em manter grandes acervos íntegros, organizados, seguros e disponíveis;
b) a escassez de recursos humanos capacitados em administrar esses acervos;
c) a precariedade, inadequação ou falta de edificações para abrigar os acervos;
d) o custo crescente de armazenamento e manutenção de centenas ou milhares de metros lineares de papel;
e) as ameaças naturais ou artificiais que afetam a conservação e a durabilidade do papel (fatores físicos, biológicos e climáticos, sinistros, fenômenos da natureza);
f) os riscos de perdas documentais por causas humanas como acidentes, negligência, roubo, extravio, sabotagem, atentados, guerras;
g) a degradação natural do papel (FIG. 1), considerando adicionalmente o custo para a restauração de documentos, um processo quase artesanal;
h) a dificuldade e a demora de acesso aos documentos por parte dos interessados;

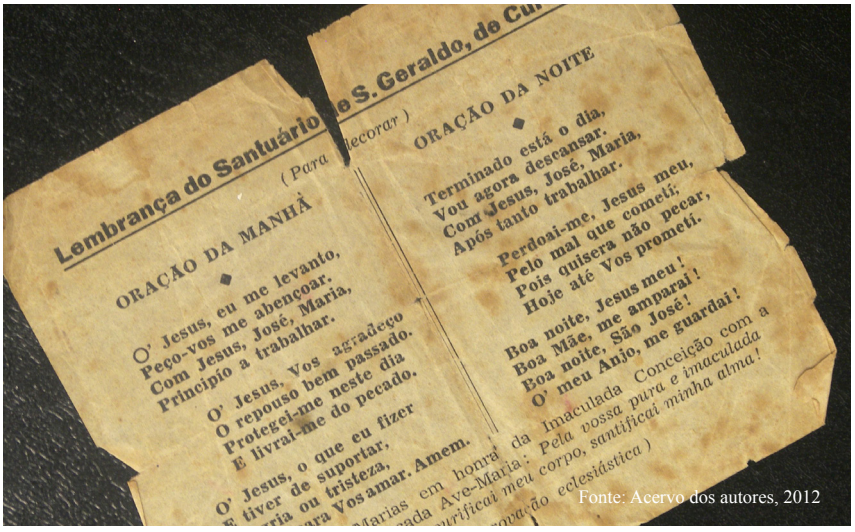


Figura 1 – A degradação de documentos em papel

i) o prejuízo ao meio ambiente devido à destruição da cobertura vegetal para produção de celulose.

Para eliminar ou minimizar esses fatores, uma série de medidas de segurança teria que ser definida e adotada. Entretanto, o que se observa na maioria dos casos é que essas medidas não são implantadas ou, quando implantadas, não são satisfatórias e continuadas.

Enfim, se a segurança de acervos em papel é precária e os acervos não param de crescer, por que não procurar alternativas? O suporte digital traz uma série de vantagens com relação ao papel, considerando o potencial da Tecnologia da Informação e Comunicação (TIC). As facilidades de pesquisa e acesso por meio de sistemas de informação eletrônicos permitem que documentos digitais possam ser acessados por vários usuários simultaneamente, sem restrições geográficas e com a segurança necessária para cada caso.

3. O suporte digital

O avanço exponencial da tecnologia da informação e comunicação pode ter a princípio contribuído para a disseminação do uso do papel. A disponibilidade de acesso à informação digital, aliada à facilidade e ao barateamento dos custos de impressoras, tornou o ato da impressão em papel quase imperceptível. Imprime-se, reimprime-se e copia-se a um simples toque de mouse ou teclado. Mesmo nas grandes instalações de impressão corporativas, um enorme volume de informações digitais é repassado para centenas de milhares de folhas de papel, em muitos casos sem necessidade.

Esse quadro, porém, vem se alterando significativamente. A maioria das indústrias voltadas para equipamentos e insumos de impressão está se redirecionando, até por sobrevivência, e dando cada vez mais atenção ao suporte digital.

Os documentos digitais, como qualquer arquivo digital, são cadeias de código binário (compostas de zeros e uns) capazes de serem reconhecidos por computadores. Para serem compreendidos pelas pessoas, necessitam de uma interface tecnológica baseada principalmente em ferramentas de software, hardware e comunicação.

De forma simplificada, essa interface é composta de:

a) programas de computador capazes de gerar, interpretar e tornar disponível uma extensa gama de formatos de arquivos binários que representam textos, gráficos, imagens, áudio e vídeo, entre outros;
b) computadores para executar os programas;
c) dispositivos de armazenamento eletrônico para gravar e manter disponíveis os arquivos digitais;
d) redes de comunicação de dados para disseminar as informações para vários locais, simultânea e concorrentemente.

O suporte para os documentos digitais é físico como o papel, mas diferenciado e evolutivo. São mídias como fitas magnéticas, discos magnéticos, discos óticos (CD, DVD, Blu-Ray) e, mais recentes, dispositivos de memória flash. Diferentemente do papel, as tecnologias digitais evoluem e algumas são substituídas por outras. Novas alternativas são desenvolvidas rapidamente com capacidade crescente e custo decrescente.

As mídias digitais são densas. Elas podem armazenar em suportes, cada vez mais reduzidos e sofisticados, quantidades de informação extremamente maiores que aquelas possíveis na mídia papel. Exemplos didáticos como o armazenamento de todas as dezenas de volumes impressos de uma grande enciclopédia em um único DVD já não representam a realidade. Em um dispositivo portátil de memória flash, por exemplo, se pode armazenar uma biblioteca inteira. Fato é que já não se imprimem mais enciclopédias, pois são muito mais caras que as digitais, mais difíceis de pesquisar e as pessoas não têm onde armazená-las.

Por um lado, a rapidez e a facilidade de acesso, por meio da web, e a capacidade de armazenar enormes volumes de informação em espaços reduzidos, impraticáveis para acervos em papel, são grandes estímulos para o uso da documentação digital, notadamente em uma sociedade que gera e acessa informações continuadamente.

Por outro, um dos maiores desafios de segurança dos documentos digitais é inerente à sua própria preservação. Documentos de arquivo, sejam analógicos (como papel e microfilme) ou digitais, devem manter-se íntegros e disponíveis por décadas. O papel, apesar das várias ameaças que enfrenta, pode corresponder razoavelmente, se convenientemente tratado, à expectativa de durabilidade.

Como foi dito, para terem acesso às informações em meio digital, as pessoas necessitam de artefatos tecnológicos de software, hardware e comunicação que estão em contínua evolução. Por ironia, a evolução exponencial da TIC gera a rápida obsolescência tecnológica dos dispo-

sitivos necessários para manter, interpretar e distribuir as informações armazenadas em suporte digital. O suporte digital evolui, e os equipamentos e sistemas hoje de ponta estarão descartados em poucos anos. A própria mão de obra também é migratória, tornando difícil encontrar profissionais capazes de trabalhar com tecnologias legadas e obsoletas.

Os principais desafios da documentação digital são:

a) obsolescência tecnológica (FIG. 2);
b) fragilidade de mídia digital.

Fonte: Acervo Prodemge

Figura 2 - A obsolescência da mídia digital

Essa segunda se refere à incerteza, devido ao pouco tempo de existência e uso das mídias digitais, de como elas se comportarão ao longo de prazos mais dilatados (dezenas de anos). Como estarão os documentos gravados em um DVD, por exemplo, daqui a 20 ou 30 anos? Suportes digitais também estão sujeitos a degradação por fatores como temperatura, umidade, erosão de superfície ótica e desmagnetização. Devido à grande comercialização alguns suportes, como CDs e DVDs, fabricados a baixo custo, não atendem aos requisitos de qualidade.

A obsolescência tecnológica atinge os equipamentos, sistemas, formatos e suportes. Formatos digitais passam por mudanças ao longo do tempo e, não raramente, as informações neles contidas não podem mais ser reconhecidas devido à inexistência de programas e equipamentos capazes de processá-los. Isso pode acontecer mesmo que o suporte digital mantenha a integridade da informação nele armazenada.

Tais desafios têm sido estudados pela indústria, pelas empresas de serviços de TIC e pelos pesquisadores acadêmicos. Não estão completamente equacionados, mas uma série de políticas e inovações já os minimizam. Significativos avanços têm sido obtidos visando garantir a durabilidade do documento digital em ambientes seguros.

Exemplos podem ser citados como o PDF/A, um formato criado especificamente para servir como padrão para a preservação de documentos digitais por longos períodos. Um dos principais objetivos do PDF/A é ser independente de plataformas de

hardware e software, podendo ser acessado por ferramentas básicas.

Outro exemplo é a evolução de equipamentos de arquivamento digital (**archiving**) capazes de armazenar por longos períodos grandes volumes de informação digital (da ordem de terabytes e petabytes,) de acordo com a necessidade de acesso. Documentos pouco pesquisados podem ser armazenados em dispositivos mais lentos e baratos que aqueles intensamente acessados.

Vários fatores devem ser considerados com relação ao uso seguro e à longevidade dos documentos digitais, como a criação de políticas para preservação e segurança, a não dependência de hardware e software específicos e proprietários, a migração de suportes e formatos ao longo do tempo, a replicação do acervo documental digital em locais físicos distintos, o uso de cópias de segurança (backup) e o controle do lixo digital.

A garantia de autenticidade é outro fator importante para a adoção da documentação digital. Para isso, a solução já legalizada e estabelecida no Brasil é a certificação digital, cujo uso vem se disseminando a cada ano.

4. A conversão de acervos

Os acervos em papel podem ser integralmente convertidos para o formato digital de uma só vez ou de forma escalonada, segundo critérios de prioridade, demanda, prazos e custos.

A conversão de acervos trata da organização, preparação, tipificação, digitalização, controle de qualidade e indexação dos documentos. Documentos digitais indexados poderão ser posteriormente gerenciados e pesquisados por sistemas de informação de gestão de conteúdo.

No dia a dia das organizações, novos documentos são absorvidos, gerados e oportunamente agregados ao acervo documental, de acordo com seu ciclo de vida. É importante que esses documentos sejam convertidos para o meio digital ou que já sejam criados digitalmente, eliminando na fonte o uso do papel. Uma solução de gerenciamento eletrônico de documentos deve englobar documentos legados e correntes.

Um projeto de gestão documental leva em conta a situação e as especificidades dos acervos e dos documentos correntes, estabelecendo a melhor maneira de convertê-los e incorporá-los em um repositório digital, e cria um sistema de informação capaz de permitir a preservação, a integridade e o acesso com segurança.

4.1. A utilização de data center para armazenamento de documentos digitais

Data centers são instalações sofisticadas voltadas para prestar serviços completos de TIC. Possuem uma estrutura tecnológica atualizada e robusta, capaz de atender a várias empresas simultaneamente, com custos competitivos em relação às vantagens que oferece.

Um data center caracteriza-se por:

a) possuir toda a estrutura de TIC necessária para abrigar as soluções informatizadas das organizações que atende;
b) garantir segurança, integridade e disponibilidade a essa estrutura;
c) ser construído, aparelhado e monitorado segundo normas reconhecidas internacionalmente;
d) ter fornecimento contínuo de energia: sistema de fornecimento de energia elétrica redundante, utilização de grupos geradores e equipamentos nobreaks;
e) ter climatização redundante em seus ambientes;
f) ter segurança física contra acesso indevido (biometria, circuito de TV etc.);
g) ter segurança lógica para evitar acesso indevido às informações armazenadas (firewall, VPN, detecção de tentativas de intrusão, controle de vírus etc.);
h) possuir salas-cofre com proteção contra incêndio, fumaça, gases, água, poeira e explosão;
i) possuir estrutura de backup e contingência para as informações e sistemas sob sua responsabilidade.

Para órgãos públicos que processam ou pretendem processar grandes e crescentes volumes de informação digital, é aconselhável a utilização de um data center em vez de manter instalações próprias de processamento eletrônico, principalmente quando a TIC não é a sua atividade-fim, mas um meio para executá-la.

O data center fornece mais serviços, possui pessoal especializado, é mais seguro, funciona 24 horas por dia, 365 dias no ano, e está sempre atualizado tecnologicamente. Cada cliente pode negociar e estabelecer seus níveis de serviço para serem atendidos pelo data center e definir seus custos. Manter estrutura semelhante em instalações próprias se torna muito mais custoso e difícil de gerenciar.

Soluções diferenciadas e atualizadas de sistemas operacionais, de banco de dados e outros softwares básicos, bem como de aplicativos e de todo ferramental de TIC com custos elevados, são comumente disponíveis em data center, propi-

ciando mais alternativas aos seus usuários.

