UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO II

GILBERTO CALIXTO

SEGURANÇA E MANUTENÇÃO DE DADOS E INFORMAÇÕES FISCAIS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2014

GILBERTO CALIXTO

SEGURANÇA E MANUTENÇÃO DE DADOS E INFORMAÇÕES FISCAIS

Monografia apresentada ao Curso de Especialização em Gestão de Tecnologia da Informação e Comunicação II, como requisito parcial para obtenção do título de "Especialista em Gestão de Tecnologia da Informação e Comunicação.
Orientado por: Professor Christian Carlos de Souza Mendes

CURITIBA
2014

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba
Diretoria de Pesquisa e Pós-Graduação
II CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

TERMO DE APROVAÇÃO

SEGURANÇA E MANUTENÇÃO DE DADOS E INFORMAÇÕES FISCAIS

Por

GILBERTO CALIXTO

Esta monografia foi apresentada às 16:00 h do dia 09/10/2014 como requisito parcial para a obtenção do título de Especialista no CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, da Universidade Tecnológica Federal do Paraná, **Câmpus Curitiba**. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho:

_____

Prof. Msc. Alexandre Jorge Miziara
UTFPR - Examinador

_____

Prof. Christian Carlos de Souza Mendes
UTFPR – Orientador

_____

Prof. Msc. Alexandre Jorge Miziara
UTFPR – Coordenador do Curso

SUMÁRIO

RESUMO

Tem se como objeto de estudo dados/informações fiscais - segurança e manutenção, haja vista que existe hoje uma gama de documentos e informações que são recebidas por meio eletrônico, tais como: Nota Fiscal Eletrônica, Conhecimento de Transporte Eletrônico, Escrituração Fiscal Digital e Contábil, Processo Eletrônico, dentre outras. O trabalho fiscal executado em papel se tornou uma raridade. O fato é que diante da grande gama de informações que são obtidas por meio eletrônico, há que se discutir como o fisco trata das questões relacionadas com a segurança e a manutenção destas informações. Assim sendo, são extremamente necessárias as medidas preventivas de proteção e controle para que as ocorrências de riscos sejam, significativamente, reduzidas ou inibidas, atentando-se sempre para que a aplicação das medidas não gere suspensão ou interrupção dos serviços ou mesmo violação de dados. Faz-se necessário um sistema de informação que exerça com veemência este papel de segurança, prezando pela clareza e sigilo dos dados fiscais obtidos junto aos contribuintes.

Palavras Chave: Segurança. Informação. Pública. Programas.

ABSTRACT

Has as its object of study data / tax information - security and maintenance, and there is now a range of documents and information that are received by electronic means, such as: Electronic Invoice, Electronic Transport Knowledge, Digital Tax Bookkeeping and Accounting, Electronic process, among others. The tax work performed on paper became a rarity. The fact is that given the wide range of information that is obtained through electronic means, we have to discuss with the taxman comes to the issues related to security and the maintenance of this information. Thus preventive measures of protection and control for the occurrence of risks are significantly reduced or inhibited, always paying attention the measures to not occur suspension or interruption of services or even data breach being, are badly needed. It is necessary an information system that performs this role vehemently security, valuing clarity and confidentiality of organizational data.

Keyword: Public safety. Information. Programs

1 INTRODUÇÃO

1.1 CONSIDERAÇÕES INICIAIS

É correto afirmar que o fisco, desde que atenda aos requisitos previstos na legislação, possa quebrar sigilo bancário dos contribuintes com o objetivo de obtenção de dados para subsidiar suas ações de fiscalização.

Além disso, existe hoje uma gama de documentos e informações que são recebidas por meio eletrônico, tais como: Nota Fiscal Eletrônica, Conhecimento de Transporte Eletrônico, Escrituração Fiscal Digital e Contábil, Processo Eletrônico, dentre outras.

O trabalho fiscal executado em papel se tornou uma raridade.

O fato é que diante da grande gama de informações que são obtidas por meio eletrônico, há que se discutir como o fisco trata das questões relacionadas com a segurança e a manutenção destas informações.

Afinal de contas, é responsabilidade de o fisco manter as informações obtidas sob sigilo absoluto, ainda mais quando se está diante de um bem extremamente relevante dos seus contribuintes, relacionado principalmente com o aspecto financeiro da vida daqueles, o que pode influenciar em muito sua existência.

Assim, mais do que necessário, é vital para o Fisco a análise das condições de segurança, às quais as informações estão submetidas, bem como qual o cuidado com a manutenção destes dados que deve ser tomado pelos Auditores Fiscais.

Neste aspecto, com o auxílio da Segurança da Informação e das técnicas já desenhadas e experimentadas ao longo do desenvolvimento do processo tecnológico, procurar-se-á enfrentar a questão inicialmente posta, para, então, analisar alguns dos comportamentos extraídos do dia a dia das repartições fiscais.

1.2 JUSTIFICATIVA

Este estudo justifica-se pela necessidade de conhecimento do que vem a ser a segurança de informações sendo que não é objeto deste enfrentar aqui a forma de obtenção nem a origem das informações, mas tão somente enfrentar os aspectos relacionados com a segurança e a manutenção das informações já obtidas pelo fisco.

Inicia-se tratando das questões relacionadas com informações e dados, evoluindo seus conceitos e construindo uma base para, após, adentrar-se ao tema da Segurança da Informação e em seguida da manutenção dos dados.

As ameaças, os riscos, a construção de uma Política de Segurança da Informação, visualizando, ao final, como a Receita Estadual trata do tema e no que poderia esse estudo agregar ao seu dia a dia.

1.3 PROBLEMA

Qual a importância da segurança da informação na atualidade?

1.4 OBJETIVOS

1.4.1 Objetivo Geral

Analisar a importância de dados/informações fiscais, segurança e manutenção.

1.4.2 Objetivos Específicos

- Apresentar os conceitos e definições da informação;
- Abordar os conceitos de segurança e riscos, dando ênfase ao estudo das medidas de segurança;
- Elencar tópicos de direito digital a fim de conhecer a legislação vigente no que concerne ao tema em estudo;
- Analisar a responsabilidade dos provedores no que tange à segurança da informação.

1.5 METODOLOGIA

A pesquisa realizada é do tipo bibliográfica e qualitativa.

Os dados qualitativos são coletados para aprofundar conhecimento acerca de

algumas coisas que não podem ser observadas e medidas diretamente.[1]

O objetivo de uma pesquisa qualitativa é obter uma visão e compreensão mais ampla referente ao estudo.

A pesquisa qualitativa ajuda a identificar questões e entender porque elas são importantes e é muito utilizada em algumas situações que envolvem o desenvolvimento e aperfeiçoamento de novas ideias.

Lakatos e Marconi definem pesquisas bibliográficas, “não é mera repetição do que já foi dito ou escrito sobre certo assunto, mas propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras.”[2]

Segundo Antônio Carlos Gil, entende-se por pesquisa bibliográfica como aquela desenvolvida em cima de materiais já elaborados, tais como: artigos científicos e livros. Há também as pesquisas elaboradas e desenvolvidas tendo como ponto inicial as fontes bibliográficas.[3]

A coleta de dados foi realizada por análise documental através de coleta de informações, conceitos e dados em livros, revistas, apostilas, publicações eletrônicas e outros documentos escritos (publicados ou não).

---

[1] MINAYO, M.C. de S. (Org.) **Pesquisa social: teoria, método e criatividade**. 22 ed. Rio de Janeiro: Vozes, 2003. p.22.
[2] LAKATOS, E. M. **Técnicas de Pesquisa**. 5. ed. São Paulo: Ed. Atlas, 2008. p.72.
[3] GIL, A.C. **Métodos e técnicas de pesquisa**. São Paulo: Atlas, 1999.

2 REFERENCIAL TEÓRICO

2.1 INFORMAÇÃO

A informação, que já no início do trabalho de Marcos Sêmola[4], é tida como "*ativo cada vez mais valorizado*", o que de fato é verdadeiro, tem vivido, principalmente em relação à forma de sua obtenção ou de acesso, momento único na história.

E isso talvez esteja diretamente vinculado ao fato de termos um desenvolvimento tecnológico singular nas últimas décadas, principalmente quando nos referimos ao processo de evolução dos computadores e da internet.

E a informação tem toda a influência hoje em todo o tipo de relação existente, principalmente quando se refere ao cumprimento de obrigações tributárias e fiscais por parte das empresas e a participação do fisco nesses processos.

Segundo Capurro e Hjorland:

> O conceito de informação como usado na linguagem cotidiana, no sentido de conhecimento comunicado, tem um importante papel na sociedade contemporânea. Este conceito ganhou relevância principalmente a partir do final da Segunda Guerra Mundial com a disseminação global do uso das redes de computadores. É o nascimento da ciência da informação (CI), em meados dos anos cinquenta, que testemunha este fato. [5]

A evolução do sistema pode ser exemplificado com o surgimento da Nota Fiscal Eletrônica NF-e, que surge formalmente como obrigatória no âmbito dos Estados a partir do Ajuste SINIEF 7, de 2005, editado pelo Conselho Nacional de Política Fazendária – CONFAZ, que é o órgão responsável pela regulamentação das obrigações acessórias e pela uniformização dos procedimentos exigidos dos contribuintes no âmbito nacional.

Efetivamente, o objetivo do exemplo é o de tão somente apontar que há 10 anos a única forma de obter os principais documentos emitidos pelos contribuintes, quando se fala do ICMS – Imposto sobre a Circulação de Mercadorias e Serviços, carecia, além da abertura da necessária Ordem de Serviço, da notificação do contribuinte para que apresentasse os documentos fiscais que emitiu (em papel, por

---

[4] SÊMOLA, Marcos. **Gestão da Segurança da Informação**: visão executiva da segurança da informação: aplicada ao Security Officer. Rio de janeiro: Campus, 2003.

[5] Capurro e Hjorland (2003, p.78):

lógico).

Com o surgimento da NFe, os dados relativos às operações realizadas pelos contribuintes passaram a ser entregues ao Fisco imediatamente, por via eletrônica, deixando de existir a figura da nota fiscal impressa e da necessidade do Fisco notificar o contribuinte para apresentá-las, isso em análise simplificada.

Rayssa Lara Oliveira de Andrade[6] elenca que:

> [...] a informação sempre esteve e estará presente em toda a evolução histórica da humanidade, e que (citando DRUKER, 2000, P. 3) "nada na história econômica evoluiu tão depressa nem teve tanto impacto quanto a revolução da informação.

Ainda fazendo menção à Drucker (2000, p. 7), Rayssa Lara Oliveira de Andrade considera que "*a revolução da informação até agora – isto é, desde os primeiros computadores, em meados da década de 1940 - apenas transformou processos que já existiam*".

E é considerando esta transformação do processo que faz que surja a necessidade de que o Fisco venha a se atentar para o momento no qual está inserido, e de que forma vai tratar o seu negócio neste contexto, tendo em vista a rápida evolução da informação.

Além destas linhas iniciais sobre a evolução da informação, cumpre, também, trazer algumas ideias sobre o conceito de informação.

Rayssa Lara Oliveira de Andrade[7] cita Dudziak (2003, p. 23), que diz que "existem muitos significados que definem o termo informação, e devido a isso, os mesmos variam de acordo com a área do conhecimento em que o termo está inserido". Assim, na concepção dela, "*tal abrangência impulsiona diversas interpretações e, consequentemente, gera conceitos distintos*".

Outras definições citadas por Rayssa Lara Oliveira de Andrade[8]:

> "Baseando-se então, na Ciência da Informação (CI), para Hashimoto

[6] ANDRADE, Rayssa Lara Oliveira de. **A Biblioteca 2.0 sob a ótica da Gestão da Segurança da Informação**: um estudo de caso com a Biblioteca Nacional de Brasília. Disponível em: (http://repositorio.ufrn.br:8080/monografias/bitstream/1/85/1/RayssaLOA_Monografia.pdf). Natal, 2011. Acesso em 20 de julh. de 2014.
[7] ANDRADE, Rayssa Lara Oliveira de. Ibidem.
[8] ANDRADE, Rayssa Lara Oliveira de. Idem.

> (2009):
>
> [...] a informação é: Uma visão pessoal sobre um conjunto de dados – as relações percebidas associam ao dado um significado próprio, na medida em que são específicas para cada indivíduo, pois dependem de suas experiências anteriores, do que ele tem armazenado em sua memória e de sua capacidade de estabelecer essas relações. Assim, um mesmo conjunto de dados não gera a mesma informação para diferentes pessoas. Nos casos mais simples, envolvendo dados e relações menos complexas, as informações percebidas por diferentes pessoas poderão ser mais semelhantes. Quanto maior a complexidade da informação, mais ela dependerá do repertório anterior e da capacidade de cada indivíduo de estabelecer essas relações e, portanto, mais pessoal será.

Nesse conceito de Hashimoto, vê-se que a interpretação dos dados é pessoal e "[...] depende das capacidades de absorção e acúmulo, ou seja, da experiência adquirida pela formação de origem e a aprendizagem ou a ação" (JULIEN, 2010, p. 193)."

Para Oliveira (2002, p.11), em relação aos efeitos sociais das tecnologias da informação "a profundidade do seu impacto é uma função da penetrabilidade da informação para toda a estrutura social". O resultado histórico dessa estratégia parcialmente consciente é muito indeterminado, visto que a interação da tecnologia e da sociedade depende de relações fortuitas entre um número excessivo de variáveis parcialmente independentes.

Segundo Dudziak (2003, p. 24), "[...] a informação é o conjunto de representações mentais codificada e socialmente contextualizadas". Tal conceito pode ser comparado ao de Sêmola (200 3, p. 45), quando o mesmo caracteriza a informação como um "[...] conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos".

Já para Le Coadic (1997, p. 5), "[...] a informação é um conhecimento inscrito (gravado) sob a forma escrita (impressa ou numérica), oral ou audiovisual".

Por outro lado, Setzer (1999, p. 2) conceitua a informação como "uma abstração informal [...] que representa algo significativo para alguém através de textos, imagens, sons ou animação".