5. Os acervos documentais nos órgãos públicos

Durante séculos não existiu alternativa viável para o papel como suporte para documentos. A microfilmagem, suporte analógico mais recente, pode ser considerada um contraponto, mas possui restrições de uso, segurança e dificuldade de acesso semelhantes ao papel.

As tecnologias da informação e comunicação vêm possibilitando a mudança dos suportes analógicos para os suportes digitais, modificando sobremaneira os modos de produção da informação e do conhecimento. Nesse contexto, observa-se que os órgãos públicos têm, em sua maioria, acervos documentais no suporte papel.

A administração pública no Brasil foi e continua sendo uma grande geradora de documentação em papel nos seus diversos níveis de atividade: administração, planejamento, finanças, jurisprudência, educação, saúde, serviços e segurança.

Acervos documentais proliferaram e acumularam documentos há décadas, e vêm enfrentando dificuldades proporcionais ao seu gigantismo para se manterem íntegros, organizados e acessíveis. A cada dia novos documentos são produzidos e incorporados a esses acervos.

Esses acervos encontram-se, em grande parte, sem o devido tratamento pelos profissionais das áreas de Arquivologia, Ciência da Informação, Museologia e afins. Com isso, por diversas vezes, ficam desprotegidos e sem a possibilidade de manter a integridade do conteúdo informacional da forma necessária, incorrendo no risco de perder documentos com um valor de cunho histórico, raro e precioso.

Em visitas a acervos documentais físicos dos órgãos, é possível fazer um balanço e relatar o pouco interesse em resguardar a memória da instituição e, muitas vezes, da informação estratégica utilizada em seus processos mais críticos.

Os acervos não apresentam segurança contra possíveis incidentes, tais como: incêndios, enchentes, ataques por agentes biológicos e outros. Em grande parte, se ocorrer um desastre dessa magnitude, o acervo não poderá ser recuperado. Muitas informações importantes serão perdidas sem qualquer possibilidade de recuperação. É ainda notório que, para os responsáveis por manter o acervo, basta colocá-lo em estantes dentro de caixas para ficar seguro. Logo, faz-se necessário divulgar a importância de uma política de gestão documental para todos os órgãos.

Outro fator importante diz respeito à falta de segurança quanto ao acesso físico. Com diversas tecnologias (dispositivos móveis, câmeras digitais, tablets, PDAs) é muito fácil extrair informações sigilosas, confidenciais e estratégicas de dentro dos órgãos. Um celular com câmera pode facilmente copiar o conteúdo de documentos sigilosos em poucos segundos e ser disseminado com uma rapidez vertiginosa nas redes sociais.

O volume dos acervos nos órgãos do Estado de Minas Gerais pode ser estimado em um montante considerável quando o suporte é o papel: cerca de 800 milhões de páginas.

Os problemas enfrentados por todos os órgãos de maneira geral são os mesmos: falta de espaço físico para a guarda dos documentos, grande volume de impressão, gerando altos custos, processos morosos na recuperação de informação, redundância nos acervos e muitos outros.

Além disso, existem os problemas com a segurança ao tratar o documento em papel, e mesmo quando tratados com as políticas de segurança, não constituem uma certeza para os órgãos que não possam ser alterados, copiados e descartados de forma indesejada, apresentando muitos riscos e vulnerabilidades como foram citados anteriormente.

6. A legislação sobre a segurança da informação nos órgãos públicos

A organização deve identificar todo tipo de leis, regulamentos, normas, resoluções e recomendações relacionadas ao seu negócio. A política de segurança da informação da empresa precisa respeitar toda a legislação pertinente e implementá-la de maneira a maximizar a sua eficácia.

A lei n° 12.527, de 18 de novembro de 2011, dispõe sobre os procedimentos a serem observados pela União, estados, Distrito Federal e municípios, a fim de garantir o acesso a informações. Conhecida como Lei da Transparência, deverá exigir, de todos os setores públicos, alterações na forma de disponibilizar as informações para o cidadão que faz uma solicitação junto ao respectivo órgão detentor da referida informação.

Entre a legislação federal sobre o assunto, cabe destacar a nova lei sancionada neste ano: a lei nº 12.682, que dispõe sobre a elabora-

ção e o arquivamento de documentos em meios eletromagnéticos. A publicação dessa lei, de 9 de julho de 2012, propiciou uma oportunidade para alguns órgãos públicos colocar o foco novamente no seu acervo documental.

Dada a importância da lei, e como alguns artigos dela foram vetados, ainda não se pode utilizá-la com o intuito de diminuir as grandes quantidades de acervo em papel nos órgãos públicos do estado. A lei teve inicialmente oito artigos, dos quais foram vetados o segundo, o quinto e o sétimo.

A lei deverá ser vista como um novo indicativo da importância em se tratar os acervos, quer no meio físico ou no meio digital. Os artigos vetados foram entendidos como parte de um questionamento jurídico, pois segundo um deles, os documentos em papel após digitalizados poderiam ser descartados. No entanto, isso acabaria gerando controvérsias jurídicas devido à forte cultura em ter o documento no suporte papel. Com isso, e baseando-se na legislação arquivística, optou-se por retirar tais artigos.

Assim, deve-se esperar que outras iniciativas legais possam ser discutidas e colocadas em pauta, a fim de procurar resolver os problemas informacionais levantados, dando a devida importância que o assunto necessita.

7. Considerações finais

A gestão de conteúdo digital é alternativa para solucionar os problemas decorrentes dos grandes acervos documentais mantidos pelos órgãos da administração pública. Constitui uma excelente forma de melhorar a capacidade dos órgãos em solucionar as questões decorrentes dos documentos em papel.

Cabe ressaltar que o documento digital possui alguns pontos críticos, os quais devem ser tratados no momento de se pensar a concepção da solução da conversão dos acervos físicos.

O tema conversão de acervos versus documento em papel ainda é matéria de debates nos meios acadêmicos, jurídicos e sociais, pois reflete a preocupação com a importância crucial dos documentos tratados, o seu papel informacional e a cultura de um povo contida nos mesmos.

Os órgãos públicos não podem desconsiderar e retardar o uso da tecnologia digital para solucionar os problemas decorrentes do gigantismo dos acervos em papel sob pena de perda de grande parte de seu arcabouço informacional.

Referências

ARAYA, Elizabeth R. M.; VIDOTTI, Silvana A. B.G. *Criação, proteção e uso legal de informação em ambientes da World Wide Web*. São Paulo: Cultura Acadêmica, 2010.

BRASIL. Lei n° 12.682 de 9 de julho de 2012. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. *Diário Oficial*. Brasília, DF, Ano CXLIX, n. 132. 10 jul. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12682.htm>. Acesso em: 12 set. 2012.

CAMPOS, André. *Sistema de Segurança da informação*: controlando os riscos. 2. ed. Florianópolis: Visual Books, 2007.

CASTELLS, Manuel. *A sociedade em rede* – a era da informação: economia, sociedade e cultura. v. 1. São Paulo: Paz e Terra, 1999.

JAMIL, George Leal. *Repensando a TI na empresa moderna*: atualizando a gestão com a tecnologia da informação. Rio de Janeiro: Axcel Books, 2001.

PDF/A, *Wikipedia, the free enciclopedia*. Disponível em: <http://wikipedia.org>. Acesso em: 28 set. 2012.

VALETIM, Marta Lígia Pomim (Org.). *Gestão, mediação e uso da informação*. São Paulo: Cultura Acadêmica, 2010.

Engenharia da segurança: computação em nuvem e privacidade


Divulgação

Leonardo Barbosa

Professor adjunto do Departamento de Ciência da Computação da UFMG. Bacharel (UFMG), mestre (UFMG), doutor (Unicamp) e pós-doutor (Unicamp) em Ciência da Computação. Realizou parte do seu doutorado na Dublin City University e no Information Security Group da Universidade de Londres. Pesquisador colaborador do Instituto de Computação da Unicamp. Agraciado com os prêmios IEEE Young Professional Award e Microsoft PhD Fellowship Award. Seus principais interesses de pesquisa estão nas áreas de segurança e criptografia aplicada à computação ubíqua.

RESUMO

Na medida em que a computação torna-se ubíqua e que, concomitantemente, o número de ataques a sistemas computacionais cresce vertiginosamente, "segurança" passa a ser objeto de estudo multidisciplinar e, por conseguinte, de interesse dos mais diversos públicos. Diferentemente do passado, quando era encarada como necessária apenas em aplicações críticas, segurança é hoje pré-requisito para o funcionamento de qualquer sistema computacional. Sua inoperância, seja por ataques ou falhas, pode acarretar severas consequências.

A engenharia da segurança possui como objeto de estudo o desenvolvimento de sistemas computacionais seguros. Nesse contexto, "seguro" possui a conotação de confiável (*dependable*), seja da perspectiva da robustez (*reliable*) ou da segurança propriamente dita (*trustworthy, safe*..., enfim, *secure*). A engenharia da segurança pesquisa políticas, metodologias, implementações, testes e ferramentais de segurança e, para tal, engloba diferentes áreas: do controle de acesso e detecção de intrusão à auditoria, criptografia e desenvolvimento de hardware seguro.

Este artigo apresenta alguns dos atuais desafios da engenharia da segurança. Mais precisamente, ele aborda os desafios da segurança em computação em nuvem e os problemas de privacidade contemporâneos.

1. Introdução

Na medida em que a computação torna-se ubíqua e que, concomitantemente, o número de ataques a sistemas computacionais cresce vertiginosamente, segurança passa a ser objeto de estudo multidisciplinar e, por conseguinte, de interesse dos mais variados públicos.

Diferentemente do passado, quando era encarada como necessária apenas em aplicações críticas, segurança é hoje pré-requisito para o funcionamento de qualquer sistema computacional. Sua inoperância, seja por ataques ou falhas, pode acarretar severas consequências, por exemplo, a inoperância de: (i) sistemas de monitoramento nuclear coloca em perigo as comunidades em seu entorno; (ii) sistemas de caixas eletrônicos e transações on-line resultam em prejuízo financeiro; (iii) sistemas de alarmes facilitam furtos; e (iv) sistemas de prontuário médico eletrônico expõem a vida alheia e violam a privacidade de indivíduos.

A engenharia da segurança possui como objeto de estudo o desenvolvimento de sistemas computacionais seguros. Nesse contexto, "seguro" possui a conotação de confiável (*dependable*), seja da perspectiva da robustez (*reliable*) ou da segurança propriamente dita (*trustworthy, safe*..., enfim, *secure*). A engenharia da segurança pesquisa políticas, metodologias, implementações, testes e ferramentais de segurança e, para tal, engloba diferentes áreas: do controle de acesso e detecção de intrusão à auditoria, criptografia e desenvolvimento de hardware seguro – também chamado de resistente ou à prova de violação (*tamper-resistant* e *tamper-proof*, respectivamente).

Atualmente, alguns dos princi-

pais desafios da engenharia da segurança estão nas áreas de segurança em computação em nuvem e privacidade. Em computação em nuvem, em particular, existe uma grande demanda por soluções que viabilizem sua adoção por usuários com requisitos de segurança mais rígidos, bem como soluções que forneçam bases seguras para novos serviços baseados na tecnologia. Em relação à privacidade, o desafio é projetar soluções para garanti-la num mundo como hoje, isto é, num contexto repleto de informações disponíveis on-line. Note-se que tais desafios são interdependentes e o primeiro torna o segundo mais desafiador e vice-versa. Por exemplo, enquanto a garantia de privacidade é condição *sine qua non* para a adoção universal de computação em nuvem, o advento de computação em nuvem tornou o desafio de se garantir privacidade ainda mais complexo.

A seguir, exploramos com mais detalhes, respectivamente, as questões atuais de segurança em computação em nuvem e privacidade.

2. Segurança em computação em nuvem

O avanço da tecnologia de comunicação aliado à crescente demanda por recursos computacionais levaram muitas organizações a terceirizar o armazenamento e processamento de dados. A esse novo paradigma computacional é dado o nome de computação em nuvem. Ele inclui diversos tipos de serviço, a saber: (i) infraestrutura como serviço (*Infrastructure as a Service* – IaaS), em que clientes usufruem do processamento, armazenamento e infraestrutura de rede do provedor; (ii) plataforma como serviço (*Platform as a Service* – PaaS), em que clientes tiram proveito dos recursos do provedor para executarem aplicações personalizadas (*custom applications*); e (iii) software como serviço (*Software as a Service* – SaaS), em que clientes utilizam algum software executado no provedor.