É com esse foco que Beuren (2000, p. 43) afirma que "a informação é fundamental no apoio às estratégias e processos de tomada de decisão, bem como no controle das operações empresariais".[9]

Devido a sua importância, Beal (2004, p. 22) ressalta que:

> O desempenho de uma organização está condicionado à qualidade das ligações e relações entre as unidades organizacionais, e estas Le Coadic conceitua em sua obra o conhecimento como ‘um saber’, que para ele seria o resultado do ato de conhecer ou de formar ideia acerca de alguma coisa.[10]

A importância e a necessidade da informação para determinar as decisões dos administradores, sejam da área privada ou da pública, estão mais do que claros neste estudo. E, ao longo do tempo, como visto no exemplo da NFe, o Fisco procurou acompanhar essa revolução da informação desenvolvendo também novas formas para a obtenção considerando os mais recentes meios eletrônicos.

Assim sendo, a revolução da tecnologia da informação sofreu influências de vários fatores institucionais, econômicos e culturais. As empresas e os países capitalistas passaram por um processo de reestruturação organizacional e econômico, no qual a nova TI exerceu um papel fundamental e foi decisivamente moldada pelo papel que desempenhou. A disponibilidade de novas redes de telecomunicações e de sistemas de informação preparou terreno para integração dos mercados financeiros e a articulação segmentada da produção e do comércio mundial. O mercado financeiro funciona muito pouco por questões econômicas e muito mais por "turbulências informacionais”. (OLIVEIRA, 2002)

Resta dizer, então, confirmada a obtenção de dados e de informação, enfrentar os desafios que mostram a partir de então.

2.2 DADOS E INFORMAÇÕES

---

[9] BEAL, Adriana. **Gestão Estratégica da Informação:** como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2004.

[10] BEAL, Adriana.**Ibidem.**

Importante, ainda, para o deslinde do estudo, é proceder a um esclarecimento visando distinguir “dado” de “informação”.

Como já citado, informação tem um vínculo determinante com o subjetivo, consistindo já em uma emissão de opinião ou análise pessoal devidamente valorada. Aqui também me valho do conceito de Hashimoto que determina informação como sendo uma visão pessoal sobre um conjunto de dados.

O “dado”, por sua vez, pode ser determinado como um elemento objetivo, frio, que destituído de subjetivismo nada de diferente representaria independente do seu usuário.

Uma definição de “dados” bastante elucidativa consta de “Dado, Informação, Conhecimento e Competência” de Valdemar W. Setzer[11], veja-se:

> *Dado* é uma sequência de símbolos quantificados ou quantificáveis. Portanto, um texto é um dado. De fato, as letras são símbolos quantificados, já que o alfabeto por si só constitui uma base numérica. Também são dados imagens, sons e animação, pois todos podem ser quantificados a ponto de alguém que entra em contato com eles ter eventualmente dificuldade de distinguir a sua reprodução, a partir da representação quantificada, com o original. É muito importante notar-se que qualquer texto constitui um dado ou uma sequência de dados, mesmo que ele seja ininteligível para o leitor. Isso ficará mais claro no próximo item.
> Como são símbolos quantificáveis, dados podem obviamente ser armazenados em um computador e processados por ele.
> Em nossa definição, um dado é necessariamente uma entidade matemática e, desta forma, puramente *sintática*. Isto significa que os dados podem ser totalmente descritos através de representações formais, estruturais. Dentro de um computador, trechos de um texto podem ser ligados virtualmente a outros trechos, por meio de contiguidade física ou por "ponteiros", isto é, endereços da unidade de armazenamento sendo utilizada. Ponteiros podem fazer a ligação de um ponto de um texto a uma representação quantificada de uma figura, de um som, etc.

Pode-se dizer, portanto, que a partir da análise de um dado, o usuário aplicando sua análise, considerando o conhecimento e sua experiência previamente obtida, tem-se o surgimento da informação.

São coisas diferentes, mas que neste estudo, em muitas oportunidades, podem ter o mesmo tratamento, haja vista que é perfeitamente possível entender que o dado sempre estará incluso em uma informação.

---

[11] SETZER, Valdemar W. Dado, **Informação, Conhecimento e Competência.** Disponível em: http://www.ime.usp.br/~vwsetzer/datagrama.html. Acesso em 20 de julh. de 2014.

2.3 DA SEGURANÇA DA INFORMAÇÃO

Marcos Sêmola em seu livro “Gestão da Segurança da Informação”[12] conceitua Segurança da Informação:

> [...] uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Na sequência, propondo análise considerando uma forma mais ampla, diz também considerá-la como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação.

No caso, é a Segurança da Informação que nos dará condições de estudar o que pode ser feito e o que está sendo efetuado com vistas à manutenção, ao gerenciamento e ao acesso ao conjunto de informações já obtidas pelo fisco, o que garante efetivamente a credibilidade do processo e a manutenção do sigilo fiscal.

Os autores, de maneira geral, entendem que a Segurança da Informação visa assegurar a confidencialidade, a disponibilidade e a integridade das informações que agora se encontram na responsabilidade do Fisco.

Patrícia Peck Pinheiro, em seu Livro “Direito Digital”, faz referência à *“norma ISO/IEC 27002 (antiga 17799, p.2005),* segundo a qual segurança da informação 'é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio'”[13].

Cumpre-nos salientar, ainda, que a referida norma ISO/IEC 27002, na sequência, propõe que “a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware”.

Na publicação Boas Práticas em Segurança da Informação[14] do Tribunal de

---

[12] SÊMOLA, Marcos. **Gestão da Segurança da Informação:** visão executiva da segurança da informação: aplicada ao Security Officer. Rio de janeiro: Campus, 2003.

[13] PINHEIRO, Patrícia Peck. **Direito Digital**. 5.ed. revista, atualizada e ampliada de acordo com as Leis n. 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013.

[14] **Boas Práticas em Segurança da Informação**. 4.ed. do Tribunal de Contas da união . Disponível em: http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF. Acesso em 20 de julho de 2014.

Contas da União consta o objetivo da Segurança de Informações, qual seja o de "garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição".

Na sequência, no mesmo trabalho se complementa o tema afirmando que:

> [...] a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações.

Interessante, então, que se enfrente cada uma das garantias que se objetiva ter com a Segurança da Informação, inclusive citando outras que também são mencionadas por alguns autores.

A confidencialidade consiste na manutenção do segredo. Segundo o Tribunal de Contas da União é a garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação, e de que pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.

Para Marcos Sêmola confidencialidade significa que toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas[15].

Importantíssima esta garantia, ainda mais quando se trata de informações fiscais, as quais devem ser resguardadas desde a geração por parte do contribuinte, passando pelo caminho que percorre, até o seu receptor, que é o Fisco. E essas informações, relacionadas com os aspectos financeiros e patrimoniais das pessoas, têm como proteção a exigência do sigilo por parte do fisco, sendo, portanto, de alto grau de confidencialidade.

Complementando, para Patrícia Peck Pinheiro[16], esta garantia consiste no fato de que a informação somente deve ser acessada por quem de direito.

Outra garantia é a da integridade que, segundo a definição de autores citados por Rayssa Lara Oliveira de Andrade[17]: "pode ser considerada como a garantia da

---

15 SÊMOLA, Marcos. Ob. Cit.
16 PINHEIRO, Patrícia Peck. Ob. Cit.
17 ANDRADE, Rayssa Lara Oliveira de. Ob. Cit.

criação legítima e da consistência da informação ao longo de seu ciclo de vida, em especial, prevenção contra criação, alteração ou destruição não autorizada de informações".

Segundo Beal (2005, p. 1) "ou envolveria a manutenção da informação na forma originalmente produzida pelo autor, ou a garantia de não alteração indevida do conteúdo, para SILVA et al. (2008, p. 19)".

Aqui cabe ressaltar a importância da referida garantia, em especial em razão de que o corrompimento danifica a própria informação a ponta de torná-la inútil para os fins aos quais se destina.

Nesta linha, Marcos Sêmola afirma que toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais[18], sendo esta a garantia da integridade.

A quebra da integridade pode ser considerada em dois aspectos primordiais: quando realizadas inserções, substituições ou exclusões de parte do conteúdo da informação e alterações que fornecem suporte, tais como na estrutura física ou lógica onde a informação esteja armazenada.

É a ação de evitar que os dados sejam apagados ou alterados sem a devida autorização do proprietário, para Patrícia Peck Pinheiro[19].

A autenticidade, por sua vez, diz respeito à garantia da veracidade da fonte das informações, é a garantia de origem, o conhecimento acerca do autor. Além disso, pode se incluir neste processo de autenticação todos os demais elementos envolvidos na comunicação ou em uma transação eletrônica que permite o acesso à informação.

Patrícia Peck Pinheiro[20] define a autenticidade como sendo a "capacidade de identificar e reconhecer formalmente a identidade dos elementos de uma comunicação eletrônica".

A disponibilidade, segundo as Boas Práticas em Segurança da Informação[21] do Tribunal de Contas da União:

> Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática". Além disso, complementa afirmando que "manter a disponibilidade de

18 SÊMOLA, Marcos. Ob. Cit.
19 PINHEIRO, Patrícia Peck. Ob. Cit.
20 PINHEIRO, Patrícia Peck. Ibidem.
21 Boas Práticas em Segurança da Informação. Ob. Cit.

> informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

No tocante à disponibilidade, Marcos Sêmola cogita que *toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade*[22].

Outro aspecto que deve ser considerado relevante é aquele que diz respeito à legalidade, que consistiria na aplicação de leis, regulamentos, licenças, contratos e princípios éticos a qualquer uma das outras garantias apontadas anteriormente.

“A legalidade é 'característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes'”, segundo Marcos Sêmola, em citação de Patrícia Peck Pinheiro[23].

---

[22] SÊMOLA, Marcos. Ob. Cit.
[23] PINHEIRO, Patrícia Peck. Ibidem.

3 SEGURANÇA X AMEAÇAS

Segundo Marcos Sêmola, ameaças são “agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização”[24].

No tocante à classificação das ameaças, me parece mais completa aquela trazida por Raíssa de Oliveira Andrade:

> Apesar das ameaças terem sido classificadas pelos autores de diferentes maneiras, todas essas classificações se complementam e se referem às mesmas origens. Entretanto serão utilizadas como base para as classificações aquelas sugeridas por Silva, A. e Silva, E. (2008), por especificarem e englobarem melhor as classificações feitas pelos outros autores.
> As ameaças físicas, naturais e ambientais são aquelas “decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc. (SÊMOLA, 2003, p. 47). Estes acontecimentos têm uma probabilidade de ocorrência muito baixa, porém, se vierem a ocorrer, as organizações poderão sofrer sérios problemas no tocante à disponibilidade da informação.

As ameaças internas, de acordo com Silva, A. e Silva, E. (2008):

> [...] são provenientes de ações involuntárias e voluntárias realizadas por funcionários de uma organização. As involuntárias são ameaças inconscientes, quase sempre causadas pelo desconhecimento ou ainda por acidentes, erros, e até mesmo falta de energia. Enquanto que as ameaças voluntárias são aquelas “propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computadores.
>
> As ameaças involuntárias e voluntárias podem ser incorporadas às ameaças internas, uma vez que, ambas ocorrem dentro do ambiente organizacional. Nesse caso as ameaças humanas (erro de operação, fraude e sabotagem), também podem ser incorporadas devido ao fato dessas operações terem a possibilidade de serem causadas também por funcionários. Nessa classificação também é possível englobar as ameaças técnicas, que segundo BEAL (2005) são referentes a problemas de configuração de sistemas.
> No âmbito das ameaças externas, as ameaças humanas também podem ser incorporadas, uma vez que, são as pessoas que exploram as vulnerabilidades dos sistemas de informação comprometendo, assim, a segurança dos mesmos (SILVA, A. E SILVA, E., 2008, P. 38). Às ameaças externas ainda podem ser incorporadas as ameaças lógicas (códigos maliciosos e/ou invasão de sistemas).”[25]

---

[24] SÊMOLA, Marcos. Ob. Cit.
[25] ANDRADE, Rayssa Lara Oliveira de. Ob. Cit.

3.1 RISCOS

Para que se faça uma boa avaliação acerca da segurança da informação, é importante analisar a questão do risco (em todos os seus aspectos, quantitativo ou qualitativo).

Riscos, segundo Marcos Sêmola, é a “probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios”[26].

Para Raíssa Lara Oliveira Andrade:

> [...] a análise de riscos é, então, um processo fundamental na organização e tem sua importância maior na construção de medidas de controle e prevenção de riscos. Pois, com as possíveis ameaças e riscos identificados, é possível identificar também as causas bem como os efeitos e suas consequências[27].

Complementa, ainda, a citada autora, afirmando que:

> [...] partindo desse ponto, é possível definir também a responsabilidade de controle e, por conseguinte, a tomada de providências contra os danos sofridos e a elaboração de métodos preventivos para possíveis problemas futuros em tempo hábil (SANTOS, SILVA, GOUVÊIA, 2010)[28].

3.2 VULNERABILIDADES

Marcos Sêmola fala, ainda, em vulnerabilidades, que seria a:

> Fragilidade presente ou associada a ativos que manipulam e/ou processam informações que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade[29].

Essas estariam classificadas em: físicas, naturais, hardware, software, mídias, comunicação e humanas.

---

[26] SÊMOLA, Marcos. Ob. Cit.
[27] ANDRADE, Rayssa Lara Oliveira de. Ob. Cit.
[28] ANDRADE, Rayssa Lara Oliveira de. Ibidem.
[29] SÊMOLA, Marcos. Ob. Cit.

3.3 MEDIDAS DE SEGURANÇA

Marcos Sêmola conceitua medidas de segurança como sendo:

> [...] as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades, a redução das vulnerabilidades, a limitação do impacto ou minimização do risco de qualquer outra forma[30].

Raíssa Lara Oliveira Andrade observa que são necessárias as aplicações das medidas de proteção e controle para que as ocorrências de riscos sejam, significativamente, reduzidas ou inibidas, e que é importante estar atento quando da aplicação destas medidas para que não ocorra suspensão ou interrupção dos serviços. Cita, ainda, com base nas suas referências BEAL (2005) e FONTES (2000), que classificariam as medidas de segurança em preventivas, corretivas, reativas, detectivas, de contenção, de desmotivação, e de continuidade de controle[31].

Neste caso, vou ficar com a classificação de Marcos Sêmola e suas explicações, que se encontram abaixo citadas:

> Preventivas - medidas de segurança que tem como objetivo evitar que incidentes venham a ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança na instituição. Como exemplos podemos citar as políticas de segurança, instruções e procedimentos de trabalho, especificação de segurança, campanhas e palestras de conscientização de usuários; ferramentas para implementação da política de segurança (firewall, antivírus, configurações adequadas de roteadores e dos sistemas operacionais etc.)
> Detectáveis - medidas de segurança que visam identificar condições ou indivíduas causadoras de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades. Alguns exemplos são: análises de riscos, sistemas de detecção de intrusão, alertas de segurança, câmeras de vigilância, alarmes, etc.
> Corretivas - ações voltadas à correção de uma estrutura tecnológica e humana para que as mesmas se adaptem às condições de segurança estabelecidas pela instituição, ou voltadas à redução dos impactos: equipes para emergências, restauração de backup, plano de continuidade operacional, plano de recuperação de desastres.

---

30 SÊMOLA, Marcos. Ob. Cit.
31 ANDRADE, Rayssa Lara Oliveira de. Ob. Cit.

4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para Raíssa Lara Oliveira Andrade “a Política de Segurança da Informação (PSI), conforme BEAL (2005, p. 43) é o 'documento que registra os princípios e as diretrizes de segurança adotados […] a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos'”[32]. Por outro lado, ainda segundo Raísa Lara Oliveira Andrade, “a PSI é um 'conjunto de regras estabelecidas pela organização que objetivam as melhores práticas para o manuseio, armazenamento, transporte e descarte das informações' (COSMO) et al., 2008, p. 64)”[33].

Segundo a cartilha de “Boas Práticas em Segurança da Informação - 4ª Edição” do Tribunal de Contas da União:

> Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações[34].

Já para a Norma NBR ISO/IEC 27002, o objetivo da Política de Segurança da Informação é “prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”, sendo conveniente que:

> [...] a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

Para Emílio Tissato Nakamura e Paulo Lício de Geus o desenvolvimento da Política de Segurança da Informação é o primeiro e o principal passo da estratégia de segurança das informações, sendo que por meio dessa política é que todos os aspectos envolvidos na proteção dos recursos existentes são definidos e, portanto,

---

32 ANDRADE, Rayssa Lara Oliveira de. Ob. Cit.
33 ANDRADE, Rayssa Lara Oliveira de. Ibidem.
34 Boas Práticas em Segurança da Informação. Ob. Cit.

grande parte do trabalho é dedicada a sua colaboração e seu planejamento[35].

Outra boa análise de Política de Segurança da Informação pode ser extraída do texto de Claudete Aurora da Silva, que informa que:

> [...] escrever uma política de SI envolve comprometimento de diversas áreas de interesse e deve ser abraçada por todos, desde a direção da organização até cada um dos funcionários, clientes e fornecedores com acesso ao sistema de informação, ou que possam de alguma forma comprometer o ativo protegido, sendo que o documento de política de SI deve ser elaborado de forma a servir como uma regra a ser seguida, devendo ser também de fácil leitura e compreensão e exigirá atualizações que reflitam as necessidades do negócio e a realidade da organização.[36]

4.1 TÉCNICAS E TECNOLOGIAS DISPONÍVEIS PARA DEFESA DE INFORMAÇÕES

Após a análise e estudo de Política de Segurança da Informação (PSI), que consiste, basicamente, no conjunto de procedimentos que devem ser conduzidos por uma entidade com vistas a cuidar das informações que obtém ou mantém sob sua responsabilidade e ao atendimento das garantias objetivadas pela segurança da informação, interessante tratar ponto a ponto daqueles componentes ou procedimentos que integram uma sólida e correta aplicação de uma Política de Segurança da Informação.

4.1.1 Firewall

O Firewall, segundo Marcos Sêmola, é um “velho conhecido dos ambientes de rede”, o qual “pode assumir a forma de um software e também incorporar um hardware especializado, tem o papel de realizar análises do fluxo de pacotes de dados, filtragens e registros dentro de uma estrutura de rede”[37]. Complementa, ainda, o citado, afirmando que “como o próprio nome diz, ele - Firewall - representa uma parede de fogo que executa comandos de filtragem previamente especificados com base nas necessidades de compartilhamento, acesso e proteção requeridos pela rede e pelas informações disponíveis através dela”.

---

35 NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de. Ob. Cit.

36 http://www.bibliotecadigital.puc-campinas.edu.br/tde_arquivos/2/TDE-2009-07-15T053257Z-1515/Publico/Claudete%20Aurora%20da%20Silva.pdf

37 SÊMOLA, Marcos. Ob. Cit.

Emílio Tissato Nakamura e Paulo Lício de Geus apresentam uma definição de cunho histórico para o referido componente de sistema de segurança, veja-se:

> A mais antiga definição para *firewalls* foi dada por Bill Cheswick e Steve Bellovin, em *Firewalls and Internet Security: Repelling the Wily Hacker* [CHE 94]. Segundo eles, o firewall é um ponto entre duas ou mais redes, no qual circula todo o tráfego. A partir desse único ponto, é possível controlar e autenticar o tráfego, além de registrar, por meio de *logs*, todo o tráfego de rede, facilitando sua auditoria [AVO 99].
> Já Chapman [CHA 95] define firewall como sendo um componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a internet, ou entre outros conjuntos de redes.[38]

Na sequência, os citados autores definem *firewall* como sendo:

> [...] um ponto entre duas ou mais redes, que pode ser componente ou um conjunto de componentes, por onde passa todo o tráfego, permitindo que o controle, a autenticação e os registros de todo o tráfego sejam realizados[39].

Segundo Adriana Beal:

> Firewall consiste numa barreira de proteção entre um computador ou uma rede interna e seu ambiente externo", sendo que "o tráfego de informações entre esse computador ou rede e o mundo exterior é examinado e bloqueado quando uma informação não atende a critérios pré-definidos de segurança"[40].

4.1.2 Sistema de detecção de intrusão

O *firewall* é apenas um dos componentes de segurança da estratégia de segurança, sendo que praticamente pode ser entendido como a primeira linha de defesa do sistema.

O detector de intrusos, conhecido pela sigla inglesa IDS, segundo Marcos Sêmola:

> É um dispositivo complementar ao firewall que agrega maior inteligência ao processo de combate a ataques e invasões"; "é orientado por uma base de dados dinâmica contendo informações sobre comportamentos suspeitos de pacotes de dados e assinaturas de ataques"; e, "é uma verdadeira enciclopédia de ameaças consultada a todo momento para que o dispositivo possa transcender a análise binária de situações e avaliar a probabilidade de um acesso ser um conhecido tipo de ataque ou uma nova técnica de invasão"[41].

---

38 NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de. Ob. Cit.
39 NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de. Ibidem.
40 BEAL, Adriana. **Gestão Estratégica da Informação**: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2004, p. 94.
41 SÊMOLA, Marcos. Ob. Cit.

Emílio Tissato Nakamura e Paulo Lício de Geus informam que:

> O IDS é um elemento importante dentro do arsenal de defesa da organização, tendo como objetivo detectar atividades suspeitas, impróprias, incorretas ou anômalas, e que, além de ser crucial para a segurança interna, o IDS pode detectar ataques que são realizados por meio de portas legítimas permitidas e que, portanto, não podem ser protegidas por firewall[42].

Este componente pode obter informações importantes sobre tentativas de ataques, que não se pode obter normalmente, além de ser capaz de detectar e alertar os administradores quanto a possíveis ataques ou comportamentos anormais na organização.

4.1.3 Criptografia

Segundo Patrícia Peck, criptografia é:

> O método de codificação de dados que permite o acesso apenas de pessoas autorizadas, possuidoras de chave de acesso. Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, entre outras finalidades, para autenticar a identidade de usuários e autenticar transações bancária; proteger a integridade de transferências eletrônicas de fundos e proteger o sigilo de comunicações pessoais e comerciais.[43]

Para Marcos Sêmola, quando se fala de privacidade de comunicações o uso da criptografia é inevitável. E para ele:

> Criptografia é uma ciência que estuda os princípios, meios e métodos para proteger a confidencialidade das informações através da codificação ou processo de cifração e que permite a restauração da informação original através do processo de decifração[44].

Emílio Tissato Nakamura e Paulo Lício de Geus afirmam que a cifragem (*encryption*) é o processo de disfarçar a mensagem original, o texto claro (*plaintext* ou *cleartext*), de tal modo que sua substância é escondida em uma mensagem com texto cifrado (*ciphertext*), enquanto a decifragem (*decryption*) é o processo de transformar

---

[42] NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de. Segurança de Redes em Ambientes Corporativos. São Paulo: Novatec Editora, 2007, p. 265.

[43] PINHEIRO, Patrícia Peck. Direito Digital. 5ª Edição revista, atualizada e ampliada de acordo com as Leis n. 12.735 e 12.737, de 2012 – São Paulo: Saraiva, 2013.

44 SÊMOLA, Marcos - Gestão da Segurança da Informação: visão executiva da segurança da informação: aplicada ao Security Officer. Rio de janeiro: Campus, 2003. p. 122.

o texto cifrado de volta em texto original[45].

As técnicas principais de criptografia utilizadas atualmente são: simétrica e assimétrica, cuja diferença reside na quantidade de senhas e tipos de chaves, utilizadas para cifrar as informações, entre remetente e destinatário.

Por meio deste elemento da segurança da informação há a possibilidade de se alcançar as garantias necessárias à proteção dos dados, quais sejam: integridade, autenticidade, não-repúdio e sigilo.

O quadro abaixo (de KUROSE, James F., ROSS, Keith W.[46]) trazido em trabalho de Sergio Roberto Fuchs da Silva[47], expressa muito bem o que foi dito acima, acerca das funções e ou garantias atendidas pela criptografia:

Confidencialidade	Garante que apenas a origem e o destino tenham conhecimento da mensagem e que somente pessoas autorizadas possam vir a acessar as informações
Autenticação	Garante a identidade de quem está enviando a mensagem bem assim de um usuário ou de um dispositivo, permitindo o controle de acesso aos recursos de sistema computadorizado.
Integridade	Garante que o conteúdo da mensagem não sofreu alteração nem sofrerá alteração indevida,
Não repúdio	Previne que alguém negue a autoria de uma ação, garantindo que somente determinado usuário poderia ter realizado determinada ação em um sistema de informação.

4.1.4 Certificados digitais

Os certificados digitais são um dos elementos que têm como base a criptografia de chave pública, utilizado por esses protocolos, e são essenciais em um modelo de segurança como o do ambiente cooperativo, no qual diversos níveis de acesso devem ser controlados e protegidos, segundo Emílio Tissato Nakamura e Paulo Lício de Geus[48].

Acrescentam, ainda, os citados autores, que quando a criptografia de chave

45 NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de. Segurança de Redes em Ambientes Corporativos. São Paulo: Novatec Editora, 2007, p. 301.

46 KUROSE, James F., ROSS, Keith W. **Rede de Computadores e a Internet**. Uma abordagem top-down. 3ª Ed. São Paulo: Pearson Education do Brasil, 2006.

47 SILVA, Sérgio Roberto Fuchs da Silva. Proposta de modelo de controle de acesso lógico por servidores públicos aos recursos computacionais da administração pública. 2008.SRF SILVA - Brasília: UNB, nov, 2008 - academic.googlecode.com

48 NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de. Segurança de Redes em Ambientes Corporativos. São Paulo: Novatec Editora, 2007, p. 317

pública é utilizada, as chaves públicas de usuários ou sistemas podem estar assinadas digitalmente por uma autoridade certificadora (Certification Authority – CA) confiável, de modo que a utilização ou publicação falsa dessas chaves pode ser evitada.

As chaves públicas assinadas digitalmente por uma autoridade certificadora confiável constituem, assim, os certificados digitais.

Acerca da grande aplicabilidade do certificado digital em processo de autenticação e criptografia, destaca Marcos Sêmola, na publicação de informações, acessos a ambientes físicos, aplicações e equipamentos, envios de mensagens eletrônicas, redes virtuais privadas, ou na troca eletrônica de informações em geral[49].

4.1.5 Infraestrutura de chaves públicas

Uma citação de trecho do trabalho de Sergio Roberto Fuchs da Silva, parece ser necessário à introdução do tema:

> A Infraestrutura de Chaves Públicas – ICP pode ser definida como um conjunto de hardware, software, instalações, pessoas, políticas e procedimentos necessários à geração, gerenciamento, distribuição armazenamento e revogação dos certificados digitais.

Do ponto de vista organizacional, uma ICP pode ser entendida, segundo Nakamura e Geus (2002), como:

> [...] uma coleção de políticas, regras, responsabilidades, decisões, serviços e controles para a utilização da criptografia [...] além de ser um conjunto de ideias, entendimentos, convenções, concordâncias, contratos, leis, regulamentos, instituições, pessoas e confiança (grifo nosso), que permite que os certificados e as assinaturas digitais sejam utilizadas do mesmo modo que os documentos são utilizados e que os documentos em papel são assinados.

Boa, também, é a explicação didática proferida por Marcos Sêmola, para quem o processo de certificação se assemelha a um cartório, ou seja, para que a compra de um bem seja concretizada muitos documentos precisam ser autenticados por uma estrutura que tenha fé pública ou, no mínimo, confiança das partes envolvidas na transação, em processo que requer a presença física para identificação das partes através de documentos, comprovação visual da autenticidade dos documentos

49 SÊMOLA, Marcos - Gestão da Segurança da Informação: visão executiva da segurança da informação: aplicada ao Security Officer. Rio de janeiro: Campus, 2003. p. 125.

originais para, então, estender a originalidade às cópias.