O uso de computação em nuvem por parte dos clientes acarreta diversas vantagens, por exemplo, ao migrarem sistemas e dados para a "nuvem", clientes poupam gastos com a implantação e manutenção de uma solução própria. Em contrapartida, precisam apenas pagar uma mensalidade (por vezes relativamente pequena) aos provedores de computação em nuvem. Para muitos clientes, isso é bem mais vantajoso.

Computação em nuvem, todavia, não é uma panaceia. Ela introduz sérias questões de segurança e, em razão disso, tem atraído bastante a atenção da comunidade científica. Parte das principais questões é relativa ao sigilo e à integridade dos dados armazenados na nuvem. Embora pessoas físicas (pelo menos até hoje) acreditem que o saldo do compromisso entre a privacidade e a conveniência de serviços web (webmail, por exemplo) tenha lhes sido favorável, o mesmo não ocorre para muitas pessoas jurídicas, em particular para organizações governamentais e grandes instituições privadas.

Tal comportamento pode ser atribuído a diversos fatores: da preocupação quanto à proteção de informações estratégicas, a leis que requerem o sigilo e a integridade de dados. Sobre o primeiro, não é difícil concluir que colaboradores da Microsoft não deveriam, por exemplo, trocar mensagens sobre depósito de patentes utilizando o Gmail. Nesse caso, há um evidente conflito de interesse entre a Microsoft e o Google acerca de propriedade intelectual. Já o segundo pode ser verificado em aplicações de prontuário médico eletrônico ou de registros financeiros. O vazamento dessas informações pode resultar em prejuízos morais e de ordem financeira e, por conseguinte, sua privacidade é garantida por lei.

Em suma, por um lado computação em nuvem promete ser um grande ferramental tecnológico capaz de minorar custos e incrementar a utilização e eficiência de sistemas. Por outro, ela traz consigo questões científicas complexas que podem e devem ser abordadas sob a ótica da engenharia da segurança. Eis algumas delas (KAMARA; LAUTER, 2010):

a) Conformidade regulatória. Muitos países possuem leis que responsabilizam organizações pela proteção dos dados sob sua custódia. Isso é especialmente verdade quando os dados custodiados são de natureza pessoal, ou seja, prontuários médicos ou declarações de impostos. Assim, o emprego de computação em nuvem sobre esses dados (ou seja, seu armazenamento em provedores de computação em nuvem) pode oferecer sérios riscos legais ao custódio, no caso, às organizações. Uma forma de contornar esse problema é fazer com que as organizações cifrem os dados antes de subirem (upload) os dados para os provedores. Dessa forma, elas garantem o sigilo dos dados independentemente das ações do provedor de computação em nuvem sobre os mesmos e, portanto, reduzem consideravelmente o risco legal do seu modelo de negócios.

b) Jurisdição. Dados submetidos à nuvem de certa localização geográfica podem estar armazenados em outra completamente diferente e, portanto, estarem sujeitos a leis que não correspondem às de seu lugar de origem. Pior, dado que em computação em nuvem é difícil apontar onde certo dado se encontra (muitos provedores possuem centros de dados (data centers) espalhados pelo globo), existe certa incerteza jurídica, o que, por sua vez, causa apreensão e desestimula seus potenciais usuários. Novamente, uma solução seria as organizações cifra-

rem os dados antes de subi-los (upload) para a nuvem. Nesse caso, o sigilo dos dados estaria garantido e sua informação pouco sujeita às idiossincrasias de cada jurisdição.

c) Intimações judiciais. Caso uma organização torne-se alvo de investigação, a justiça pode requisitar acesso a seus dados. Se dados são armazenados na nuvem, a requisição pode ser feita diretamente ao provedor, até mesmo sem que a organização tome ciência. Ademais, ao consultar dados de investigados, a justiça pode, ainda que não intencionalmente, se deparar com dados de outrem. Isso porque provedores usualmente armazenam dados de múltiplos clientes em um mesmo disco físico. Isso tudo desestimula a adoção de computação em nuvem. O emprego de criptografia, novamente, pode mitigar tais inconveniências. No caso, é possível atrelar o acesso aos dados ao emprego da chave criptográfica privada, a qual é particular e intransferível e ficaria em posse exclusiva da organização. Em outras palavras, qualquer requisição teria que passar obrigatoriamente pela organização.

d) Brechas de segurança. Ainda que provedores de computação em nuvem levem a sério a adoção de boas práticas de segurança, existe sempre a possibilidade dos mesmos sofrerem ataques devido a brechas em sistemas. Caso isso ocorra e haja vazamento de dados de terceiros, organizações podem ser responsabilizadas. Se soluções criptográficas forem adotadas, o sigilo dos dados é garantido e sua integridade pode ser aferida a qualquer momento. Assim sendo, brechas de segurança apresentariam pouco ou nenhum risco às organizações.

e) Retenção ou descarte de informação. Muitas vezes a responsabilidade pela devida retenção ou descarte de informação de terceiros é das organizações. Se a informação estiver na nuvem, contudo, pode ser difícil verificar sua integridade ou mesmo se foi efetivamente descartada. O uso correto de criptossistemas, contudo, atenua esses problemas. O uso de assinaturas digitais provê formas de se checar a integridade dos dados, ao passo que a destruição da chave criptográfica usada na cifração (*encryption*) dos mesmos garante seu descarte.

3. Privacidade

Nunca antes dados puderem ser acessados tão eficientemente e numa escala tão grande (MASIELLO; WHITTEN, 2010). A internet e a web em particular permitem que instituições privadas, organizações governamentais ou mesmo indivíduos tenham acesso a enormes fontes de dados. Sem dizer que esses dados podem ser apreciados de forma agregada e correlacionada, destacando a interdependência entre os mesmos. Na medida em que tecnologias móveis vão sendo rapidamente adotadas, tornando a computação não apenas ubíqua, mas também pervasiva (*pervasive*), outras classes de dados (de localidade, por exemplo) tendem a aparecer, aumentando ainda mais a abundância de dados. As implicações não concernem apenas à sociedade e à forma com a qual ela se interage. Ela diz respeito também à maneira com a qual fazemos ciência.

Se obtivermos êxito em extrairmos informações dessa profusão de dados, poderemos resolver vários dos problemas que hoje afligem a sociedade. Em outras palavras, se através de análises estatísticas ou mineração de dados angariarmos informações acuradas, seremos capazes de conceber soluções para, por exemplo, monitorar pandemias, antever tendências (de diferentes naturezas) e aumentar a transparência do consumo de recursos públicos.

Analisemos com mais detalhe o monitoramento de pandemias. O Google, por exemplo, possui um serviço chamado *Google Flu Trends*. Ele objetiva a identificação de surtos de doenças em estágio embrionário (note-se que esse é um problema que, caso solucionado, poderia evitar grandes pandemias). Imagine um médico que, logo no início do plantão, consultasse um paciente com sintomas de gripe. De posse do prontuário médico do indivíduo, isoladamente, o plantonista provavelmente iria apenas receitar antigripais e repouso, ainda que o início de uma epidemia estivesse se originando ali. Caso, por outro lado, o médico tivesse ciência das informações sobre muitos ou todos os demais pacientes, ele certamente seria capaz de identificar o início de um surto de uma (eventualmente nova) doença.

Paralelamente à profusão de informações e seus benefícios, surge também certa inquietação. Parte dela advém da preocupação acerca da privacidade. A possibilidade de coleta desse enorme volume de dados lança questões quanto ao acesso não autorizado de informações e, por conseguinte, à violação de privacidade. Assim, por um lado estamos permeados de dados que, se legalmente disponibilizados e competentemente analisados, podem servir à sociedade. Por outro, existe o anseio natural e, deve ser frisado, legítimo de se manter dados alheios secretos. Nesse contexto, surge a seguinte questão: é possível preservar a privacidade sem restringir a coleta e análise de dados?

Para respondermos a essa pergunta, temos que primeiro poder responder a questões mais diretas, mas ainda muito desafiadoras, a saber (MASIELLO; WHITTEN, 2010):

a) Relacionar ações de um mesmo indivíduo sem que o mesmo seja identificado. Grande parte dos benefícios trazidos pela

análise de dados refere-se a estatísticas acerca de indivíduos. Portanto, é de suma importância correlacionar ações de uma mesma pessoa. Em verdade, mais que isso. É preciso colocar essas ações em sequência. Assim sendo, é possível projetar formas de registrar e manter a sequência de ações de indivíduos sem, no entanto, identificá-los?

b) Possibilitar aos usuários usar sem abusar dos sistemas. Parte das razões para o monitoramento do uso de sistemas advém da necessidade de impedir seu abuso. Por exemplo, o monitoramento de conteúdo de mensagens busca filtrar spams, impedindo que sistemas sejam vítimas de ataques de negação de serviço (denial of service) ou que usuários caiam em golpes (phishing). Como então monitorar sistemas, impedir seu abuso e ainda preservar a privacidade?

c) Dar ciência sobre a reputação sem revelar informação adicional. Comumente indivíduos buscam informações acerca deles próprios para tomarem conhecimento sobre o que se sabe a seu respeito, isto é, para conhecerem sua própria reputação. Frequentemente, essa curiosidade é motivada pelo desejo de saberem se houve alguma violação de sua privacidade. Muitas vezes, paradoxalmente, essa busca era justamente a informação que faltava para que outros lograssem violar sua privacidade. Logo, uma questão que surge naturalmente é a seguinte: como possibilitar aos usuários saberem sobre sua reputação preservando sua privacidade?

A lista acima definitivamente não é exaustiva. Existe quase uma infinidade de questões a serem abordadas do ponto de vista científico para que possamos, com propriedade, responder à pergunta original, ou seja, se é possível preservar a privacidade sem restringir a coleta e análise de dados.

4. Potenciais soluções

Embora os desafios de computação em nuvem e privacidade supracitados possam ser abordados com primitivas criptográficas tradicionais (algoritmos de assinatura digital ou cifras tradicionais, o DAS/RSA, por exemplo), seu emprego resultaria em considerável sobrecarga (overhead) de comunicação e computação.

Para ilustrar, considere um caso de computação em nuvem. Imagine uma organização que cifra e assina seus dados antes de subi-los (upload) para a nuvem. Por um lado, isso de fato preserva o sigilo e a integridade dos dados. Por outro, faz com que a organização tenha que armazenar um índice localmente ou baixar toda a informação, decifrá-la, para então realizar a busca. Acerca da integridade e autenticidade dos dados, analogamente, nota-se que as organizações teriam novamente que reaver todos os dados para poderem verificar assinaturas. Em todos esses casos fica evidente a perda dos benefícios advindos do uso de computação em nuvem.

Felizmente, existem criptossistemas emergentes que, embora diferente dos tradicionais, podem ser empregados para tanto proteger computação em nuvem de forma mais efetiva, como para aprimorar os processos de garantia de privacidade. São eles:

a) Cifração consultável (searchable encryption). Essa classe de criptossistemas oferece formas de cifrar um índice de busca de forma que apenas indivíduos autorizados possam acessá-los. Em outras palavras, considere um índice gerado a partir de uma coleção de arquivos. Usando um esquema de cifração consultável, o índice da busca é cifrado de forma que apenas aqueles autorizados a buscar por uma palavra-chave podem reaver ponteiros para criptogramas (arquivos cifrados) que contêm aquela palavra-chave. Existem diversas subclasses de cifração consultável (simétrica, assimétrica, multiusuário, etc.) e a melhor depende do contexto em que é empregada.

b) Cifração baseada em atributos (attributed-baseden cryption) Essa é uma nova classe de técnicas criptográficas que permite que políticas de decifração sejam associadas a criptogramas. Em particular, conjuntos de atributos são associados a chaves de decifração e, em seguida, atribuídos a usuários. Paralelamente, usuários podem cifrar mensagens com chaves atreladas a certa política. Dessa forma, a decifração de uma mensagem será bem-sucedida apenas se os atributos associados à chave de decifração casarem com a política usada para cifrá-la.

c) Provas de armazenagem (proof of storage). Um protocolo do tipo prova de armazenagem é aquele que fornece formas de um servidor provar a um cliente que seus dados continuam íntegros. As principais vantagens desse tipo de protocolo são: (i) podem ser executados quantas vezes for necessário e (ii) a sobrecarga (overhead) de comunicação entre o cliente e o servidor acarretada pelo protocolo é mínima.

Apesar dos criptossistemas acima serem mais efetivos ao abordarem problemas atuais de engenharia da segurança, eles estão longe de resolverem os diferentes tipos de problemas na área. Isso porque criptossistemas sozinhos são poucos efetivos. É necessário não apenas orquestrá-los em protocolos criptográficos, mas preencher adequadamente suas caixas-pretas (black-box) e implementá-los, considerando as idiossincrasias do ambiente em que serão executados.