A infraestrutura de chaves públicas é, com toda a certeza, um elemento essencial em um ambiente caracterizado pela complexidade das conexões e pelos diferentes níveis de usuários que têm de ser autenticados e controlados. E, neste sentido, é cada vez mais usada na garantia de identificação em transações eletrônicas e emails.

4.1.6 Esteganografia

Outra técnica que pode ser citada, cujo objetivo também está voltado para a privacidade no envio de informações, é a chamada “esteganografia”.

Trata-se de uma técnica que propõe o uso de métodos de camuflagem de informações sigilosas em mensagens e arquivos aparentamente inofensivos que só poderiam ser extraídas pelo destinatário, que detém o conhecimento do mapa de camuflagem, sendo essa a explicação dada por Marcos Sêmola[50].

Diferentemente da criptografia, cuja informação cifrada já a denuncia, a técnica da esteganografia não sinaliza a potenciais atacantes que determinada mensagem carrega informações sigilosas.

4.1.7 Autenticação e autorização

Trata-se de método bastante importante para os atuais padrões de informatização, automação e compartilhamento de informações, identificando a origem e o agente que está realizando o acesso.

Não há como imaginar a possibilidade do compartilhamento de informações valiosas sem a existência deste elemento de controle.

Neste segmento, pode-se listar:

- Senhas;
- Cartão com código barras;
- Cartão magnético;

[50] SÊMOLA, Marcos - Gestão da Segurança da Informação: visão executiva da segurança da informação: aplicada ao Security Officer. Rio de janeiro: Campus, 2003. p. 129.

- Smartcard;
- Tokens;
- Biometria;
- Geometria das mãos;
- Geometria da face;
- Identificação digital;
- Reconhecimento de voz;
- Leitura de íris;

É um processo de definição lógica, em que os elementos acima citados podem se apresentar individualmente ou em conjunto, com a exigência de mais de uma forma de processo de autenticação ou autorização. Sendo que, neste caso, há também a se considerar o nível de segurança necessário exigido pelas informações que são o objeto do procedimento, bem como o orçamento disponível para realização do processo de aquisição.

Contudo, é necessário criar uma regra para os equipamentos identificando estes de forma que fique clara a necessidade de exclusão de dados do equipamento em questão. Uma forma simples de implantação para esta regra, é etiquetar o equipamento e seu disco rígido para facilitar o trabalho de identificação.

Equipamentos servidores e portáteis devem passar obrigatoriamente pela limpeza de disco a fim de remover informações que podem ser consideradas pessoais e sigilosas.

Equipamentos servidores costumam, além de dados da empresa, possuir pastas compartilhadas, e nestas, usuários descuidados podem ter armazenado informações importantes, já os portáteis são normalmente utilizados em vários lugares, e por este motivo tendem a possuir os mais variados dados em seu interior.

Na sociedade em que se vive, um dos maiores ativos (coisas de valor) para as empresas e também para as pessoas comuns é a informação. Seja um projeto de algo ou uma foto tirada em um feriado na praia. Umas possuem valores muitas vezes inestimáveis e duradouros. Para outras esse tempo é mais descartável, porém não deixam de possuir algum valor ou trazer consequência no ambiente onde elas existem. Muita gente deve achar que jogar no lixo ou excluir (“deletar”) do computador irá fazer aquilo sumir definitivamente, mas isso não passa de um enganoso “achismo”.

O maior problema na classificação das condutas consideradas ilícitas para os crimes digitais reside no fato de que muitas vezes o computador é um simples meio para a concretização do delito. Nestes casos, seria totalmente dispensável a classificação na realização da conduta. Esses delitos, considerados como de ação livre, poderiam ser cometidos por várias maneiras, com o mesmo resultado esperado. De outra forma, existem crimes que só podem ser cometidos contra um sistema de informações ou contra as informações que estão nele armazenadas.

Na década de 80, Klaus Tiedemann[51] classifica os delitos de informática no campo dos crimes econômicos, conforme o seguinte:

a) Manipulações, que podem alterar a entrada, a saída dos dados e até mesmo o seu processamento;

b) Espionagem, que consiste no furto de informações armazenadas, inclusive com o uso inadequado ou criminoso de software.

c) A Sabotagem, com a destruição deliberada de algumas informações ou de todas;

d) Furto de tempo de utilização, que consiste no uso dos computadores do sistema para atividades estranhas ao serviço, pelos empregados.

Como em todas as classificações, existem diversas controvérsias, sendo que o mais comum é a separação das condutas em duas: a primeira, em que o computador é o meio para a concretização do crime, e a segunda abrangendo as demais condutas.

[51] Tiedemann, Klaus. **Poder econômico y delito**. trad. Amelia Mantilla Villegas. Barcelona: Ariel, 1985.

5 DIREITO DIGITAL

5.1 ACESSO NÃO AUTORIZADO OU HACKING

A conduta do acesso não autorizado ou indevido a um sistema de informação pode se dar por vários motivos, seja por mera curiosidade, seja com intenções francamente dolosas. É a porta de entrada para a concretização de outros ilícitos possíveis.

Tanto redes de computadores domésticos, de uma empresa e de órgãos governamentais, são sistemas compostos por elementos físicos (processadores e placas), comandados por elementos lógicos (programas específicos), ou mesmo por sistemas operacionais, tal como Windows ou Linux, que fazem a interligação dos elementos físicos, comandando-os a realizarem uma série de tarefas. A Internet nada mais é do que uma grande interligação de sistemas.

Para que ocorra a comunicação entre as redes e que os dados sejam compartilhados ou transferidos de uma forma segura e ordenada, tem que existir uma regulamentação do tráfego dessas informações. O conjunto dessas regras recebe o nome de “protocolo”. Na Internet, cada máquina que está interligada recebe uma numeração, um identificador chamado IP, que vem da sigla inglesa *internet protocol* ou protocolo da Internet. Porém, como o manuseio destes protocolos é algo extremamente complexo, foi criado um sistema, também conhecido pela sigla DNS, de *Domain Name System* – sistema de nomes de domínio, que executa a correspondência entre os endereços de IP e nomes ou termos específicos. Desta forma, facilita-se ao usuário a digitação de um endereço específico na Internet, ao invés da manipulação de uma série de números, tornando a comunicação muito mais amigável.

> Quanto à conduta de acessar, temos que se trata de obter acesso. Este, segundo o dicionário eletrônico Houaiss, é “a possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo, etc., visando receber ou fornecer dados”. Dessa forma, um tipo penal que descreva a conduta “acessar, sem autorização, sistema computacional” é bastante abrangente no sentido de coibir não só a conduta dos *hackers* que tentam remotamente acessar um sistema, bem como a de qualquer indivíduo com conhecimento menos técnico que diante de um computador alheio o acesse.[52]

[52] CRESPO, Marcelo Xavier de Freitas, op. cit., p.65

O acesso às informações ou sistemas de informação pode se dar em diversas formas, seja uma simples leitura, a execução de um programa e até mesmo a manipulação e edição desses dados. Isto depende de uma hierarquia de autorizações de acesso, de modo que, o sistema não fique inoperante nem tampouco devassado e exposto. Em resumo, parte-se da presunção de que o acesso a um sistema de informações tenha sido autorizado pelo seu proprietário, de modo que o acesso não autorizado é ilegítimo, constituindo então, uma conduta delituosa.

Todo sistema de informações possui um tipo de administrador, também conhecido por *webmaster*. Trata-se de um usuário com plenos poderes de acesso aos arquivos. O poder de acessar livremente as informações está ligado à ideia de operacionalização dos sistemas computacionais, mas não dá direito a manipular as informações e dados armazenados, não podendo o acesso ser feito para satisfazer uma curiosidade, mas tão somente para garantir a estabilidade e a funcionalidade do sistema.

As primeiras tentativas de acesso não autorizado às informações datam da década de 80, e se destinavam a fraudes com cartões de crédito e bancários, tecnologia esta que estava em seus primórdios de utilização. Da mesma forma, linhas telefônicas também foram alvos de ataques, fato que perdura até os dias de hoje, com as linhas digitais.

O modo mais comum de acesso não autorizado consiste em enganar a vítima, fazendo com que esta, ao pensar que está acessando uma página específica da Internet, na verdade esteja sendo direcionada para outra, sem saber. Não é absoluto que desta atividade resulte benefícios ou prejuízos financeiros.

No Brasil, mesmo que não esteja tipificada de forma clara a conduta do acesso não autorizado a sistemas de informação, no Direito Eleitoral, existe uma menção a este fato, na Lei 9.504/97, que faz a regulamentação do processo eleitoral:

> “Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
> I – obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem dos votos; (...)”.

Como um exemplo claro da falibilidade da legislação vigente, tem-se que a conduta tipificada é dirigida exclusivamente à interferência na contagem ou apuração dos votos, não abrangendo, por exemplo, se o acesso não autorizado foi realizado com o intuito de extorsão ou para obter dados como endereços e nomes, para o envio

de material comercial não solicitado.

Como já relatado anteriormente, na maioria das vezes, o acesso a um sistema é o princípio da prática de outros delitos. O acesso a informações ou bancos de dados nem sempre é desautorizado, haja visto o teor dos Arts. 313-A e 313-B do Código Penal:

> 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:
> Pena – reclusão de 2 a 12 anos e multa.
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 meses a 2 anos e multa.

Como ensina Guilherme de Souza Nucci, a inserção, alteração ou exclusão de dados em sistemas informatizados ou bancos de dados da Administração Pública, por funcionário autorizado (ou permitir que outra pessoa o faça), com o fim de obter vantagem indevida, que pode ser lucro, ganho, privilégio ou benefício ilícito, ainda que apenas ofensivo aos bons costumes; pode levar alguém a receber uma aposentadoria indevida ou se o beneficiário de uma aposentadoria faleceu, que seus herdeiros ou outra pessoa continue a receber indefinidamente, tudo isto causando prejuízo à Administração Pública.[53]

Outra forma de acesso não autorizado às informações ou aos bancos de dados são os chamados programas espiões (*Spywares)*. Estes nada mais são que programas destinados a rastrear informações do computador do usuário, como as preferências de páginas que costuma visitar**.**

Uma das formas mais inocentes de programas espiões são os chamados *cookies*, que nada mais são do que marcadores, que relacionam as preferências dos usuários, e destinam a eles propagandas e ofertas direcionadas ao seu perfil, sem que isso, na maioria das vezes, constitua uma prática comercial abusiva. No entanto, também existem os programas espiões que por meio de técnicas avançadas de informática, conseguem entrar na intimidade dos usuários, através inclusive das

---

[53] *Apud* PINHEIRO, Patrícia Peck. **Direito Digital**. 5.ed. revista, atualizada e ampliada de acordo com as Leis n. 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013.

câmaras de vídeo dos computadores, configurando uma total invasão de privacidade.

Há, ainda os programas chamados *keyloggers*, que monitoram as teclas digitadas em um teclado físico ou virtual e são de extrema importância para a obtenção de números de cartões de crédito, senhas bancárias e senhas pessoais.

5.2 DISSEMINAÇÃO DOS VÍRUS ELETRÔNICOS

Como os crimes digitais não precisam ser cometidos diretamente contra o computador da vítima, não se pode esquecer da existência de programas chamados *malwares*, em que o delito é perpetrado através de ataques virtuais contra redes de computadores e sistemas de grandes conglomerados ou sistemas computacionais governamentais.

Entre eles, tem-se os chamados vírus, códigos de programação que se agregam a outros programas, de modo a contaminar outras máquinas através do acesso, muitas vezes inocente, de outros usuários. Eles se propagam também através da transmissão de dados por um sistema que esteja corrompido, e sua intenção principal é explorar falhas de segurança dos sistemas e expandi-las, muitas vezes deixando o sistema inoperável ou extremamente lento.

Em 1988, o estudante do primeiro ano de mestrado em computação da *Cornell University*, Robert Tappan Morris, lança na rede um pequenino programa que segundo ele, teria o intuito de testar a capacidade de multiplicação do próprio programa. Esse programa é chamado de *worm* e fez com que 10% do sistema fosse totalmente destruído. Morris foi o primeiro a lançar um vírus na rede e o primeiro também a ser processado e condenado. Apelou da sentença, mas seu apelo foi rejeitado, fazendo com que se criasse uma jurisprudência, usada para condenar todos que praticassem este tipo de conduta.[54]

Assim como os vírus que atacam o organismo humano, os vírus da informática variam de acordo com o seu poder ofensivo, podendo causar até mesmo a perda total das informações armazenadas.

Uma vez infectado o sistema por estes programas, causam lentidão nos computadores, perda total dos dados e o contágio para outras máquinas através da

---

[54] PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: ed. Atlas, 2002.

troca de material móvel, como pen drives, e num passado recente, disquetes e cds. Eles, em algumas invasões, permitem que o computador infectado seja controlado remotamente, sendo que um terceiro pode, por meio deste controle externo, ler arquivos, acessar senhas e contas, excluir programas, até destruir totalmente o sistema operacional da máquina.

5.3 DIVULGAÇÃO DE INFORMAÇÕES NÃO SOLICITADAS

Um dos maiores problemas encontrados na Internet é o *spam.* Ele se assemelha às correspondências de mala direta que as pessoas recebem e nem se dão ao trabalho de abrir quando percebem tratar-se de propaganda. O *spam* é enviado sem que haja uma solicitação do usuário, em massa, para um número considerável de endereços. Os elementos que caracterizam o *spam*, portanto, são dois: a não solicitação da mensagem e o número excessivo de mensagens enviadas.

Como relatado por Marcelo Xavier de Freitas Crespo (p. 78), o primeiro *spam* documentado foi enviado em 3 de maio de 1978, um anúncio da DEC, um fabricante de computadores, falava sobre a máquina DEC-20, convidando para a apresentação do novo produto, na Califórnia. Esta mensagem gerou polêmica na rede exatamente por violar suas regras de uso. Curioso comentário, à época, do guru do GNU/Linux, Richard Stallman, que disse não achar o *spam* um problema, posição totalmente contrária à que tem hoje.

A informática e a tecnologia facilitaram muito o trabalho da propaganda: é absurdamente mais barato e também mais rápido conseguir atingir consumidores em potencial enviando inúmeros e-mails (obviamente não solicitados) com informações sobre quaisquer produtos ou ofertas, que por meio do correio convencional ou mesmo de distribuição de folhetos nas ruas. Além do aspecto de incômodo, já que muitas vezes rouba tempo de trabalho do usuário em ler e apagar as mensagens, isto se traduz em perdas financeiras para muitos e lucros para poucas pessoas.[55]

Não existem, atualmente, meios de coibir o envio de *spams* no Brasil, apenas o uso do mecanismo de multas contra as empresas. De acordo com a advogada

[55] PINHEIRO, Patrícia Peck. **Direito Digital**. 5.ed. revista, atualizada e ampliada de acordo com as Leis n. 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013. p.89.

Patrícia Peck Pinheiro, o *spam* configura crime previsto no art. 163 do Código Penal, o chamado crime de dano.[56]

> Art. 163. Destruir, inutilizar ou deteriorar coisa alheia:
> Pena – detenção, de 1 a 6 meses, ou multa.
> Dano qualificado
> Parágrafo único. Se o crime é cometido:
> I – com violência à pessoa ou grave ameaça;
> II – com emprego de substância inflamável ou explosiva, se o fato não constituir crime mais grave;
> III – contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista;
> IV – por motivo egoístico ou com prejuízo considerável para a vítima.
> Pena – detenção, de 6 meses a 3 anos, e multa, além da pena correspondente à violência.[57]

Porém, entende-se que isto somente seria admissível caso a quantidade de mensagens enviadas fosse enorme, a tal ponto de prejudicar o funcionamento normal da rede, como é o caso quando acontece o bombardeio intencional de mensagens, congestionando as comunicações e prejudicando um sem número de usuários.

[56] PINHEIRO, Patrícia Peck. **Direito Digital**. 5.ed. revista, atualizada e ampliada de acordo com as Leis n. 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013.

[57] Código Penal. Decreto-Lei nº 2.848/40. Vade Mecun Saraiva, Op. Cit.

5.4 ATAQUES INTENCIONAIS PARA PREJUDICAR O SISTEMA

Outro grande problema que vem incomodando muitos usuários da Internet é o ataque deliberado a uma página ou a um sistema, de modo a tirá-lo do ar, e desta forma, causar prejuízos ao proprietário, ou extorqui-lo.

Os ataques acima mencionados são chamados de ação de ataques de *DoS* (*Denial of Service*), ou simplesmente, negação de serviço. Começa com um acesso em massa a um determinado serviço ou computador conectado à Internet, sobrecarregando o sistema de processamento de dados, de tal forma que os outros usuários não consigam utilizá-lo, ou forçando a retirada de serviços de um provedor de acesso.

Para se ter uma ideia do prejuízo que pode ser causado, cogite-se que um ataque de denegação de serviço (*DoS*) consiga tirar de serviço uma página de uma loja de departamento na Internet. Os danos seriam muito grandes e talvez de difícil reparação. As redes internas das grandes empresas ou escritórios também podem ser afetadas, mesmo que se acredite que elas estejam protegidas.

5.5 ENGENHOSIDADE SOCIAL E PHISHING

O que atualmente se entende por Engenhosidade Social, há muito tempo é relatado no Direito Penal como um ardil ou artifício fraudulento. Trata-se de uma forma de ludibriar um usuário que detenha dados ou informações importantes a quem alguém deseje ter acesso. Não requer conhecimento especializado, portanto está ao alcance de qualquer pessoa.

Desta forma, usando meios aparentemente lícitos, o invasor “conquista” a confiança do usuário detentor da informação, na maioria das vezes inocente, e contando com a curiosidade deste, faz com que ocorra o preenchimento de formulários ou questionários. Esta conduta, utilizada em conjunto com técnicas apuradas de agentes criminosos, termina por se tipificar como um estelionato. Porém, como a identificação do agente infrator é muito difícil, quando não impossível, este crime acaba impune.

A página usada nestas práticas delituosas quase sempre é cópia de uma página de um órgão oficial, de operadoras de cartão de crédito e de empresas do sistema financeiro. Estas páginas falsas, extremamente bem confeccionadas, levam o usuário visitante a preencher um formulário com informações, que são desviadas para o *site* do criminoso, que usa os dados para cometer toda a sorte de desvios financeiros e trazendo grandes prejuízos às instituições financeiras.

Neste sentido, sempre que ocorrer a combinação simultânea dos elementos fraude ou ardil com vantagem indevida e prejuízo alheio, tem-se, a tipificação de um crime de estelionato. Porém, o simples fato de se enviar mensagens fraudulentas ou capazes de induzir ao erro, não é considerado como fato típico em nosso ornamento jurídico.

Com isto, um Substitutivo ao Projeto de Lei (PL) nº 84/99 prevê a criação de uma figura jurídica que seria chamada de “estelionato eletrônico”. Pela proposta apresentada, incluir-se-ia um inciso no § 2º do artigo referente ao crime de estelionato (Art. 171 do Código Penal), tipificando que aquele que propagasse, por qualquer meio, mensagem ou código malicioso com a intenção de facilitar ou mesmo permitir o acesso indevido a sistema de computador, responderia pelo ato nas mesmas penas do *caput* do referido artigo.

Outra forma de crime é informar ao usuário que ele fez determinada operação financeira (de que ele, obviamente não se lembra ou não tem certeza), e que o mesmo terá seu nome incluído no cadastro de devedores, se não efetivar um pagamento. A vítima, na maioria das vezes fragilizada, imprime o boleto ou paga a conta fazendo uma transferência para um *site* que ele imagina ser o oficial do banco. Está concretizado o delito.

Um dos casos mais comentados, recentemente, que inclusive levou à edição de uma lei que foi apelidada com o nome da atriz envolvida, aparece na Internet como um *link* para determinada página, que mostraria fotos de pessoas públicas em posições ou situações que as comprometam; ou imagens de determinada pessoa nua. Isto atiça a curiosidade da maioria das pessoas, mas esta página não exibe as fotos ou imagens que alardeia, mas um arquivo executável.

5.6 INTERCEPTAÇÃO ILEGAL DE DADOS

A Constituição Federal consagra como um dos direitos fundamentais a inviolabilidade das comunicações (telefone, correspondência, dados e Internet). Porém, esta inviolabilidade não é absoluta, podendo, via judicial, ser retirada e autorizada a interceptação das comunicações para fins de investigação policial.

Desta forma, a Lei nº 9.296/96, de 24 de julho de 1996, que trata da interceptação de comunicações telefônicas, autoriza também a quebra de sigilo em sistemas de informática. Além disso, prevê a ocorrência de crime na conduta de quem realiza essas interceptações sem autorização judicial ou em condições diversas da que foi concedida.[58]

Estas permissões, concedidas por meio de lei ordinária, trouxeram alguns questionamentos a respeito da Constituição Federal autorizar a interferência em comunicações que não sejam de natureza estritamente telefônica. Em seu artigo 5º, a Constituição diz, expressamente:

> Art. 5º (...)
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Da leitura do texto legal acima citado, duas posições doutrinárias são encontradas, uma admitindo a interceptação das comunicações por meio da informática ou telemática e a outra não permitindo seu emprego. Conforme ensina Vicente Greco Filho[59], a posição mais coerente com o texto constitucional, é o entendimento de que a possibilidade de interceptação contempla somente as comunicações telefônicas, nunca as de transmissão ou recepção de dados nem as telegráficas (estas, atualmente, totalmente anacrônicas). Tudo isto pelo conceito de que o telefone transmite e recebe sinais vocais e todos os outros sistemas conectados aos telefones não são equiparados a eles. Mas não há como negar que a informática e a telemática sejam usadas como meios de comunicação.[60]

Afastada a discussão sobre a legalidade ou não das interceptações, tem-se que

---

[58] GRECO FILHO, Ibidem.

[59] GRECO FILHO, Vicente. **Interceptação telefônica: considerações sobre a Lei nº 9.296/96, de 24 de julho de 1996**. São Paulo: Saraiva, 2006.

[60] GRECO FILHO, Ibidem.

a Lei nº 9.296/96 também prevê, em seu art. 10, a tipificação como conduta criminosa, a alguém que realizar essas violações sem autorização judicial ou de forma diversa da autorizada. Não resta a menor dúvida que a conduta de quebra do sigilo das comunicações, especificamente a transmissão e recepção de dados em sistemas informatizados deve ser evitada e condenada, uma vez que as pessoas dependem cada vez mais desse tipo de comunicação para o relacionamento diário, seja no âmbito pessoal, seja no âmbito profissional. Uma nova redação acerca da tipificação constante naquele instrumento legal afastaria possíveis questionamentos e melhoraria sua abrangência.

5.7 VIOLAÇÕES DE DIREITOS AUTORAIS (CRIMES DIGITAIS IMPRÓPRIOS)

Crimes digitais impróprios são aqueles já tipificados no ordenamento jurídico, praticados atualmente com o auxílio das novas tecnologias.

O problema da violação dos direitos autorais é extremamente complexo, porque envolve tanto o direito à informação quanto o direito à propriedade intelectual. A legislação que regula o assunto é considerada recente, mas ao mesmo tempo, ultrapassada e obsoleta. O chamado Marco Civil da Internet não desfaz todas as dúvidas.

A lei brasileira específica sobre Direitos Autorais, Lei nº 9.610/98, é de uma época em que as conexões à Internet eram feitas por meio de linhas telefônicas, as chamadas conexões discadas, a banda larga era um sonho de consumo distante. Segundo Sérgio Staut, professor de Teoria do Direito na Universidade Federal do Paraná (UFPR), autor do livro “Direitos Autorais: entre as relações humanas e as relações jurídicas”, a realidade do tempo em que a referida Lei foi promulgada era tão diferente que a palavra Internet sequer consta no texto legal.

A violação dos direitos autorais, bem como o uso indevido das marcas registradas e a distribuição ilegal de cópias de programas com propriedade intelectual reconhecida, a chamada pirataria, é um problema constante nos dias de hoje. Muitas pessoas tentam justificar o ato de “baixar” um arquivo ou programa pela Internet para usá-lo e repassá-lo aos amigos, como sendo algo aparentemente inofensivo, quase uma pequena brincadeira. Mas o reflexo destes pequenos atos gera grandes prejuízos, pois a cópia não autorizada atinge dimensões planetárias, quase sem

qualquer chance de controle.

A legislação brasileira protege a propriedade intelectual, que compreende a propriedade industrial referindo-se às patentes, ao desenho industrial do produto e às marcas propriamente ditas; e os direitos autorais referentes ao desenvolvimento dos programas, bancos de dados e documentação técnica pertinente. Não é o fato de um programa ou aplicativo estar disponível na rede, que isto o torna de domínio público, podendo desta forma ser usado por qualquer pessoa, sem que isto gere, de alguma forma, uma retribuição pecuniária ao seu proprietário legal.

Desta forma, é considerada conduta criminosa a violação dos direitos de propriedade de programa ou aplicativo de computador, assim como a compra e venda, o depósito ou a ocultação de original ou cópia indevida, produzida por meio ilícito, com fins de comercialização. Este é o espírito da Lei nº 9.609/98, a Lei do software. Já as condutas delitivas não diretamente ligadas ao software são punidas com base no art. 184 do Código Penal. Quanto às violações relativas a propriedade industrial, estas são tipificadas com base na Lei 9.279/96 (Código de Propriedade Industrial).

Como um exemplo recente, no início de 2012, foi preso na Austrália, o proprietário do maior site de compartilhamento de arquivos então existente, o Megaupload, a pedido do FBI. O neozelandês Kit Dotcom (não por acaso seu sobrenome significa ponto com, uma designação da Internet para identificar páginas comerciais) foi acusado de violar os direitos autorais e distribuir material pirateado. Respondendo ao processo em liberdade, enquanto o governo americano pede sua extradição, mesmo que o homem que ficou riquíssimo ao criar uma página na Internet para o compartilhamento de arquivos de filmes e músicas seja condenado e punido, é totalmente inviável localizar e identificar os milhões de usuários do Megaupload. A pergunta que resta é como proteger adequadamente algo não físico, intangível, e se é preciso ou eficaz buscar alguma forma de punição.

O Marco Civil da Internet traz em seu bojo uma proposta que se não resolve o problema dos direitos autorais na rede, deve gerar muita polêmica. Em seu art. 15, o texto legal diz que o provedor de acesso pode ser responsabilizado se não tomar as devidas providências para que no âmbito de seu serviço e dentro do prazo designado, tornar indisponível o conteúdo considerado impróprio.

O presidente da comissão da Câmara dos Deputados criada para analisar o projeto do Marco Civil da Internet, deputado João Arruda (PMDB-PR), sugeriu que a questão dos direitos autorais é o único ponto frágil de todo o projeto e que a Internet

deve ser um espaço sem restrições, para divulgar a cultura.

6 RESPONSABILIDADE DOS PROVEDORES E DISPONIBILIZADORES DE INFORMAÇÕES

Os provedores de acesso são aquelas empresas que conectam os usuários à Internet, e os provedores de serviços ou conteúdo proveem contas de e-mail, hospedagem de páginas, serviços de troca de mensagens e mercadorias, etc. os provedores de acesso também podem prestar serviços de fornecimento de conteúdo.