Divulgação

A segurança e a informação

Bruno Castro

Gestor de Negócios e TI, com mais de 16 anos de vivência e aprendizado em TI. Consultor e gestor da Breed Consultoria há vários anos, com projetos e cases de sucesso em diversas empresas, de grande, médio e pequeno porte. Foi coordenador e professor em cursos de graduação, pós-graduação e MBA em universidades e centros universitários, com mais de 13 reconhecimentos formais como gestor, consultor, professor-paraninfo e patrono.

RESUMO

A segurança da informação não é uma novidade trazida pela informatização ou mesmo pela era moderna do século XXI. Para entender de forma sólida a síntese do conhecimento acerca desse assunto, este artigo volta aos primórdios dos registros do ser humano neste planeta, detalhando de forma separada para depois unir: "a informação", "o valor da informação", "a segurança" e "a segurança da informação".

1. A informação

Palavra vinda do latim *informatio,onis*, informação significa "delinear" ou dar forma na mente para "aquilo que se vê". Portanto, pode ser entendida como registro de um acontecimento, evento, organização de dados, descrição de um conhecimento e outras definições. Um evento ou um acontecimento, por mais importante que seja, é somente um evento isolado e sem possibilidade de ser lembrado, se não for registrado por algo ou por alguém.

Desde o surgimento do universo, a natureza registra informações que até hoje são aos poucos entendidas, analisadas e nos permitem tirar conclusões sobre os acontecimentos do passado. Foram através desses registros da natureza que o ser humano conseguiu estimar a idade do planeta e, por exemplo, saber que a Terra já passou por cinco períodos glaciais no último bilhão de anos. Essas informações da natureza também permitiram aos humanos entenderem a evolução das espécies e várias outras descobertas que sempre estiveram ao nosso alcance, à nossa disposição, desde o início de nossa espécie.

Além da natureza, seres vivos também conseguem registrar informações desde os seus primórdios. Os seres humanos da Idade da Pedra devem ter aprendido rapidamente o quão útil seria registrar em suas memórias acontecimentos, locais privilegiados ou mesmo reconhecer perigos mediante lembranças. Essas informações seriam rapidamente perdidas se esses humanos do passado não pudessem replicá-las a outros seres humanos, e então surgiu a ideia de registro dessas informações nas paredes das cavernas, com os famosos desenhos que registraram acontecimentos e crenças daquela época.

Muitos anos se passaram e os seres humanos conviveram com um problema desse método de armazenamento da informação, pois, quando se mudavam de um local para outro, a informação era perdida, e outros vários anos se passaram até que na Antiguidade inventaram (ou descobriram) o papiro, papel que foi uma verdadeira revolução no registro da informação.

Com a invenção da imprensa por Gutenberg em 1439, o papel tornou-se um meio eficaz de não só armazenar a informação, mas também replicá-la. No século XX, com a chegada da informática, uma nova revolução aconteceu, permitindo à raça humana armazenar, gerir e processar a informação a limites até então inimagináveis. Alguns anos depois, explode o uso da internet no planeta Terra, fazendo com que a informação seja também circulada e compartilhada a limites também até então inimagináveis!

Portanto, a informação sempre

existiu, desde que o mundo é mundo, desde que a Via Láctea foi formada. Ela está e sempre esteve presente. O que muda nos dias de hoje é a capacidade humano de armazenar, gerir e compartilhar a informação com uma força cada vez maior.

2. O valor da informação

O valor de uma informação é e sempre será relativo. Relativo a quanto importante ela é, a quão rara é e a quanto ela pode modificar algo ou mesmo alguém se utilizada de forma estratégica no momento certo. Para entender melhor o quanto pode valer ou não uma informação, uma boa técnica seria sempre analisá-la sobre o aspecto de seu "poder de modificação" em relação ao tempo ou ao momento em que se utilizará a informação. Explica-se com os exemplos a seguir:

a) Em um jornal tem-se a seguinte manchete: "Extra!! Extra!! Confidencial!! O fabricante de veículos Alpha lançará o novo carro Beta!!".

Dependendo do quão confidencial fosse esse novo projeto, e o quão se investiu em um lançamento surpresa desse veículo, uma informação dessa, que "vazasse" de alguma forma da fábrica, poderia causar facilmente prejuízos de milhões de reais ao fabricante que, devido ao "vazamento" da informação, teria que rever as campanhas de *marketing* planejadas ou até mesmo mudar a data de lançamento frente às novas ações da concorrência e do mercado por causa da divulgação dessa informação. Certamente, no momento do planejamento até o seu lançamento, é uma informação de alto valor e que, se não utilizada e manuseada conforme planejado, poderá jogar todo um esforço corporativo a perder. É uma informação de alto poder de modificação naquele determinado momento.

De toda forma, após um pequeno espaço de tempo da divulgação oficial ou não dessa informação, ela passa a ser um informativo do passado, reduzindo consideravelmente o seu valor. Ela pode continuar interessante para historiadores, colecionadores de notícias, ou mesmo para pessoas que ainda não souberam da novidade. Porém, como essa informação é agora algo associado ao passado, atribui-se pequeno poder de modificação nesse momento "pós-novidade".

O valor financeiro dessa informação estará diretamente ligado aos danos financeiros que causariam à organização que a possui e que luta para mantê-la em sigilo.

b) Em uma conversa informal alguém anuncia: "Nossa empresa está fechando um negócio de milhões com o cliente XYZ".

Sendo uma informação estratégica de uma negociação recente, essa informação poderia valer milhares ou milhões de reais, sem mesmo que o interlocutor da mesma pudesse ter conhecimento. Basta imaginar como essa informação poderia ser manuseada por concorrentes, fornecedores e outros clientes, ou mesmo caracterizar uma quebra contratual, gerando grandes multas por divulgação antecipada da negociação.

Porém, sendo uma informação não mais estratégica, após a definição das regras de negócio, operacionalização do negócio e formalização da negociação, provavelmente ela se tornaria uma informação histórica, de pouco valor financeiro aos concorrentes, fornecedores e demais clientes.

O valor financeiro dessa informação estará diretamente ligado ao quão uma pessoa jurídica ou física poderia deixar de lucrar ou ainda perder baseado na utilização indevida dessa informação.

c) Um amigo anuncia: "Houve uma colisão entre dois carros com capotamento na avenida Afonso Pena com avenida Brasil".

A informação poderia causar espanto ou mesmo curiosidade, mas poderia ser de baixo valor se nada pudesse ser feito a respeito (baixo poder de modificação de algo).

Por outro lado, poderia ter algum valor para o ouvinte que, ao saber da informação, alterou o seu trajeto para evitar o congestionamento causado pela colisão.

O valor financeiro dessa informação estará diretamente ligado ao quanto alguém poderia economizar ou deixar de perder baseado, por exemplo, no desvio de trajeto entre dois pontos na cidade, evitando o local onde há impeditivo de se trafegar.

Em resumo, o valor da informação estará diretamente ligado ao seu poder de mudança ou transformação em relação ao tempo e à forma em que será utilizada.

3. A segurança

A palavra segurança tem origem no latim *securus*, que significa "sem temor, garantido" e, embora sugira diretamente o que a maioria das pessoas entende por segurança, é possível afirmar: "Nada é 100% seguro ou 100% garantido".

Segurança está diretamente ligada à redução dos riscos de acontecimento de algo. Está referida como um mal a ser evitado e está diretamente ligada à tentativa de ausência de ris-

co e à tentativa de certeza quanto ao futuro. O quão mais seguro se está depende do quão foi possível reduzir os riscos de acontecimento de algo (problemas que deseja evitar). É possível ter alta segurança quando há baixos riscos. É possível ter baixa segurança quando há altos riscos.

Segurança, portanto, é nada mais e nada menos do que a relação entre o segurado e o risco, e a dedicação a tornar algo seguro estará sempre focada na redução desses riscos.

Para reduzir os riscos e consequentemente tornar algo seguro, é possível sintetizar três importantes fatores:

a) conhecimento: o conhecimento em relação ao que se deseja proteger;
b) estratégia: a estratégia correta de segurança em relação ao que se deseja proteger;
c) ação: os esforços (inclusive financeiros) e as ações para implementar a estratégia adotada para reduzir os riscos.

Quanto maior for o conhecimento de quem irá proteger algo ou alguém tanto maior será sua capacidade de proteger. Mais importante inclusive do que as ferramentas que serão utilizadas na proteção, o conhecimento permitirá a elaboração das estratégias mais eficazes para se reduzir os riscos.

As estratégias de segurança permitirão a quem irá proteger algo ou alguém fazê-lo de forma assertiva. Toda redução de riscos pressupõe, além de entendimento (conhecimento), a análise de riscos e possibilidades de acontecimentos, necessitando, assim, de pensamento, de inteligência, de estratégia.

De nada adianta o conhecimento e a estratégia se não houver ações concretas para se reduzir os riscos. Essas ações, resultado do conhecimento e do pensamento estratégico, implementarão medidas de redução de riscos, trazendo, então, o conceito de segurança ao segurado.

Outro ponto interessante é que se pode dizer que não há limite para se reduzir os riscos ou aumentar a segurança de algo ou alguém. À medida que se aumenta os esforços (inclusive financeiros) para a redução dos riscos, espera-se um consequente aumento na segurança do segurado, se unidos os três pilares: conhecimento, estratégia e ação.

Sugere-se, assim, que se encontre um equilíbrio entre os valores do que se deseja proteger (segurado) e os valores despendidos nos esforços para reduzir riscos (aumento de segurança). Tornar algo seguro ou proteger algo está diretamente ligado à quantidade de esforço (inclusive financeiro) que se deseja fazer para reduzir riscos.

4. A segurança da informação

A informação sempre existiu. O valor da informação, mesmo que relativo, sempre existiu. O conceito de segurança sempre existiu. E a segurança da informação? A resposta é simples: também sempre existiu.

Sempre que houve a necessidade de se proteger uma informação, geralmente valiosa financeira ou estrategicamente, o homem trabalhou para protegê-la. A segurança da informação, ao longo da história humana, possibilitou a permanência ou a queda de impérios, civilizações, governos, grandes organizações e muitos outros resultados de impacto, pelo simples fato da informação estar guardada ou não no momento certo. Basta lembrar-se do conceito do "poder de modificação", relacionado ao tempo e à forma em que a informação é utilizada.

Mas por que este assunto (a segurança da informação) é cada vez mais discutido, lido e estudado? A resposta poderia ser encontrada nas seguintes constatações em nível mundial:

a) a informática: por causa dos computadores, lidamos com um número cada vez maior de informações;
b) a internet: por causa das redes de computadores, transitamos e compartilhamos um número cada vez maior de informações;
c) a Era da Informação: lidar com informações é pré-requisito para viver no planeta Terra no século XXI.

Segundo pesquisa do Instituto Gartner em 2009, o mundo já havia ultrapassado a marca de um bilhão de computadores. Em 2014, a previsão seria atingir a marca de dois bilhões de computadores, chegando à média de um computador para cada três pessoas no planeta Terra.

A internet já conta com mais de dois bilhões de usuários, segundo a União Internacional de Telecomunicações (UIT) da ONU (Organização das Nações Unidas), e recebe, por dia, mais de 500 mil novos internautas.

A era em que os seres humanos vivem atualmente, pós-Era Industrial, trouxe mais do que uma mudança social, uma mudança na condição da vida humana, sendo as capacidades criativas e pensantes aliadas ao manuseio da informação, à base do funcionamento e ao sucesso das pessoas e empresas na economia mundial.

Para se ter uma ideia da importância da informação na era em que vivemos, citam-se os seguintes exemplos:

a) a maioria do dinheiro que circula no planeta é apenas informação;

De fato, as instituições financeiras possuem alguma quantidade de dinheiro vivo em seus cofres, mas os valores dos correntistas nada mais são do que bit e byte nos computadores que armazenam e processam tais informações.

b) o maior valor financeiro das grandes marcas mundiais é apenas informação;

A maioria das empresas com grandes marcas tem maior valor financeiro atrelado a suas marcas e a suas informações de resultados do que ao seu patrimônio líquido.

c) o trabalho de grande parte das pessoas no século XXI está relacionado aos computadores;

De fato boa parte do esforço produtivo em nível mundial não pode ser sequer tocado, pois está todo em meio digital.

d) empresas têm cada vez mais suas informações nos computadores;

Devido à concorrência em quaisquer níveis, mundial, regional ou local, tem sido difícil encontrar empresas sem qualquer índice de informatização. O motivo é simples: fica difícil competir no mercado de hoje sem a melhoria de eficiência da informática. Para muitos empresários, computadores representam verdadeiro "terror" à sua gestão do negócio. Mas, mesmo assim, não podem ficar livres deles sob pena de não conseguirem ser competitivos.