Conforme cita Marcelo Xavier de Freitas Crespo[61]:

> [...] Chega-se a apontar algumas condutas que poderiam ser atribuídas aos provedores de acesso, como é o caso da desobediência, quando descumpridas requisições das autoridades competentes, débito não autorizado em cartão de crédito que poderia configurar delito de estelionato e favorecimento real de usuário ou criminoso. A doutrina estrangeira, por seu turno, não traz muitas considerações sobre o tema, senão a questão da responsabilidade penal dos provedores de conteúdo ou serviços, especialmente por crimes envolvendo questões relativas ao ódio, pornografia infantil e terrorismo. Guilherme Guimarães Feliciano parte de um conceito do que seja difusão, entendendo como tal conduta de tornar público conteúdo ilícito. Depois, parte de conceito restritivo, considerando que, caso o tipo penal preveja a conduta de “difundir”, então, os provedores poderiam ser incursos como autores do delito. Assevera, ainda, que muitas vezes os provedores serão omissos. Ocorre que, nesse caso, somente poderiam ser responsabilizados caso tivessem conhecimento do conteúdo ilícito armazenado em seus computadores. Até porque a diretiva 200/31/CE do Parlamento Europeu e do Conselho da Europa dispõe que os provedores só poderão ser responsabilizados caso tenham efetivo conhecimento de que as pessoas mantém conteúdo ilícito nas suas máquinas, devendo agir de imediato para retirá-lo do ar.

Em se tratando de Direito brasileiro, a Constituição Federal contempla a responsabilidade penal da pessoa jurídica apenas na ocorrência de crimes ambientais. A ideia da responsabilização criminal das pessoas jurídicas, no caso dos provedores de acesso, seria possível através de uma Emenda Constitucional, porém devendo permanecer como *ultima ratio*.

---

[61] CRESPO, Marcelo Xavier da Silva, op. cit., p. 109

6.1 DEEP WEB – O LADO OBSCURO DA INTERNET

Muito é escrito e falado sobre a parte não comercial da rede de computadores, mais por desconhecimento e receio, do que um perigo real. A chamada *Deep Web*, ou numa tradução literal, Rede Profunda. Como a maioria das aplicações atuais destinadas a computadores reflete a inclinação comercial da rede, era natural que atividades marginais procurassem um espaço alternativo para a sua existência.[62]

O navegador especial, conhecido como TOR (*The Onion Router*, “o roteador da cebola”, evidenciando a referência física às camadas de uma cebola) foi criado pelo Laboratório de Pesquisa Naval da Marinha dos Estados Unidos, em 2002, como uma alternativa, um método seguro de enviar e receber informações. Ele tenta garantir o anonimato do usuário. Porém, o projeto tornou-se independente da ação governamental em 2003 e a partir de 2006 é financiado por uma organização própria.

Criptografando diversas vezes os dados e informações, tornando muito difícil o rastreamento, como uma forma de manter um mínimo de segurança. Ao contrário do que usualmente ocorre na Internet comum, onde as informações são compartilhadas diretamente pelos usuários, o sistema da *Deep Web* cria um ponto de confluência, para o qual são direcionadas todas as informações a serem trocadas. As páginas encontradas na rede TOR não possuem as terminações comumente encontradas na rede de computadores, mas sempre terminam com .onion, como é o caso do *site* Silk Road, e não são acessíveis por outros mecanismos de busca.

Também como uma forma de confundir possíveis ações governamentais ou policiais, as páginas têm seu endereço composto por letras e números numa combinação sem sentido.

Mas, nem tudo é bizarro ou criminoso nessa rede. O Wikileaks, que revelou segredos desconfortáveis para a diplomacia americana, nasceu na *Deep Web*. Habitantes dos países onde regimes totalitários impedem o acesso à informação, usam esse espaço para a comunicação, como uma forma de desviar da censura oficial.

---

[62] ANDRADE, Rayssa Lara Oliveira de. **A Biblioteca 2.0 sob a ótica da Gestão da Segurança da Informação**: um estudo de caso com a Biblioteca Nacional de Brasília. Disponível em: (http://repositorio.ufrn.br:8080/monografias/bitstream/1/85/1/RayssaLOA_Monografia.pdf). Natal, 2011. . Acesso em 20 de julh. de 2014.

7 POLITICAS DA SEGURANÇA DA INFORMAÇÃO

Nas concepções de Kurose, uma política de segurança trata dos aspectos humanos, culturais e tecnológicos de urna organização, levando também em consideração os processos e os negócios, além da legislação local. “[...] é com base nessa política de segurança que as diversas normas e os vários procedimentos devem ser criados”.[63]

Além de seu papel primordial nas questões relacionadas com a segurança, a política de segurança, uma vez fazendo parte da cultura da empresa, tem uma importante função como facilitadora e simplificadora do gerenciamento de todos os seus recursos. Nakamura entende que “[...] de fato, o gerenciamento de segurança é a arte de criar e administrar a política de segurança, pois não é possível gerenciar o que não pode ser definido”.[64]

Assim, a política de segurança trata dos aspectos humanos, culturais e tecnológicos de urna organização, levando também em consideração os processos e os negócios, além da legislação local. É com base nessa política de segurança que as diversas normas e os vários procedimentos devem ser criados.

Desta forma, elenca-se que o devido planejamento da política de segurança exige uma visão englobada de todos os aspectos, visto que os riscos sejam entendidos para que possam ser enfrentados. Normalmente, a abordagem com relação à segurança é reativa, o que pode, invariavelmente, trazer futuros problemas para a organização. Nesta esfera, uma abordagem proativa é primordial e depende de uma política de segurança bem definida, na qual a definição das responsabilidades individuais deve estar bem clara, de modo a facilitar o gerenciamento da segurança em toda a organização.[65]

As organizações podem aprovar uma política de segurança apenas para satisfazer os auditores, e isso acaba comprometendo a própria organização, que pode obter uma política incoerente e sem os detalhes essenciais para o seu sucesso. Tal tipo de comportamento faz com que os executivos devam ser convencidos de que o

---

[63] KUROSE, James F., ROSS, Keith W. **Rede de Computadores e a Internet**. Uma abordagem top-down. 3.ed. São Paulo: Pearson Education do Brasil, 2006. p.43.
[64] NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Corporativos**. São Paulo: Novatec, 2007.p.88.
[65] Ibidem. p. 89.

melhor a fazer é atuar de modo proativo, em oposição ao comportamento reativo. Sendo reativos, em caso de algum incidente de segurança, os executivos serão obrigados a agir em circunstâncias negativas e de extrema urgência e pressão, trazendo, como principal consequência, problemas quanto à confiança de clientes e de parceiros de negócios, e também com a opinião pública. O ideal é mostrar os estudos que provam que é mais barato considerar a perspectiva de 'prevenir, deter e detectar o que a de 'corrigir e recuperar'.[66]

Ou seja, as dependências existentes nos diversos tópicos da política, das normas e dos procedimentos deverão ser consideradas para que não sejam feitos esforços em vão. Por exemplo, unia política que torna obrigatório o uso de uma autenticação eficiente para todo acesso remoto deve tratar também dos aspectos que dela dependem, como a arquitetura da solução e dos produtos-padrão a serem utilizados. Sem isso, sua implementação fica comprometida; os usuários irão reclamar que não conseguem trabalhar remotamente (comprometendo sua produtividade) e os executivos, por sua vez, irão reclamar que os usuários não podem trabalhar remotamente, porque não existe a tecnologia que possibilita o acesso remoto seguro.[67]

Urna visão abrangente dos problemas relacionados à segurança, juntamente com o conhecimento dos processos de negócios da organização, é fundamental para o desenvolvimento da política. É imprescindível que exista um líder técnico, que seja profundo conhecedor dos aspectos de segurança e tenha uma visão sobre as tendências e tecnologias nessa área, a fim de possibilitar a implementação das normas e dos procedimentos definidos na política.[68]

7.1 CONHECIMENTO TÉCNICO DA INFORMAÇÃO

É necessário conhecer a complexidade que envolve a rede e os sistemas de informação, para que os recursos adequados sejam alceados no desenvolvimento da política de segurança. O fato de algum desses aspectos ser complexo não significa que deva ser ignorado. Para tanto, é preciso recorrer ao auxílio de ferramentas para

---

[66] NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Corporativos**. São Paulo: Novatec, 2007. p.98.
[67] KUROSE. Ob. Cit, p.44.
[68] Ibidem.p.56.

a realização dessa tarefa, tais como um software de planejamento de contingência. [69]

Tal complexidade exige que a organização aloque recursos para sistemas de gerenciamento de redes, sistemas de detecção de intrusões, sistemas de automação de distribuição de software, sistemas de checagem de licenças de software e outros mecanismos de automação, os quais as pessoas não podem realizar sozinhas. É importante demonstrar para os executivos as novas ferramentas existentes e o porquê de sua popularidade, a fim de comprovar que essa complexidade específica pode ser gerenciada.[70]

Silva ainda lembra que “[...] um processo disciplinar específico para os casos de não cumprimento da política definida é importante para a organização”. Por exemplo, se um usuário cometer um erro, a primeira medida é avisá-lo de sua falta. Se o erro se repetir, o chefe do usuário deve receber um comunicado. Se houver um terceiro erro, o usuário será suspenso por duas semanas e se esse erro persistir, o usuário será demitido. Essa abordagem é crucial para evitar situações em que o usuário seja sumariamente demitido, logo no seu primeiro erro, somente para mostrar aos outros funcionários quem detém o poder na organização.[71]

---

[69] SETZER, Valdemar W. Dado, **Informação, Conhecimento e Competência.** Disponível em: http://www.ime.usp.br/~vwsetzer/datagrama.html. Acesso em 20 de julh. de 2014.

[70] SILVA, Sérgio Roberto Fuchs da Silva. **Proposta de modelo de controle de acesso lógico por servidores públicos aos recursos computacionais da administração pública**. 2008.SRF SILVA - Brasília: UNB, nov, 2008 - academic.googlecode.com

[71] Ibidem.

CONCLUSÃO

Entende-se por meio deste estudo que a informação sintoniza o mundo, pois referencia o homem ao seu semelhante e ao seu espaço vivencial em um ponto imaginário do presente, com uma perspectiva do passado e uma visão de esperança do futuro, sendo ela um recurso essencial para a tomada de decisão, e aplicando adequadamente os conceitos apresentados, informações rápidas e com alto valor agregado, que tendem a estar disponíveis na forma, agregação, quantidade, local e tempo exigidos na tomada de decisão.

Assim sendo, é notório que existem muitos conceitos de informação e eles estão inseridos em estruturas teóricas mais ou menos explícitas. Quando se estuda informação, é fácil perder a orientação, para tanto é necessário saber o que é a informação e como e onde se aplica, sendo que na percepção deste estudo, a distinção mais importante é aquela entre informação como um objeto ou coisa e informação como um conceito subjetivo, e para tal deve-se cuidar desta informação.

Diante de tais aspectos são extremamente necessárias as medidas preventivas de proteção e controle para que as ocorrências de riscos sejam, significativamente, reduzidas ou inibidas, atentando-se sempre a aplicação das medidas para que não ocorra suspensão ou interrupção dos serviços ou mesmo violação de dados.

Faz-se necessário um sistema de informação que exerça com veemência este papel de segurança, prezando pela clareza e sigilo dos dados organizacionais, porque é por meio destes que as empresas têm seu diferencial de trabalho, bem como todos os outros órgãos e repartições públicas.

Na Coordenação da Receita do Estado e na Secretaria da Fazenda a necessidade não é diferente.

Importante aqui é tomar o conhecimento pontual das ocorrências que podem inviabilizar o processo de manutenção dos dados obtidos junto aos contribuintes, manter estes dados e utilizá-los, sempre garantida a qualidade de segurança por meio de uma política série de segurança de informação, que contemple a observação dos crimes que podem ser praticados contra a Fazenda com o intuito de desestabilizá-la.

Esse o intuito deste estudo, cuja atenção quanto à segurança dos dados e sua manutenção, deve ser prática da Secretaria da Fazenda e da Coordenação da Receita do Estado do Paraná.

REFERÊNCIAS

ANDRADE, Rayssa Lara Oliveira de. **A Biblioteca 2.0 sob a ótica da Gestão da Segurança da Informação**: um estudo de caso com a Biblioteca Nacional de Brasília. Disponível em: (http://repositorio.ufrn.br:8080/monografias/bitstream/1/85/1/RayssaLOA_Monografia.pdf). Natal, 2011. Acesso em 20 de julho de 2014.

BEAL, Adriana. **Gestão Estratégica da Informação:** como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2004.

Boas Práticas em Segurança da Informação. 4.ed. do Tribunal de Contas da União. Disponível em: http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF. Acesso em 20 de julho de 2014.

GIL, A.C. **Métodos e técnicas de pesquisa**. São Paulo: Atlas, 1999.

GRECO FILHO, Vicente. **Interceptação telefônica**: considerações sobre a Lei nº 9.296/96, de 24 de julho de 1996. São Paulo: Saraiva, 2006.

KUROSE, James F., ROSS, Keith W. **Rede de Computadores e a Internet**. Uma abordagem top-down. 3.ed. São Paulo: Pearson Education do Brasil, 2006.

LAKATOS, E. M. **Técnicas de Pesquisa**. 5. ed. São Paulo: Ed. Atlas, 2008.

MINAYO, M.C. de S. (Org.) **Pesquisa social: teoria, método e criatividade**. 22 ed. Rio de Janeiro: Vozes, 2003.

NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Corporativos**. São Paulo: Novatec, 2007.

OLIVEIRA, Djalma de Pinho Rebouças de. **Sistemas de informação e métodos**: Uma abordagem gerencial. 9.ed. São Paulo: Atlas, 2002.

PINHEIRO, Patrícia Peck. **Direito Digital**. 5.ed. revista, atualizada e ampliada de acordo com as Leis n. 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** visão executiva da segurança da informação: aplicada ao Security Officer. Rio de janeiro: Campus, 2003.

SETZER, Valdemar W. Dado, **Informação, Conhecimento e Competência.** Disponível em: http://www.ime.usp.br/~vwsetzer/datagrama.html. Acesso em 20 de julho de 2014.

SILVA, Sérgio Roberto Fuchs da Silva. **Proposta de modelo de controle de acesso lógico por servidores públicos aos recursos computacionais da administração pública**. 2008.SRF SILVA - Brasília: UNB, nov, 2008 - academic.googlecode.com

ANEXO

DECRETO Nº 7.845, DE 14 DE NOVEMBRO DE 2012

Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

A PRESIDENTA DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, **caput**, incisos IV e VI, alínea "a", da Constituição, e tendo em vista o disposto nos arts. 25, 27, 29, 35, § 5º, e 37 da Lei nº 12.527, de 18 de novembro de 2011,

DECRETA:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Este Decreto regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo federal, e dispõe sobre o Núcleo de Segurança e Credenciamento, conforme o disposto nos arts. 25, 27, 29, 35, § 5º, e 37 da Lei nº 12.527, de 18 de novembro de 2011.

Art. 2º Para os efeitos deste Decreto, considera-se:

I - algoritmo de Estado - função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal;

II - cifração - ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem clara por outros ininteligíveis por pessoas não autorizadas a conhecê-la;

III - código de indexação - código alfanumérico que indexa documento com informação classificada em qualquer grau de sigilo;

IV - comprometimento - perda de segurança resultante do acesso não autorizado;

V - contrato sigiloso - ajuste, convênio ou termo de cooperação cujo objeto ou execução implique tratamento de informação classificada;

VI - credencial de segurança - certificado que autoriza pessoa para o tratamento de informação classificada;

VII - credenciamento de segurança - processo utilizado para habilitar órgão ou entidade pública ou privada, e para credenciar pessoa para o tratamento de informação classificada;

VIII - decifração - ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

IX - dispositivos móveis - equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento;

X - gestor de segurança e credenciamento - responsável pela segurança da informação classificada em qualquer grau de sigilo no órgão de registro e posto de controle;

XI - marcação - aposição de marca que indica o grau de sigilo da informação classificada;

XII - medidas de segurança - medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

XIII - órgão de registro nível 1 - ministério ou órgão de nível equivalente habilitado pelo Núcleo de Segurança e Credenciamento;

XIV - órgão de registro nível 2 - órgão ou entidade pública vinculada a órgão de registro nível 1 e por este habilitado;

XV - posto de controle - unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo;

XVI - quebra de segurança - ação ou omissão que implica comprometimento ou risco de comprometimento de informação classificada em qualquer grau de sigilo;

XVII - recurso criptográfico - sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração; e

XVIII - tratamento da informação classificada - conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

CAPÍTULO II

DO CREDENCIAMENTO DE SEGURANÇA

Seção I

Dos Órgãos

Art. 3º Compete ao Núcleo de Segurança e Credenciamento, órgão central de credenciamento de segurança, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República, nos termos do art. 37 da Lei nº 12.527, de 2011:

I - habilitar os órgãos de registro nível 1 para o credenciamento de segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada;

II - habilitar postos de controle dos órgãos de registro nível 1 para armazenamento de informação classificada em qualquer grau de sigilo;

III - habilitar entidade privada que mantenha vínculo de qualquer natureza com o Gabinete de Segurança Institucional da Presidência da República para o tratamento de informação classificada;

IV - credenciar pessoa que mantenha vínculo de qualquer natureza com o Gabinete de Segurança Institucional da Presidência da República para o tratamento de informação classificada;

V - realizar inspeção e investigação para credenciamento de segurança necessárias à execução do previsto, respectivamente, nos incisos III e IV do **caput**; e

VI - fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada.

Art. 4º Fica criado o Comitê Gestor de Credenciamento de Segurança, integrado por representantes, titular e suplente, dos seguintes órgãos:

I - Gabinete de Segurança Institucional da Presidência da República, que o coordenará;

II - Casa Civil da Presidência da República;

III - Ministério da Justiça;

IV - Ministério das Relações Exteriores;

V - Ministério da Defesa;

VI - Ministério da Ciência, Tecnologia e Inovação;

VII - Ministério do Planejamento, Orçamento e Gestão; e

VIII - Controladoria-Geral da União.

§ 1º Os membros titulares e suplentes serão indicados pelos dirigentes máximos dos órgãos representados, e designados pelo Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República.

§ 2º A participação no Comitê será considerada prestação de serviço público relevante, não remunerada.

§ 3º Poderão ser convidados para as reuniões do Comitê representantes de órgãos e entidades públicas e privadas, ou especialistas, para emitir pareceres e fornecer informações.

Art. 5º Compete ao Comitê Gestor de Credenciamento de Segurança:

I - propor diretrizes gerais de credenciamento de segurança para tratamento de informação classificada;

II - definir parâmetros e requisitos mínimos para:

a) qualificação técnica de órgãos e entidades públicas e privadas, para credenciamento de segurança, nos termos dos arts. 10 e 11; e

b) concessão de credencial de segurança para pessoas, nos termos do art. 12; e

III - avaliar periodicamente o cumprimento do disposto neste Decreto.

Art. 6º Compete ao Gabinete de Segurança Institucional da Presidência da República:

I - expedir atos complementares e estabelecer procedimentos para o credenciamento de segurança e para o tratamento de informação classificada;

II - participar de negociações de tratados, acordos ou atos internacionais relacionados com o tratamento de informação classificada, em articulação com o Ministério das Relações Exteriores;

III - acompanhar averiguações e processos de avaliação e recuperação dos danos decorrentes de quebra de segurança;

IV - informar sobre eventuais danos referidos no inciso III do **caput** ao país ou à organização internacional de origem, sempre que necessário, pela via diplomática; e

V - assessorar o Presidente da República nos assuntos relacionados com credenciamento de segurança para o tratamento de informação classificada, inclusive no que se refere a tratados, acordos ou atos internacionais, observadas as competências do Ministério das Relações Exteriores.

Parágrafo único. O Gabinete de Segurança Institucional da Presidência da República exercerá as funções de autoridade nacional de segurança para tratamento de informação classificada decorrente de tratados, acordos ou atos internacionais.

Art. 7º Compete ao órgão de registro nível 1:

I - habilitar órgão de registro nível 2 para credenciar pessoa para o tratamento de informação classificada;

II - habilitar posto de controle dos órgãos e entidades públicas ou privadas que com ele mantenham vínculo de qualquer natureza, para o armazenamento de informação classificada em qualquer grau de sigilo;

III - credenciar pessoa que com ele mantenha vínculo de qualquer natureza para o tratamento de informação classificada;

IV- realizar inspeção e investigação para credenciamento de segurança necessárias à execução do previsto no inciso III do **caput**; e

V - fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada, no âmbito de suas competências.

Art. 8º Compete ao órgão de registro nível 2 realizar investigação e credenciar pessoa que com ele mantenha vínculo de qualquer natureza para o tratamento de informação classificada.

Parágrafo único. A competência para realização de inspeção e investigação de que trata o inciso IV do **caput** do art. 7º poderá ser delegada a órgão de registro nível 2.

Art. 9º Compete ao posto de controle:

I - realizar o controle das credenciais de segurança das pessoas que com ele mantenham vínculo de qualquer natureza; e

II - garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.

Seção II

Dos procedimentos

Art. 10. A habilitação dos órgãos e entidades públicas para o credenciamento de segurança fica condicionada aos seguintes requisitos:

I - comprovação de qualificação técnica necessária à segurança de informação classificada em qualquer grau de sigilo; e

II - designação de gestor de segurança e credenciamento, e de seu substituto.

Art. 11. A concessão de habilitação de entidade privada como posto de controle fica condicionada aos seguintes requisitos:

I - regularidade fiscal;

II - comprovação de qualificação técnica necessária à segurança de informação classificada em qualquer grau de sigilo;

III - expectativa de assinatura de contrato sigiloso;

IV - designação de gestor de segurança e credenciamento, e de seu substituto; e

V - aprovação em inspeção para habilitação de segurança.

Art. 12. A concessão de credencial de segurança a uma pessoa fica condicionada aos seguintes requisitos:

I - solicitação do órgão ou entidade pública ou privada em que a pessoa exerce atividade;

II - preenchimento de formulário com dados pessoais e autorização para investigação;

III - aptidão para o tratamento da informação classificada, verificada na investigação; e

IV - declaração de conhecimento das normas e procedimentos de credenciamento de segurança e de tratamento de informação classificada.

Art. 13. A habilitação para credenciamento de segurança e a concessão de credencial de segurança resultarão da análise objetiva dos requisitos previstos neste Decreto.

Art. 14. Os órgãos de registro nível 1 e nível 2 poderão firmar ajustes, convênios ou termos de cooperação com outros órgãos ou entidades públicas, habilitados, para:

I - credenciamento de segurança e tratamento de informação classificada; e

II - realização de inspeção e investigação para credenciamento de segurança.

Art. 15. Cada órgão de registro terá no mínimo um posto de controle, habilitado.

Art. 16. Na hipótese de troca e tratamento de informação classificada em qualquer grau de sigilo com país ou organização estrangeira, o credenciamento de segurança no território nacional se dará somente se houver tratado, acordo, memorando de entendimento ou ajuste técnico firmado entre o país ou organização estrangeira e a República Federativa do Brasil.

CAPÍTULO III

DO TRATAMENTO DE INFORMAÇÃO CLASSIFICADA

Seção I

Disposições Gerais

Art. 17. Os órgãos e entidades adotarão providências para que os agentes públicos conheçam as normas e observem os procedimentos de credenciamento de segurança e de tratamento de informação classificada.

Parágrafo único. O disposto no **caput** se aplica à pessoa ou entidade privada que, em razão de qualquer vínculo com o Poder Público, execute atividade de credenciamento de segurança ou de tratamento de informação classificada.

Art. 18. O acesso, a divulgação e o tratamento de informação classificada ficarão restritos a pessoas com necessidade de conhecê-la e que sejam credenciadas na forma deste Decreto, sem prejuízo das atribuições dos agentes públicos autorizados na legislação.

Parágrafo único. O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, constante do Anexo I, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei**.**

Art. 19. A decisão de classificação, desclassificação, reclassificação ou redução do prazo de sigilo de informação classificada em qualquer grau de sigilo observará os procedimentos previstos nos arts. 31 e32 do Decreto nº 7.724 de 16 de maio de 2012, e deverá ser formalizada em decisão consubstanciada em Termo de Classificação de Informação.

Art. 20. A publicação de atos normativos relativos a informação classificada em qualquer grau de sigilo ou protegida por sigilo legal ou judicial poderá limitar-se, quando necessário, aos seus respectivos números, datas de expedição e ementas, redigidos de modo a não comprometer o sigilo.

Seção II

Do Documento Controlado

Art. 21. Para o tratamento de documento com informação classificada em qualquer grau de sigilo ou prevista na legislação como sigilosa o órgão ou entidade poderá adotar os seguintes procedimentos adicionais de controle:

I - identificação dos destinatários em protocolo e recibo específicos;

II - lavratura de termo de custódia e registro em protocolo específico;

III - lavratura anual de termo de inventário, pelo órgão ou entidade expedidor e pelo órgão ou entidade receptor; e

IV - lavratura de termo de transferência de custódia ou guarda.

§ 1º O documento previsto no **caput** será denominado Documento Controlado - DC.

§ 2º O termo de inventário previsto no inciso III do **caput** deverá conter no mínimo os seguintes elementos:

I - numeração sequencial e data;

II - órgãos produtor e custodiante do DC;

III - rol de documentos controlados; e

IV - local e assinatura.

§ 3º O termo de transferência previsto no inciso IV do **caput** deverá conter no mínimo os seguintes elementos:

I – numeração sequencial e data;

II - agentes públicos substituto e substituído;

III - identificação dos documentos ou termos de inventário a serem transferidos; e

IV - local e assinatura.

Art. 22. O documento ultrassecreto é considerado DC desde sua classificação ou reclassificação.

Seção III

Da Marcação

Art. 23. A marcação será feita nos cabeçalhos e rodapés das páginas que contiverem informação classificada e nas capas do documento.

§ 1º As páginas serão numeradas seguidamente, devendo cada uma conter indicação do total de páginas que compõe o documento.

§ 2º A marcação deverá ser feita de modo a não prejudicar a compreensão da informação.

Art. 24. O DC possuirá a marcação de que trata o art. 23 e conterá, na capa e em todas as páginas, a expressão em diagonal "Documento Controlado (DC)" e o número de controle, que indicará o agente público custodiante.

Art. 25. A indicação do grau de sigilo em mapas, fotocartas, cartas, fotografias, quaisquer outros tipos de imagens e meios eletrônicos de armazenamento obedecerá aos procedimentos complementares adotados pelos órgãos e entidades.

Seção IV

Da Expedição, Tramitação e Comunicação

Art. 26. A expedição e a tramitação de documentos classificados deverão observar os seguintes procedimentos:

I - serão acondicionados em envelopes duplos;

II - no envelope externo não constará indicação do grau de sigilo ou do teor do documento;

III - no envelope interno constarão o destinatário e o grau de sigilo do documento, de modo a serem identificados logo que removido o envelope externo;

IV - o envelope interno será fechado, lacrado e expedido mediante recibo, que indicará remetente, destinatário e número ou outro indicativo que identifique o documento; e

V - será inscrita a palavra “PESSOAL” no envelope que contiver documento de interesse exclusivo do destinatário.

Art. 27. A expedição, a condução e a entrega de documento com informação classificada em grau de sigilo ultrassecreto serão efetuadas pessoalmente, por agente público autorizado, ou transmitidas por meio eletrônico, desde que sejam usados recursos de criptografia compatíveis com o grau de classificação da informação, vedada sua postagem.

Art. 28. A expedição de documento com informação classificada em grau de sigilo secreto ou reservado será feita pelos meios de comunicação disponíveis, com recursos de criptografia compatíveis com o grau de sigilo ou, se for o caso, por via diplomática, sem prejuízo da entrega pessoal.

Art. 29. Cabe aos responsáveis pelo recebimento do documento com informação classificada em qualquer grau de sigilo, independente do meio e formato:

I - registrar o recebimento do documento;

II - verificar a integridade do meio de recebimento e registrar indícios de violação ou de irregularidade, comunicando ao destinatário, que informará imediatamente ao remetente; e

III - informar ao remetente o recebimento da informação, no prazo mais curto possível.

§ 1º Caso a tramitação ocorra por expediente ou correspondência, o envelope interno somente será aberto pelo destinatário, seu representante autorizado ou autoridade hierarquicamente superior.