O assunto "segurança da informação" ganhou e tem ganhado tanta força que recentemente surgiram padrões e melhores práticas em nível mundial para sua aplicação. A organização mundial ISO (International Organization for Standardization) oficializou no final dos anos 90, a partir de padrões nascidos na Inglaterra, a norma ISO/IEC 17.799. Essa foi uma das primeiras normas de segurança da informação de grande relevância em nível mundial. O sucesso foi tanto que, no início dos anos 2000, a organização ISO decidiu por adotar uma numeração dedicada à segurança da informação, conhecida como família de normas 27.000.

Dentro da família ISO 27.000, é possível encontrar seis documentos divididos em:

a) ISO 27.001 – especificação para um sistema de gestão da segurança da informação;
b) ISO 27.002 – seria a principal norma da família e especifica um conjunto de melhores práticas para a segurança da informação em uma organização (foi originalmente a ISO/IEC 17.799);
c) ISO 27.003, 27.004, 27.005 e 27.006 – metodologias e padrões de gestão de sistemas, riscos e certificações.

Como a maioria das normas e conceitos de melhores práticas, esses documentos detalharão "o que fazer" e não "como fazer", ficando este último para ser desenvolvido pela instituição que deseja implantar o conceito.

Pode-se definir, finalmente, que "segurança da informação" é todo e qualquer esforço para reduzir os riscos de uso indevido de uma informação. Sua importância nos dias atuais é imensa, uma vez que problemas de segurança da informação podem facilmente levar a prejuízos financeiros e estratégicos muito piores do que problemas físicos de segurança. Basta constatar que um roubo de informações digitais pode superar em quantia financeira diversos roubos em forma física de bens ou de valores financeiros.

Esse é um assunto que já é discutido nos dias de hoje e que inevitavelmente será abordado com cada vez mais frequência dentro das organizações do planeta. Se sua empresa ou organização ainda não se preocupou com esse assunto, tenha apenas uma certeza: ela ainda o fará e, provavelmente, bem antes do que seus integrantes esperam!

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *Tecnologia da informação – Código de prática para a gestão da segurança da informação* (NBR ISO/IEC 17.799). Rio de Janeiro, RJ: 2001.

THE ISO 27.000 DIRECTORY. *An Introduction do ISO 27.000*. 2010. Disponível em: <http://www.27000.org/index.htm>. Acesso em: 25 set. 2012.

INFO PLANTÃO. *Mundo tem 1 bilhão de PCs, diz Gartner*. São Paulo, 2008. Disponível em: <http://origin.info.abril.com.br/aberto/infonews/062008/23062008-8.shl>. Acesso em: 10 set. 2012.

COMPUTER WORLD. *Estudo aponta que empresas têm problemas para gerenciar dados*. São Paulo, 2010. Disponível em: <http://computerworld.uol.com.br/gestao/2010/08/11/estudo-aponta-que-empresas-tem-problemas-para-gerenciar-dados/>. Acesso em: 02 jan. 2011.

Júlia Magalhães

Crônica de uma morte exagerada

Obituários da privacidade na sociedade em rede

Gustavo Grossi de Lacerda

Publicitário (UFMG), mestre em Comunicação Social (PUC Minas), MBA em Marketing (FGV) e especialista em Comunicação e Gestão Empresarial (IEC/PUC Minas). Gerente de Marketing da Prodemge.

RESUMO

O processo de publicização da vida privada acirrou-se de forma exponencial na era das mídias sociais, videovigilância e reality shows. A vida on-line põe a privacidade em xeque de modo contundente na atual esfera pública interconectada. Vive-se hoje a emergência de um complexo ecossistema digital, conjugado a um ethos de espetacularização da intimidade. Nesse contexto, a privacidade está em xeque, e determinados atores sociais sequer hesitam em declará-la extinta e substituída pela publicidade como norma vigente na rede. O presente artigo problematiza esses discursos e chama atenção para as tensões e interesses envolvidos na questão.

"Nossas vidas parecem muito mais interessantes quando filtradas pela interface sexy do Facebook. Estrelamos nossos próprios filmes, fotografamos incessantemente a nós mesmos [...]. Curtimos o espelho e o espelho nos curte. Ser amigo de uma pessoa significa incluí-la em nossa lista particular de espelhos elogiosos."

Jonathan Franzen, em Como Ficar Sozinho (2012)

1. O caminho da ironia

A vida on-line extinguiu a privacidade?

Nos idos de 1897, o escritor Mark Twain (1835-1910) veio a público desmentir notícias fúnebres a seu respeito, com uma declaração que ficou famosa: "Os relatos sobre minha morte são exagerados". Hoje, proclama-se de modo recorrente o fim da privacidade em tempos de videovigilância ubíqua, *reality shows* dominantes nas grades de programação das TVs, superexposição pessoal nas mídias sociais e tecnologias invasivas web 3.0. Mas é prudente, seguindo a verve irônica de Twain, verificar se há exageros nesses obituários, bem como os interesses daqueles que se apressam a redigi-los e divulgá-los.

Quem são os redatores desses obituários? Quais as razões da naturalização da exibição pessoal nos ambientes digitais? Afinal, o que está em jogo nos discursos que, em detrimento do direito à privacidade, enunciam a elevação de certo tipo de publicidade exacerbada ao status de norma social vigente na rede?

Este artigo aborda essas questões num momento em que os habituais regimes de visibilidade estão em transição. Seu objetivo é chamar atenção para as implicações e fundamentações discursivas ligadas ao processo de publicização da vida privada em curso nos ambientes digitais, com ênfase nas redes sociais – e foco especial no Facebook. Desse modo, cabe primeiro tecer considerações de ordem conceitual, para, depois, examinar e traçar paralelos entre falas, eventos históricos e casos emblemáticos que refletem as tensões e embates em torno da privacidade na sociedade (do espetáculo e do controle) em rede.

2. A realidade ampliada

A sociedade contemporânea, tal como descrita por Manuel Castells (2002), caracteriza-se por trocas e fluxos informacionais incessantes de capital e cultura que circulam em redes que são a chave de sua organização e morfologia. No cotidiano on-line dessa *sociedade em rede*, o

processo de publicização da vida privada acirrou-se de forma exponencial, vide a eclosão das mídias sociais na web. Os desdobramentos desse fenômeno se emaranham numa intricada trama de eventos que põem em xeque conceitos, saberes e competências, no âmbito cultural, comunicacional, técnico-científico, econômico, político e jurídico.

Um cenário em plena ebulição, no qual indivíduos, grupos, coletividades, organizações públicas e privadas estabelecem laços, promovem trocas e fazem negócios, por intermédio de uma profusão de novas modalidades de interação virtual. Publicar, buscar, acessar, compartilhar, postar, curtir, adicionar, convidar, cutucar, tuitar, remover, incluir, excluir, vazar, baixar, subir, rastrear... A cada instante o vocabulário do dia a dia incorpora neologismos ou ressignifica termos relacionados a serviços e dispositivos tecnológicos que facilitam a exposição e o compartilhamento voluntário de conteúdos, em especial aqueles relativos a dados privados.

Observam-se, assim, sensíveis mudanças nos regimes de visibilidade atuais. Sobrevém o fato de que essa miríade de pessoas e instituições, a interagir vertiginosamente em rede, agora é composta por produtores-consumidores de conteúdos. O modo centralizado de produção-emissão característico das mídias irradiadas de massa é desafiado pela lógica reticular das mídias distribuídas de grupo, cujo epicentro é a internet.

Trata-se da emergência de um complexo ecossistema digital conjugado a um *ethos* de espetacularização da intimidade. O que implica aliar a fome por informação dos conglomerados midiáticos do novo capitalismo digital, em luta por hegemonia na sociedade em rede, à vontade do usuário de ver, se ver e ser visto em um espaço público interconectado.

Contudo, nem toda exposição on-line é voluntária. Quando um dispositivo pessoal ou corporativo conecta-se à rede, abrem-se flancos para práticas sub-reptícias de vigilância, controle, identificação e coleta de informações relativas a indivíduos e organizações. Todos estão interconectados em algum nível, e, com a plasticidade digital das novas mídias, o que cai na rede torna-se passível de usos e abusos à revelia de seus usuários. Vale ressaltar que essa ambiência não é prerrogativa do espaço informacional. Sensores e tecnologias discretos monitoram também o chamado espaço físico, de modo a criar uma espécie de realidade ampliada (BRUNO, KANASHIRO, FIRMINO, 2010), na qual tudo está imerso e sujeito a algum tipo de registro.

3. A força dos laços fracos

Nos discursos em torno da privacidade nas redes, é corriqueira a apologia da transparência como valor absoluto. Também é comum que o sacrifício da privacidade seja justificado em nome do que Andrew Keen – historiador, empreendedor do Vale do Silício e crítico severo das redes sociais – define como "tirania utilitária de uma rede coletiva" (KEEN, 2012, p.23). Subjacente a esse viés utilitarista, uma era de superexposição de dados privados on-line se instaura na sociedade interconectada. Renunciar ao direito à privacidade em favor da publicidade e da transparência em rede seria, nessa perspectiva, um sacrifício individual menor e inevitável, válido pelo usufruto geral dos benefícios da interconexão global.

Segundo os pesquisadores Barry Wellman e Lee Rainie, em matéria publicada na *Folha de S. Paulo*[1] (19/11/2012), a sociedade colhe hoje os benefícios da efetiva integração da sociedade que as mídias sociais propiciam. Eles argumentam, com base em pesquisas do Pew Research Center[2], que redes sociais digitais estão substituindo grupos coesos, pequenos e fechados, constituídos por familiares, amigos, vizinhos e lideranças comunitárias, na oferta de proteção e auxílio recíprocos. Um fenômeno que só faz aumentar na medida em que se ampliam o acesso à banda larga e o uso de dispositivos móveis, tais como tablets e smartphones. Agora, de acordo com Wellman e Rainie, vive-se um paradoxal novo mundo de individualismo conectado, em que grupos mais soltos e fragmentados se ajudam mutuamente, propiciando maior interação e integração social.

Nesse sentido, destacam-se os chamados laços fracos na disseminação de informações na web, em especial nas redes sociais. Pois esses laços – conexões caracterizadas pela pouca intimidade ou proximidade entre os usuários – são os maiores responsáveis por manter a rede interconectada e fazer com que a informação se amplifique e atinja mais pessoas (ZAGO, 2011). Entretanto, não se trata apenas de difundir informação. Conforme matéria da *Technology Review* (MIT), reproduzida na *Época Negócios*, em agosto deste ano, estudos re-

1 Disponível em <http://www1.folha.uol.com.br/tec/1186647-estudos-reabrem-debate-sobre-o-impacto-de-redes-sociais-na-vida-das-pessoas.shtml>. Acesso em: 20 nov. 2012.
2 Disponível em <http://pewinternet.org/Reports/2012/Online-Pictures.aspx>. Acesso em: 20 nov. 2012.

alizados pelo Data Science Team[3] do Facebook demonstram ser significativa a influência de amigos ou contatos próximos (laços fortes) nas informações compartilhadas na rede social; não obstante, essa influência está bastante aquém daquela exercida por um conjunto de laços fracos que define, em grande medida, a que tipo de informações os usuários são expostos.

Essa sociabilidade em rede, com suas práticas, valores e processos comunicativos ligados à lógica das mídias distribuídas de grupo, afeta profundamente a relação entre pessoas e organizações. Como visto no item anterior, os indivíduos agora são também produtores e disseminadores de conteúdos nas redes, com meios de expressão e influência antes inimagináveis. Instâncias públicas, privadas e do terceiro setor, além da própria mídia tradicional, se veem na contingência de formular estratégias de presença nesses ambientes digitais, para estabelecer canais de relacionamento on-line, prestar contas e proteger ou incrementar suas marcas. Difícil missão esta, a de acompanhar e tentar responder de forma coerente à dinâmica mutante de um cotidiano on-line que a todos desafia.

Cenário no qual Wellman e Rainie não constatam evidências sistemáticas de que as redes sociais tenham um efeito desagregador, ao contrário do alarido das críticas. Uma conclusão diametralmente oposta ao teor das recriminações alardeadas por Andrew Keen (2010), para quem as redes sociais estão dividindo, diminuindo e desorientando usuários que se associam a identidades criadas virtualmente, em prejuízo de suas próprias identidades.

Não obstante, a despeito das razões e desrazões que movem detratores ou apologistas das mídias sociais, há certo consenso quanto à sentença de que a privacidade estaria ameaçada, ou até mesmo condenada, pelas contingências da vida on-line – os dois pesquisadores e o historiador convergem quanto à ameaça à privacidade e aos riscos do uso indevido de dados de usuários por grandes conglomerados e entidades governamentais[4].

4. A mensuração da felicidade

Retoma-se aqui a reflexão sobre a perspectiva utilitarista de discursos que apregoam o sacrifício da privacidade em prol de um bem maior. Discursos como o de Mark Zuckerberg, fundador do Facebook, que declarou a privacidade extinta[5], em janeiro de 2010. Na ocasião, Zuckerberg justificou o sentido de alterações na política de privacidade da rede social com base em evidências de que a publicidade ascendera ao posto de valor hegemônico na rede. Desse modo, a maioria dos usuários da web no planeta teria decidido, por livre escolha, "curtir" os benefícios da publicização de seus dados privados nas redes sociais.

Dois anos depois dessa declaração, a "nação Facebook" só fez crescer, alcançando a marca de 1 bilhão de habitantes virtuais. Uma nação que produz índices peculiares. A equipe do Data Science Team do Facebook concebeu um modo de calcular a "Felicidade Interna Bruta" de um país a partir de dados computados pela rede social. Versão alternativa do usual Produto Interno Bruto (PIB), a elaboração do índice utilizou o registro de ocorrências de termos e frases que denotam emoções positivas ou negativas para gerar um modelo estatístico de análise de tendências sociais.

Não à toa, os críticos das mídias sociais retomam o fio da história para associar os princípios da filosofia utilitarista – que não tinha em grande conta a privacidade – às ideias professadas por visionários contemporâneos da web 3.0. O utilitarismo é uma linha de pensamento que busca estabelecer o cálculo do bem comum, ao propugnar uma ética de maximização da *utilidade* e da *felicidade* como resposta às questões sobre como conduzir a vida em sociedade. Seu maior expoente é o filósofo, jurista e reformador social inglês Jeremy Bentham (1748-1832)[6], autor do lema: "A maior felicidade possível para o maior número possível de pessoas".

Bentham celebrizou-se ainda pela concepção do panóptico, um modelo de prisão circular que propiciava ao observador a visualização de todos os locais onde estivessem os presos – ou alunos, trabalhadores e pacientes, uma vez que o modelo fora projetado para funcionar também em escolas, oficinas e manicômios. Transparência aí implicava, portanto, racionalização, eficiência, visibilidade e controle, na esteira de processos de disseminação progressiva e sistemática de dispositivos disciplinares nas instituições da sociedade ocidental (FOUCAULT, 2009).

3 O Data Science Team do Facebook (http://pt-br.facebook.com/data) é um "núcleo que usa ferramentas como a matemática, a programação, a psicologia e a sociologia para garimpar dados e fazer avançar o negócio da companhia", de acordo com reportagem da *Technology Review*, publicada na revista *Época Negócios*, em agosto de 2012.

4 Disponível em <http://www1.folha.uol.com.br/tec/1186647-estudos-reabrem-debate-sobre-o-impacto-de-redes-sociais-na-vida-das-pessoas.shtml>. Acesso em: 20 nov. 2012.

5 Disponível em <http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov>. Acesso em: 20 nov. 2012.

6 Disponível em <http://pt.wikipedia.org/wiki/Jeremy_Bentham>. Acesso em: 20 nov. 2012.

Tais dispositivos prefiguraram novos regimes de visibilidade e formas sutis e naturalizadas de vigilância (e voyeurismo) em rede, viabilizados pelo desenvolvimento intensivo das tecnologias da informação e comunicação, notadamente a partir da segunda metade do século XX. Trata-se, assim, da utilização de novos, sofisticados e (cada vez mais) dissimulados meios sociotécnicos para o exercício de monitoramento, coleta e manipulação de dados pessoais on-line. Nesse contexto, deve-se pensar em situações mais complexas, a exemplo das que dão ensejo a tensões e complementaridades entre os modelos panóptico, no qual poucos veem muitos, e sinóptico, em que muitos veem poucos (BRUNO, KANASHIRO, FIRMINO, 2010).

Outro aspecto dessas práticas de monitoramento e coleta de informações em rede é que elas apresentam ao menos duas faces, a proteção e o controle social. Visa-se à redução do risco de crimes e, de modo concomitante, permite-se "a organização de informações sobre certos indivíduos e grupos sociais que pode ser usada precisamente com o objetivo de supervisioná-los e controlá-los" (BOTELLO, 2010, p.18).

5. Os modelos de negócio

A organização das informações nos ambientes digitais pode ter aplicação ainda mais ampla no campo do marketing, de modo a explorar o veio de oportunidades aberto pelo lucrativo segmento dos Grandes Dados (Big Data). Quando representantes de conglomerados de mídia social anunciam o fim da privacidade, é preciso ter em mente que esse diagnóstico coincide com os modelos de negócio e os interesses estratégicos das empresas a que estão ligados. Nesse sentido, Fernanda Bruno aponta que companhias como o Facebook bradam pela redução da privacidade e, ao mesmo tempo, reivindicam com fervor "a sua própria privacidade quando são inquiridas acerca dos usos que fazem da massa de dados pessoais que capturam desses mesmos usuários (e em cujos bancos de dados residem as verdadeiras moedas de seus negócios)" (BRUNO, 2010)[7].

São precisamente as informações publicizadas voluntariamente pelos usuários nesses ambientes digitais que produzem outras camadas de dados passíveis de variados tipos de exploração – com efeito, os megavolumes de informação armazenados e processados nas bases de dados das grandes corporações das novas mídias se configuram como gigantescos e inestimáveis acervos informacionais. Para fazer a gestão dessas informações são desenvolvidas poderosas ferramentas e técnicas que geram conhecimento e, principalmente, capacidade de analisar preditivamente as ações das pessoas, com precisão e lucratividade[8].

Portanto, sob os termos de políticas de uso e privacidade em geral não verificadas com a devida atenção pelos usuários comuns, forma-se essa primeira camada de dados divulgados nas redes. Mas a atuação dessas empresas pode não se restringir à camada visível em que fornecem aos indivíduos meios e facilidades para o compartilhamento de toda sorte de dados pessoais. Conforme Ronaldo Lemos, "por trás das cortinas, os dados dos usuários são processados, gerando uma biografia permanente que analisa padrões de interação com outras pessoas, sites, buscas, compras e mais. Revela o corpo e a alma da pessoa." (LEMOS, 2012).[9] Nessa mesma perspectiva, Fernanda Bruno faz observação semelhante:

> Submetidos a técnicas de mineração e profiling, tais dados geram mapas e perfis de consumo, interesse, comportamento, sociabilidade, preferências políticas que podem ser usados para os mais diversos fins, do marketing à administração pública ou privada, da indústria do entretenimento à indústria da segurança, entre outros (BRUNO, 2010).[10]

Ora, é flagrante o desconhecimento dos usuários quanto ao destino de seus próprios dados nos ambientes digitais – independentemente de como se deu a inserção desses conteúdos (de modo espontâneo ou não). De acordo com Wellman e Rainier (2012)[11], qualquer informação que cai na rede ganha uma "vida social" que lhe confere um caráter público. Ademais, os ambientes digitais em rede são tão suscetíveis aos novos meios de monitoramento e manipulação de conteúdos quanto os usuários demonstram desconhecer o nível de sigilo e criticidade dos dados pessoais que publicam ou compartilham. Pesquisa recente do

7 Disponível em <http://dispositivodevisibilidade.blogspot.com.br/2010/01/o-fim-da-privacidade-em-disputa.html>. Acesso em: 20 nov. 2012.
8 De acordo com matéria da *Technology Review*, publicada na *Época Negócios*, em agosto de 2012.
9 Disponível em <http://www1.folha.uol.com.br/tec/1089398-somos-todos-carolina-dieckmann-nao-existem-mais-dispositivos-pessoais.shtml>. Acesso em: 20 nov. 2012.
10 Disponível em <http://dispositivodevisibilidade.blogspot.com.br/2010/01/o-fim-da-privacidade-em-disputa.html>. Acesso em 20 nov. 2012.
11 Disponível em <http://www1.folha.uol.com.br/tec/1186647-estudos-reabrem-debate-sobre-o-impacto-de-redes-sociais-na-vida-das-pessoas.shtml>. Acesso em: 20 nov. 2012.

Pew Research Center, realizada nos EUA, revelou que 42% dos usuários da web têm ciência de que possuem ao menos uma foto on-line; porém, o índice cai para 26% quando se trata de saber da presença do endereço de suas casas na rede.

Como e com o que exatamente alguém está se comprometendo ao instalar um software, baixar um aplicativo ou criar uma conta ou perfil em uma rede social? Quem, dentre o contingente de usuários de redes sociais e outros serviços on-line, tem o costume de ler ou consultar atualizações em termos de uso e políticas de privacidade? Pois são nesses documentos que as empresas buscam se respaldar no momento em que tomam a decisão de alterar ou pôr em prática novas regras. Tais questionamentos deveriam fazer parte de um processo de educação digital cuja premência é diretamente proporcional ao acirramento do processo de publicização da vida privada na sociedade em rede.

6. A lei para Carolina

Na contramão do que reza o senso comum, virtual não é o contrário de real. As contingências da vida on-line geram impactos concretos, variados, frequentes – e, por vezes, perturbadores. Vide o registro da ação insidiosa – e corriqueira – de criminosos cibernéticos contra indivíduos e organizações. Mas, se existe alguma apreensão com a eventual coleta e exposição não autorizada de dados e imagens privados em ambientes digitais, o comportamento de diversos segmentos de público parece não refletir tal preocupação.

A publicização quase compulsória da vida na sociedade em rede confirma a percepção inquietante de que o viver on-line desafia a todo instante o direito à privacidade – um fundamento do Estado Democrático de Direito. Daí ser um equívoco negligenciar os aspectos educacionais, comportamentais e legais envolvidos. Se mesmo quem toma os devidos cuidados está sujeito a ações criminosas em rede, o que se pode dizer daqueles que ainda carecem de adequada orientação e proteção?

Corroborando essa percepção, são eloquentes, embora não surpreendentes, os resultados da primeira pesquisa TIC Kids On-line Brasil[12], cujo objetivo principal é medir as oportunidades e os riscos relacionados ao uso da web. O estudo foi divulgado pelo Comitê Gestor da Internet no Brasil, em outubro de 2012. Foram entrevistados 1.580 pré-adolescentes e adolescentes usuários de internet, entre 9 e 16 anos, e o mesmo número de pais ou responsáveis. Os dados revelam a amplitude da exposição pessoal de jovens na internet e a falta de consciência de boa parte dos pais quanto aos riscos assumidos pelos filhos nesse ambiente:

- 70% dos entrevistados possuem perfil próprio em redes sociais – o uso das redes sociais no Brasil supera o das crianças e adolescentes europeias nessa faixa etária;
- 31% permitem que amigos possam acompanhar seus perfis públicos – nos quais qualquer um pode visualizar as atualizações;
- 37% dos pais e responsáveis acreditam que não é provável que seu filho passe por alguma situação de incômodo ou constrangimento na internet nos próximos seis meses;
- 71% dos pais acham que os filhos usam a internet com segurança;
- 35% acreditam que eles são capazes de lidar com situações que os incomodem na web;
- 23% dos usuários entre 11 e 16 anos já tiveram contato na internet com alguém que não conheciam pessoalmente; dentre esses, 25% declararam ter encontrado pessoalmente alguém que conheceram on-line;
- 47% de crianças e adolescentes entre 9 e 16 anos acessam a internet todos os dias ou quase todos os dias em diversos lugares: casas, escolas, lan houses.

O médico Jairo Bouer, em artigo na revista *Época*[13], publicado em novembro de 2012, abordou outras duas pesquisas brasileiras envolvendo jovens. A ONG Safernet[14], com atuação voltada para a segurança na rede, divulgou que, dos mais de 3 milhões de denúncias de crimes cometidos na internet no Brasil entre 2006 e 2012, 40% são casos de pornografia infantil. O Portal Educacional do Grupo Positivo também promoveu estudo que coloca em evidência a superexposição on-line e suas ameaças. Conforme a metodologia dessa pesquisa, jovens estudantes de 13 a 17 anos formularam questões que foram respondidas por quatro mil alunos de escolas particulares do país. Os resultados revelam que os pais de boa parte desses

12 Disponível em <http://www.cetic.br/usuarios/kidsonline/index.htm>. Acesso em: 20 nov. 2012.
13 Disponível em <http://revistaepoca.globo.com/Vida-util/jairo-bouer/noticia/2012/11/juventude-esta-nua-na-internet.html>. Acesso em: 20 nov. 2012.
14 Disponível em <http://indicadores.safernet.org.br/>. Acesso em: 20 nov. 2012.

jovens não controlam o uso da rede por seus filhos e ignoram os conteúdos acessados e compartilhados. Dentre os dados relevantes, vale citar:

- 28% dos jovens já encontraram na vida real pessoas que conheceram na rede;
- 20% tiveram envolvimento amoroso pela internet;
- 20% mandariam sua imagem para pessoas que conheceram na rede;
- 6% já apareceram nus ou seminus em fotos na internet;
- 14% já passaram informações pessoais em sites de bate-papo;
- 6% já mostraram partes íntimas de seu corpo para desconhecidos via webcam.

Cabe perguntar se esses jovens têm a noção precisa do preço cobrado por esse tipo de exibição on-line, abrangendo publicação de fotos, vídeos e revelações de informações de cunho íntimo, além da exposição a situações e contatos impróprios na praça pública virtual. Jairo Bouer enfatiza a importância de se trabalhar a questão na família e nas escolas, sem se esquecer da atuação das autoridades. E faz uma observação que dá pistas importantes sobre o *ethos* de espetacularização da intimidade e a dimensão do problema a ser enfrentado:

> O pior é que, mesmo sabendo de alguns desses riscos, os jovens lidam mal com a exposição. Para muitos, aparecer na rede (independentemente de como isso acontece) é melhor do que sumir do mapa virtual. Ser "popular", nesse contexto, poderia compensar alguns riscos. [...] O anonimato da rede e a barreira da tela do computador parecem criar certo distanciamento do risco real (BOUER, 2012).[15]

O fato é que os efeitos da disseminação de dados pessoais se amplificam e ganham contornos inexoráveis nos ambientes digitais. Evidenciam-se os limites do direito em restaurar de modo pleno o caráter privado daquilo que se torna inexoravelmente público numa rede como a internet e sua memória imensurável (VIANNA, 2012). Resta a quem foi afetado avaliar e lidar com as consequências de um ato irreverssível, já consumado[16]. A esse respeito, tornou-se emblemático o debate público e o processo deliberativo que se seguiram ao roubo de dados, tentativa de extorsão e, por fim, vazamento criminoso na web de fotos íntimas de uma celebridade da TV, a atriz Carolina Dieckemann. O episódio suscitou discussões sobre privacidade, sigilo e riscos nas redes. Teve o condão de ressaltar lacunas na legislação referente a crimes cibernéticos e acelerar a aprovação de projetos de lei específicos que tramitavam em banho-maria no Congresso.

Sintomaticamente, a lei sobre roubo de dados na rede foi apelidada com o nome da atriz. A chamada Lei Carolina Dieckmann foi aprovada na Câmara dos Deputados, em novembro deste ano, e agora segue para a sanção presidencial. O caso conjuga uma série de elementos que povoam nosso cenário midiático, tais como: banalização do cibercrime; invasão de privacidade; espetacularização da intimidade; interfaces entre mídias irradiadas de massa e mídias distribuídas de grupo; e recomposições entre as noções de público e privado.

7. A disputa pelo sentido

Quais noções se contraporiam de modo satisfatório às argumentações e evidências cotidianas de que a privacidade já não mais faria sentido em um mundo on-line? Numa analogia com a noção de modernidade formulada por Bauman (2001), fica a impressão de se estar sob a égide de uma "privacidade líquida", tal a dificuldade de discernir limites e formas em meio à diluição de fronteiras entre o privado e o público. Entretanto, esse modo de ver a questão revela-se desfocado – a história registra que essas fronteiras nunca estiveram livres de conflagrações e tensionamentos. As apreciações em torno da privacidade giram em torno da atribuição de valor e da disputa pelo sentido de uma categoria social sujeita a variações históricas.

As bases da oposição entre *coisa pública* e *coisa privada* remontam às origens da noção de espaço público como fórum de discussão e deliberação cidadãs na *polis* grega. Nesse sentido, os gregos sequer concebiam ou atribuíam valor a alguma ideia de privacidade: o termo inglês *idiot* advém do grego *idiotes*, palavra que designava a pessoa privada que não se engajava na vida pública da *polis* (DE HEART *apud*

15 Disponível em <http://revistaepoca.globo.com/Vida-util/jairo-bouer/noticia/2012/11/juventude-esta-nua-na-internet.html>. Acesso em: 20 nov. 2012.
16 Aqui, os aspectos comunicacionais, comportamentais e tecnológicos se entrelaçam ao arcabouço jurídico-legal. Segundo uma corrente da tradição linguístico-semiótica, um dos princípios da comunicação é a sua irreversibilidade, pois não há como retroagir naquilo que já foi comunicado (DE VITTO, 1997 *apud* SANTAELLA, 2001). O que quer que tenha sido enunciado terá o seu nível de disseminação, apreensão e repercussão no processo de significação social (ou semiose) que a partir daí se engendrará.

AMADEU, 2010).

Os ideais iluministas puseram a esfera privada sob suspeição. A reivindicação burguesa por transparência, em fins do século XVIII, buscava conferir publicidade à relação entre os agentes privados e o Estado. Uma concepção que se contrapunha ao modo aristocrático de governar, baseado no segredo; e que legou ao arcabouço jurídico dos regimes democráticos o princípio da publicidade (HABERMAS, 1984), herança legítima do "século das luzes". Vem daí a inspiração de um espaço público virtual inclusivo e facilitador da transparência dos atos administrativos na área pública, sob a chancela das políticas de governança eletrônica.

Nesse caso, transparência implica mecanismos de *accountability* (prestação de contas/responsabilização) e iniciativas de incentivo ao debate e à participação comunitária na formulação, escolha e implementação de políticas públicas – inclusive por meio das redes sociais. Um exemplo nesse campo é a lei federal nº 12.527/2011 – a chamada Lei de Acesso à Informação[17], aplicável aos três Poderes da União, dos Estados, do Distrito Federal e dos Municípios. A Lei, que entrou em vigor a partir de maio de 2012, regulamenta o direito constitucional de acesso dos cidadãos às informações públicas.

Com relação à concepção contemporânea de privacidade, Fernanda Bruno observa que esta resultou de "embates na definição das relações entre o estado e a sociedade civil, o indivíduo e o coletivo" (BRUNO, 2010)[18]. Segundo a autora, a privacidade é uma construção histórica resultante de tensões e conflitos sociais, políticos e econômicos, razão por que não se trata de uma condição "natural", sujeita a um princípio evolutivo que levaria à sua substituição pela publicidade. Nessa perspectiva, tais embates deixaram marcas fundamentais na contemporaneidade, a exemplo da separação entre público e privado – e a definição de papéis em cada uma dessas esferas –, além da valorização da família, dos direitos do indivíduo, da inviolabilidade do domínio privado, e do direito ao segredo, à solidão e à proteção do anonimato.

Patrick Charaudeau assinala que a diferença entre o público e o privado não deve ser concebida nos termos estritos de oposição fixa. A rigor, existe uma dinâmica em que um se deixa invadir pelo outro, recompondo-se e redefinindo-se a um só tempo:

> Quando revistas populares começaram a aproveitar-se da vida privada das estrelas do *show business*, era para tornar público o privado; quando a televisão moderna mostra os políticos, com esposa e amigos em programas que tratam da vida cotidiana, ou mesmo íntima, é para tornar público um outro tipo de privado; quando se fazem programas com indivíduos anônimos que são transformados em heróis por um dia diante do público e das câmeras, como nos *reality shows*, trata-se ainda de tornar público o privado até então desconsiderado. Assim sendo, é através dessa sucessão de recomposições da oposição entre público e privado que o que é transgressão num primeiro tempo torna-se norma posteriormente (CHARAUDEAU, 2012, p. 117).

Em suma, o embaralhar de fronteiras entre o público e o privado acentuou-se com a evolução das mídias no século XX, as quais investem progressivamente no domínio privado. Observe-se que, na era da videovigilância, mídias sociais e *reality shows*, a acepção de privacidade privilegia justamente a "habilidade de uma pessoa em controlar a exposição e a disponibilidade de informações acerca de si"[19], conforme definição extraída da Wikipédia. E essa habilidade remete a um jogo entre *controle* e *exposição* que comporta seus riscos, mas não autoriza ninguém a declarar cabalmente que as pessoas não mais valorizam a privacidade. Mais uma vez Fernanda Bruno ajuda a clarear a questão, quando comenta a declaração de Mark Zuckerberg sobre o fim da privacidade:

> Por um lado, a afirmação de Zuckerberg repete o que já se tornou óbvio – o processo de publicização da vida privada nos ambientes de comunicação contemporâneos [...] Esta constatação, verdadeira, não implica, contudo, o fim da privacidade. Esse fim é falso em muitos níveis. Para citar apenas um, vale lembrar que essa publicização não significa que as pessoas não se importem mais com a sua privacidade, mas sim que elas querem encená-la em público. E encenar a privacidade em público pode (com algum risco) implicar sobre ela um controle maior e

17 Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 20 nov. 2012.
18 Disponível em <http://dispositivodevisibilidade.blogspot.com.br/2010/01/o-fim-da-privacidade-em-disputa.html>. Acesso em: 20 nov. 2012.
19 Disponívem em <http://pt.wikipedia.org/w/index.php?title=Privacidade&oldid=31860591>. Acesso em: 20 nov. 2012.
20 Disponível em <http://dispositivodevisibilidade.blogspot.com.br/2010/01/o-fim-da-privacidade-em-disputa.html>. Acesso em: 20 nov. 2012.

não menor (BRUNO, 2010).[20]

As mudanças em curso não são, portanto, fruto de um encadeamento linear de fatos que evoluem rumo a um destino pré-determinado no qual somos enredados. Tampouco os enunciados sobre essas transformações devem ser apreendidos de forma passiva e acrítica. Afirmações ou negações em torno da existência da privacidade inserem-se numa arena de embates discursivos atravessados por interesses diversos e, às vezes, conflitantes e contraditórios. Pois, como lembra Fernanda Bruno, aquele que clama pelo fim da privacidade também pode clamar pelo controle da liberdade e do anonimato, ou das práticas de compartilhamento e colaboração na rede. Não, a vida on-line não extinguiu a privacidade.

Referências

AMADEU, Sérgio. *Redes cibernéticas e tecnologias do anonimato*: confrontos na sociedade do controle. In: GT Comunicação e Cultura, XVIII Encontro da Compós – PUC Minas. Belo Horizonte: Compós, 2009.

ARAGÃO, Alexandre. *Social ou Antissocial?* São Paulo: Tec Folha de S. Paulo, 2012. Disponível em <http://www1.folha.uol.com.br/tec/1186647-estudos-reabrem-debate-sobre-o-impacto-de-redes-sociais-na-vida-das-pessoas.shtml>. Acesso em: 20 nov. 2012.

BAUMAN, Zigmunt. Modernidade Líquida. Rio de Janeiro: Jorge Zahar Editor, 2001.

BENTHAM, Jeremy. *O panóptico*. Belo Horizonte: Autêntica, 2000.

BRUNO, Fernanda. *O fim da privacidade em disputa*. Postado em 24 jan. 2010. Disponível em <http://dispositivodevisibilidade.blogspot.com.br/2010/01/o-fim-da-privacidade-em-disputa.html>. Acesso em: 20 nov. 2012.

BRUNO, Fernanda; KANASHIRO, Marta; FIRMINO, Rodrigo. *Introdução*. In: BRUNO, Fernanda; KANASHIRO, Marta; FIRMINO, Rodrigo (Org.) Vigilância e Visibilidade: espaço, tecnologia e identificação. Porto Alegre: Sulina, 2010.

BOTELLO, Nelson Arteaga. *Orquestração da vigilância eletrônica*: uma experiência em CFTV no México. In: BRUNO, Fernanda; KANASHIRO, Marta; FIRMINO, Rodrigo (Org) Vigilância e visibilidade: espaço, tecnologia e identificação. Porto Alegre: Sulina, 2010.

BOUER, Jairo. *A juventude está nua na internet*. In: Revista Época. São Paulo: Editora Globo, 2012.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2002.

CHARAUDEAU, Patrick. *Discurso das mídias*. São Paulo: Contexto, 2012.

FOUCAULT, Michel. *Vigiar e Punir*: Nascimento da prisão. Petrópolis, Rio de Janeiro: Vozes, 2009.

HABERMAS, Jürgen. *Mudança estrutural da esfera pública*: investigações quanto a uma categoria da sociedade burguesa. Rio de Janeiro: Tempo Brasileiro, 1984.

KEEN, Andrew. *#vertigemdigital*: por que as redes sociais estão nos dividindo, diminuindo e desorientando. Rio de Janeiro: Zahar, 2012.

LEMOS, Ronaldo. Somos todos Carolina Dieckmann: não existem mais dispositivos pessoais. São Paulo: Folha de São Paulo, 2012. Disponível em <http://www1.folha.uol.com.br/tec/1089398-somos-todos-carolina-dieckmann-nao-existem-mais-dispositivos-pessoais.shtmll>. Acesso em: 20 nov. 2012.

SANTAELLA, Lucia. *Comunicação e pesquisa*: projetos para mestrado e doutorado. São Paulo: Hacker Editores, 2001.

SIMONITE, Tom. *O que o Facebook sabe?* In: Technology Review, MIT. Boston, 2012. Reproduzido por Época Negócios, ago. 2012.

VIANNA, Túlio. *Caiu na rede é público*. In: O Estado de S. Paulo. São Paulo, 2012. Caderno Aliás. SANTAELLA, Lucia. Comunicação e pesquisa: projetos para mestrado e doutorado. São Paulo: Hacker Editores, 2001.

ZAGO, Gabriela. *Considerações sobre a circulação de informações em sites de redes sociais*. In: revista Fonte. Belo Horizonte: Prodemge, 2011.

Segurança começa pela infraestrutura

Data Center Prodemge: de acordo com os mais exigentes padrões de qualidade - EIA/TIA 942, TIER 3 e ABNT NBR 15247.

- Maior disponibilidade às soluções de TI
- Sistema de climatização, controle de temperatura e umidade do ar de última geração
- Avançado sistema contra incêndio
- Sistema elétrico mais seguro
- Rígido controle de acesso
- Monitoramento por CFTV
- Sala-cofre certificada (ABNT)

prodemge

www.prodemge.gov.br

Divulgação

Luís Carlos Silva Eiras
luiscarloseiras@gmail.com

C-O-R-I-N-T-H-A-S

Este ano decifrei os códigos secretos que meu tio usava para marcar o custo das mercadorias na sua loja de roupas. Depois da missa de sétimo dia, conversando com meus primos que trabalharam na loja, foi-me revelado o segredo que me intrigava há mais de 50 anos: o código secreto era *C-O-R-I-N-T-H-A-S* para *1-2-3-4-5-6-7-8-9* e *X* para o zero.

O código secreto encontrado pelo agente secreto X-9, escrito por Dashiell Hammett e desenhado por Alex Raymond em 1934, é mais fácil decifrar, basta ligar os números[1].

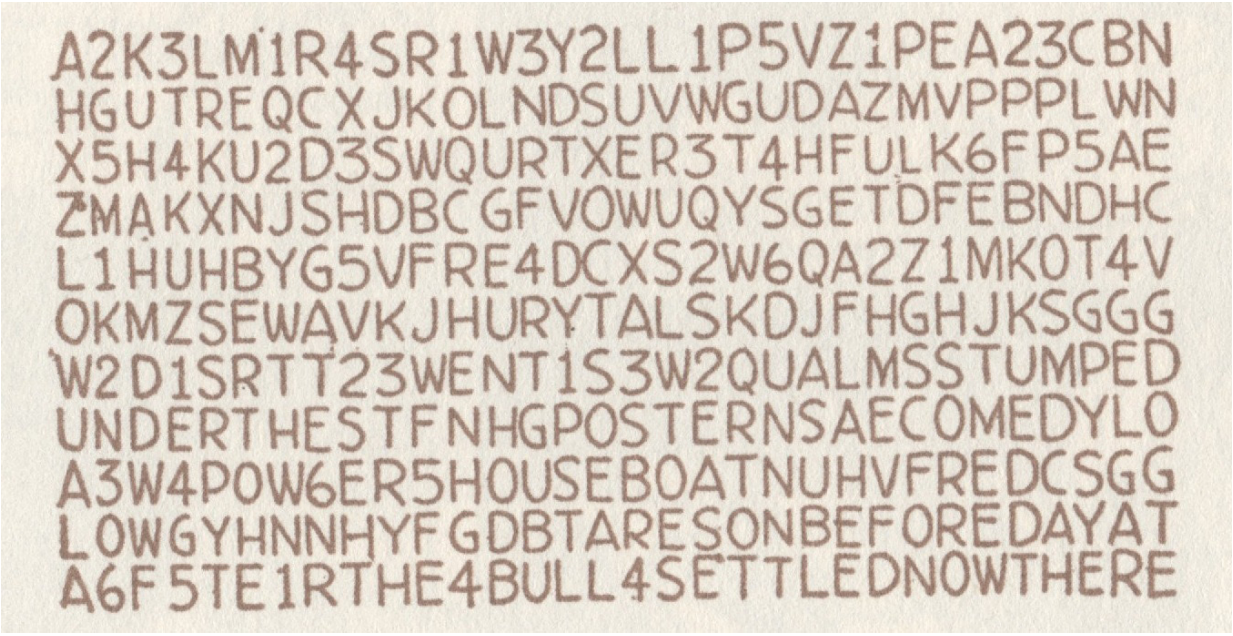


Figura 1 – Código secreto do X-9 parece complicado, mas é simples

Às vezes, decifrar um código secreto requer uma inteligência excepcional, como é o caso de Sherlock Holmes ao decifrar os códigos de *Os dançarinos*[2]. Não apenas porque as seis mensagens são curtas – o que impossibilita uma análise de frequência das cifras –, mas porque as mensagens estão erradas. O símbolo usado para "V" é o mesmo usado para "P" e o símbolo usado em algumas mensagens para "C" é o mesmo usado para "M"[3]. Assim, ao decifrar códigos secretos escritos errados, Sherlock se mostra muito mais inteligente do que credita sua fama.

1 P4THIA SAT. Agente secreto X-9, Devir Livraria, 2010, p. 27.
2 DOYLE, Arthur Conan. *Sherlock Holmes*. São Paulo: Jorge Zahar Editor, 2006, Volume 3, p. 91-124.
3 Na Figura 2, a mensagem é NEVER (nunca)

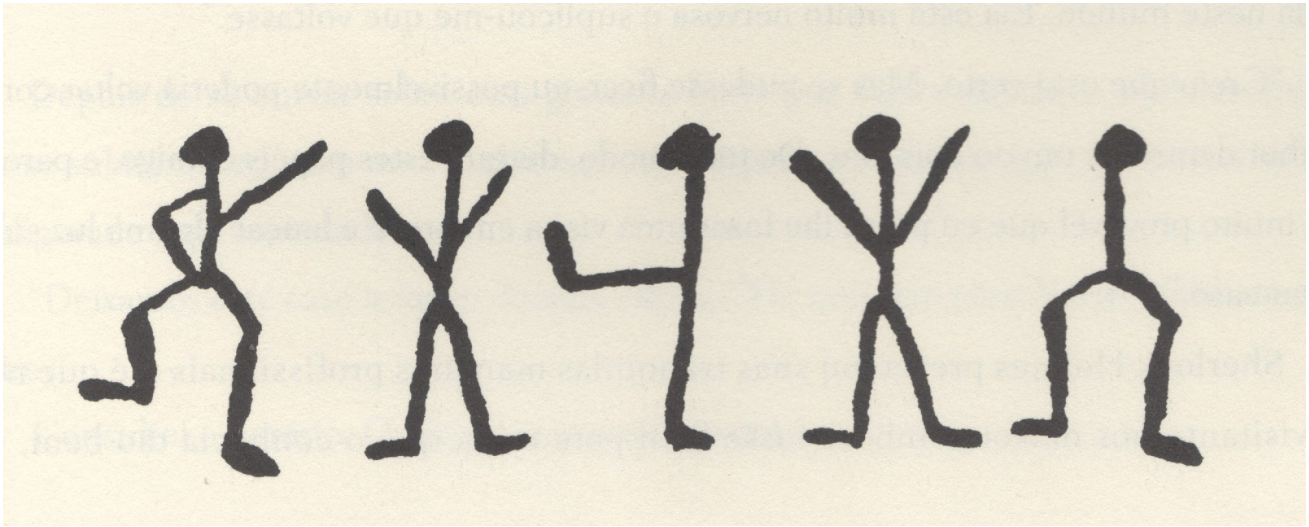


Figura 2 – Os dançarinos de Sherlock dançam errado

Lembrando que a humanidade, segundo os sherlockianos, divide-se entre aqueles que atribuem os erros a Arthur Conan Doyle (um grupo desprezível e sem imaginação) e aqueles que atribuem os muitos erros encontrados nos quatro romances e 56 contos unicamente ao desleixo narrativo do dr. Watson[4].

Já Edgar Allan Poe faz tudo direito em *O escaravelho de ouro*[5]. O código secreto é encontrado e decifrado sem nenhum erro. O tesouro é localizado e dividido. E de quebra, Poe cria o primeiro método de decifração. Daí os elogios de todos os hackers.

Michael Crichton, no romance *Esfera*[6], complica um bocado. Uma gigantesca nave alienígena, estacionada no fundo do oceano Pacífico, começa a enviar mensagens em código binário. Cada mensagem exige um tratamento diferente, até que se estabeleça um diálogo – em inglês, claro. Isso é ficção, mas, na prática, o problema do Search for Extra-Terrestrial Intelligence (Seti) – www.seti.org –, instituto de pesquisa que procura mensagens vindas do espaço, é muito pior: não há ainda mensagens a decifrar.

Mas complicado mesmo foi decifrar as mensagens das máquinas Enigmas alemãs pelos ingleses durante a Segunda Guerra Mundial. É só ver a lista dos termos técnicos utilizados entre 1940 a 1945: procedimento Banburismus, refletor Caesar, redes Dolphin, Porpoise, Shark e Triton (isto é, subcódigos), catálogo Eins, Cillis, o Herivel Tip ["dica" de Herivel, ou Herivelismus], códigos-dentro-de-códigos, engrenagens Gamma, fitas perfuradas, quadro de conexões a plugue, processo *rodding*, tabelas de Bigram, dispositivos de reprodução chamados *bombes*, baralhamento cruzado, texto conhecido e um código relacionado de nome *Geheimschreiber* (escritor secreto)[7]. E, por fim, Colossus, em 1943, o primeiro computador.

O que se pode deduzir da criptografia é que todos os códigos secretos, dos mais simples, como o utilizado pelo meu tio, aos complicados, acabam sendo decifrados. No ano passado, pesquisadores da Universidade Stanford conseguiram decifrar automaticamente os captchas – aquela sequência de letras e números distorcidos que você tem que repetir em certos sites para provar que você não é um robô. E quem viu *Os vingadores* (Joss Whedon, 2012) viu quando Loki, na cena do coquetel na Alemanha, coloca um aparelho que copia o olho da pessoa e transmite a cópia para que Gavião Arqueiro possa abrir a porta. Nem a biometria escapa.

4 GRANN, David. *O diabo e Sherlock Holmes*. São Paulo: Companhia das Letras, 2012, p. 13-55.
5 POE, Edgar Allan. *Histórias extraordinárias*. São Paulo: Abril S.A., 1981, p. 333-375.
6 CRISCHTON, Michael. *Esfera*. Editora Best Seller, 1988
7 A tempestade da guerra, Andrew Robert. Record, 2012, p. 408

Segurança e validade jurídica para os documentos eletrônicos.

Certificação digital é a tecnologia capaz de garantir segurança, confidencialidade e integridade às informações no mundo virtual.

Por meio dela, também é possível autenticar e tramitar documentos eletronicamente, válidos juridicamente de acordo com a legislação brasileira*.

Acesse **www.prodemge.gov.br/certificacaodigital** e adquira o seu certificado.

* Medida Provisória 2.200/2001 e Lei Federal nº 12.682/2012

Para saber mais, entre em contato: (31) 3339-1251 ou
prodemgecertificadora@prodemge.gov.br

ICP Brasil
O Brasil na era da certificação digital

AUTORIDADE CERTIFICADORA
prodemge

155 LigMinas

O telefone para falar com o Governo

O LigMinas é a central de atendimento telefônico do Governo de Minas. Por meio dela, o cidadão tem informações sobre os serviços prestados pelas instituições estaduais, como documentos necessários, valores de taxas, agendamento de serviços, endereços e horário de funcionamento das unidades de atendimento.

A ligação é gratuita para todo o Estado de Minas Gerais.

Para as demais localidades, o atendimento é feito pelo número (31)3303-7995

GOVERNO DE MINAS