§ 2º Envelopes internos contendo a marca “PESSOAL” somente poderão ser abertos pelo destinatário.

Art. 30. A informação classificada em qualquer grau de sigilo será mantida ou arquivada em condições especiais de segurança.

§ 1º Para manutenção e arquivamento de informação classificada no grau de sigilo ultrassecreto e secreto é obrigatório o uso de equipamento, ambiente ou estrutura que ofereça segurança compatível com o grau de sigilo.

§ 2º Para armazenamento em meio eletrônico de documento com informação classificada em qualquer grau de sigilo é obrigatória a utilização de sistemas de tecnologia da informação atualizados de forma a prevenir ameaças de quebra de segurança, observado o disposto no art. 38.

§ 3º As mídias para armazenamento poderão estar integradas a equipamentos conectados à **internet**, desde que por canal seguro e com níveis de controle de acesso adequados ao tratamento da informação classificada, admitindo-se também a conexão a redes de computadores internas, desde que seguras e controladas.

Art. 31. Os meios eletrônicos de armazenamento de informação classificada em qualquer grau de sigilo, inclusive os dispositivos móveis, devem utilizar recursos criptográficos adequados ao grau de sigilo.

Art. 32. Os agentes responsáveis pela guarda ou custódia de documento controlado o transmitirá a seus substitutos, devidamente conferido, quando da passagem ou transferência de responsabilidade.

Parágrafo único. Aplica-se o disposto neste artigo aos responsáveis pela guarda ou custódia de material de acesso restrito.

Seção V

Da Reprodução

Art. 33. A reprodução do todo ou de parte de documento com informação classificada em qualquer grau de sigilo terá o mesmo grau de sigilo do documento.

§ 1º A reprodução total ou parcial de informação classificada em qualquer grau de sigilo condiciona-se à autorização expressa da autoridade classificadora ou autoridade hierarquicamente superior com igual prerrogativa.

§ 2º As cópias serão autenticadas pela autoridade classificadora ou autoridade hierarquicamente superior com igual prerrogativa.

Art. 34. Caso a preparação, impressão ou reprodução de informação classificada em qualquer grau de sigilo for efetuada em tipografia, impressora, oficina gráfica ou similar, essa operação será acompanhada por pessoa oficialmente designada, responsável pela garantia do sigilo durante a confecção do documento.

Seção VI

Da Preservação e da Guarda

Art. 35. A avaliação e a seleção de documento com informação desclassificada, para fins de guarda permanente ou eliminação, observarão o disposto na Lei nº 8.159, de 8 de janeiro de 1991, e no Decreto nº 4.073, de 3 de janeiro de 2002.

Art. 36. O documento de guarda permanente que contiver informação classificada em qualquer grau de sigilo será encaminhado, em caso de desclassificação, ao Arquivo Nacional ou ao arquivo permanente do órgão público, da entidade pública ou da instituição de caráter público, para fins de organização, preservação e acesso.

Art. 37. O documento de guarda permanente não pode ser desfigurado ou destruído, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

Seção VII

Dos Sistemas de Informação

Art. 38. No tratamento da informação classificada deverão ser utilizados sistemas de informação e canais de comunicação seguros que atendam aos padrões mínimos de qualidade e segurança definidos pelo Poder Executivo federal.

§ 1º A transmissão de informação classificada em qualquer grau de sigilo por meio de sistemas de informação deverá ser realizada, no âmbito da rede corporativa, por meio de canal seguro, como forma de mitigar o risco de quebra de segurança.

§ 2º A autenticidade da identidade do usuário da rede deverá ser garantida, no mínimo, pelo uso de certificado digital.

§ 3º Os sistemas de informação de que trata o **caput** deverão ter níveis diversos de controle de acesso e utilizar recursos criptográficos adequados aos graus de sigilo.

§ 4º Os sistemas de informação de que trata o **caput** deverão manter controle e registro dos acessos autorizados e não-autorizados e das transações realizadas por prazo igual ou superior ao de restrição de acesso à informação.

Art. 39. Os equipamentos e sistemas utilizados para a produção de documento com informação classificada em qualquer grau de sigilo deverão estar isolados ou ligados a canais de comunicação seguros, que estejam física ou logicamente isolados de qualquer outro, e que possuam recursos criptográficos e de segurança adequados à sua proteção.

Art. 40. A cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado.

Parágrafo único. Compete ao Gabinete de Segurança Institucional da Presidência da República estabelecer parâmetros e padrões para os recursos criptográficos baseados em algoritmo de Estado, ouvido o Comitê Gestor de Segurança da Informação previsto no art. 6º do Decreto nº 3.505, de 13 de junho de 2000.

Art. 41. Os procedimentos de tratamento de informação classificada em qualquer grau de sigilo aplicam-se aos recursos criptográficos, atendidas as seguintes exigências:

I - realização de vistorias periódicas, com a finalidade de assegurar a execução das operações criptográficas;

II - manutenção de inventários completos e atualizados do material de criptografia existente;

III - designação de sistemas criptográficos adequados a cada destinatário;

IV - comunicação, ao superior hierárquico ou à autoridade competente, de anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de informações criptografadas; e

V - identificação de indícios de violação, de interceptação ou de irregularidades na transmissão ou recebimento de informações criptografadas.

Seção VIII

Das Áreas, Instalações e Materiais

Art. 42. As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade.

Art. 43. Os órgãos e entidades públicas adotarão medidas para definição, demarcação, sinalização, segurança e autorização de acesso às áreas restritas sob sua responsabilidade.

Parágrafo único. As visitas a áreas ou instalações de acesso restrito serão disciplinadas pelo órgão ou entidade responsável pela sua segurança.

Art. 44. Os materiais que, por sua utilização ou finalidade, demandarem proteção, terão acesso restrito às pessoas autorizadas pelo órgão ou entidade.

Art. 45. São considerados materiais de acesso restrito qualquer matéria, produto, substância ou sistema que contenha, utilize ou veicule conhecimento ou informação classificada em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica cuja divulgação implique risco ou dano aos interesses da sociedade e do Estado, tais como:

I - equipamentos, máquinas, modelos, moldes, maquetes, protótipos, artefatos, aparelhos, dispositivos, instrumentos, representações cartográficas, sistemas, suprimentos e manuais de instrução;

II - veículos terrestres, aquaviários e aéreos, suas partes, peças e componentes;

III - armamentos e seus acessórios, as munições e os aparelhos, equipamentos, suprimentos e insumos correlatos;

IV - aparelhos, equipamentos, suprimentos e programas relacionados a tecnologia da informação e comunicações, inclusive à inteligência de sinais e imagens;

V - recursos criptográficos; e

VI - explosivos, líquidos e gases.

Art. 46. Os órgãos ou entidades públicas encarregadas da preparação de planos, pesquisas e trabalhos de aperfeiçoamento ou de elaboração de projeto, prova, produção, aquisição, armazenagem ou emprego de material de acesso restrito expedirão instruções adicionais necessárias à salvaguarda dos assuntos a eles relacionados.

Art. 47. O meio de transporte utilizado para deslocamento de material de acesso restrito é de responsabilidade do custodiante e deverá considerar o grau de sigilo das informações.

§ 1º O material de acesso restrito poderá ser transportado por empresas contratadas, adotadas as medidas necessárias à manutenção do sigilo das informações.

§ 2º As medidas necessárias para a segurança do material transportado serão prévia e explicitamente estabelecidas em contrato.

Seção IX

Da Celebração de Contratos Sigilosos

Art. 48. A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto contenha informação classificada em qualquer grau de sigilo, ou cuja execução envolva informação classificada, é condicionada à assinatura de TCMS e ao estabelecimento de cláusulas contratuais que prevejam os seguintes requisitos:

I - obrigação de manter sigilo relativo ao objeto e a sua execução;

II - possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;

III - obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;

IV - identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso a informação classificada em qualquer grau de sigilo e material de acesso restrito;

V - obrigação de receber inspeções para habilitação de segurança e sua manutenção; e

VI - responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.

Art. 49. Aos órgãos e entidades públicas com que os contratantes mantêm vínculo de qualquer natureza caberá adotar procedimentos de segurança da informação classificada em qualquer grau de sigilo ou do material de acesso restrito em poder dos contratados ou subcontratados.

CAPÍTULO IV

DA INDEXAÇÃO DE DOCUMENTO COM INFORMAÇÃO CLASSIFICADA

Art. 50. A informação classificada em qualquer grau de sigilo ou o documento que a contenha receberá o Código de Indexação de Documento que contém Informação Classificada - CIDIC.

Parágrafo único. O CIDIC será composto por elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada, e será estruturado em duas partes.

Art. 51. A primeira parte do CIDIC será composta pelo Número Único de Protocolo -NUP, originalmente cadastrado conforme legislação de gestão documental.

§ 1º A informação classificada em qualquer grau de sigilo ou o documento que a contenha, quando de sua desclassificação, manterá apenas o NUP.

§ 2º Não serão usadas tabelas de classificação de assunto ou de natureza do documento, em razão de exigência de restrição temporária de acesso à informação classificada em qualquer grau de sigilo, sob pena de pôr em risco sua proteção e confidencialidade.

Art. 52. A segunda parte do CIDIC será composta dos seguintes elementos:

I - grau de sigilo: indicação do grau de sigilo, ultrassecreto (U), secreto (S) ou reservado (R), com as iniciais na cor vermelha, quando possível;

II - categorias: indicação, com dois dígitos, da categoria relativa, exclusivamente, ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), conforme Anexo II;

III - data de produção da informação classificada: registro da data de produção da informação classificada, de acordo com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);

IV - data de desclassificação da informação classificada em qualquer grau de sigilo: registro da potencial data de desclassificação da informação classificada, efetuado no ato da classificação, de acordo com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);

V - indicação de reclassificação: indicação de ocorrência ou não, S (sim) ou N (não), de reclassificação da informação classificada, respectivamente, conforme as seguintes situações:

a) reclassificação da informação resultante de reavaliação; ou

b) primeiro registro da classificação; e

VI - indicação da data de prorrogação da manutenção da classificação: indicação, exclusivamente, para informação classificada no grau de sigilo ultrassecreto, de acordo com a seguinte

composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos), na cor vermelha, quando possível.

Art. 53. Para fins de gestão documental, deverá ser guardado o histórico das alterações do CIDIC.

CAPÍTULO V

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 54. A implementação do CIDIC deverá ser consolidada até 1º de junho de 2013.

Parágrafo único. Enquanto não implementado o CIDIC, o Termo de Classificação de Informação será preenchido com o NUP.

Art. 55. O documento com informação classificada em qualquer grau de sigilo, produzido antes da vigência da Lei nº 12.527, de 2011, receberá o CIDIC para fins do disposto no art. 45 do Decreto nº 7.724, de 16 de maio de 2012.

Art. 56. Os órgãos e entidades deverão adotar os recursos criptográficos baseados em algoritmo de Estado no prazo de um ano a contar da definição dos parâmetros e padrões de que trata o parágrafo único do art. 40.

Parágrafo único. Até o término do prazo previsto no **caput,** compete ao Gabinete de Segurança Institucional da Presidência da República acompanhar e prestar apoio técnico aos órgãos e entidades quanto à implementação dos recursos criptográficos baseados em algoritmo de Estado.

Art. 57. Os órgãos e entidades poderão expedir instruções complementares, no âmbito de suas competências, que detalharão os procedimentos relativos ao credenciamento de segurança e ao tratamento de informação classificada em qualquer grau de sigilo.

Art. 58. O Regimento Interno da Comissão Mista de Reavaliação da Informação detalhará os procedimentos de segurança necessários para a salvaguarda de informação classificada em qualquer grau de sigilo durante os seus trabalhos e os de sua Secretaria-Executiva, observado o disposto neste Decreto.

Art. 59. Este Decreto entra em vigor na data de sua publicação.

Art. 60. Ficam revogados:

I - o Decreto nº 4.553, de 27 de dezembro de 2002; e

II - o Decreto nº 5.301, de 9 de dezembro de 2004.

Brasília, 14 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF

Márcia Pelegrini
Celso Luiz Nunes Amorim
Miriam Belchior
Marco Antonio Raupp
José Elito Carvalho Siqueira
Luís Inácio Lucena Adams
Jorge Hage Sobrinho

ANEXO I

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO - TCMS

[Qualificação: nome, nacionalidade, CPF, identidade (nº, data e local de expedição), filiação e endereço], perante o(a) [órgão ou entidade], declaro ter ciência inequívoca da legislação sobre o tratamento de informação classificada cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, e me comprometo a guardar o sigilo necessário, nos termos da Lei nº 12.527, de 18 de novembro de 2011, e a:

a) tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo(a) [órgão ou entidade] e preservar o seu sigilo, de acordo com a legislação vigente;

b) preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo a terceiros;

c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e

d) não copiar ou reproduzir, por qualquer meio ou modo: (i) informações classificadas em qualquer grau de sigilo; (ii) informações relativas aos materiais de acesso restrito do (da) [órgão ou entidade], salvo autorização da autoridade competente.

Declaro que [recebi] [tive acesso] ao (à) [documento ou material entregue ou exibido ao signatário], e por estar de acordo com o presente Termo, o assino na presença das testemunhas abaixo identificadas.

[Local, data e assinatura]

[Duas testemunhas identificadas]

ANEXO II

CÓDIGO DE INDEXAÇÃO DE DOCUMENTO

QUE CONTÉM INFORMAÇÃO CLASSIFICADA - CIDIC - CATEGORIAS

CATEGORIAS	CÓDIGO NUMÉRICO
Agricultura, extrativismo e pesca	01
Ciência, Informação e Comunicação	02
Comércio, Serviços e Turismo	03
Cultura, Lazer e Esporte	04
Defesa e Segurança	05
Economia e Finanças	06
Educação	07
Governo e Política	08
Habitação, Saneamento e Urbanismo	09
Indústria	10
Justiça e Legislação	11
Meio ambiente	12
Pessoa, família e sociedade	13
Relações internacionais	14
Saúde	15
Trabalho	16
Transportes e trânsito	17

Obs.:

1. Categorias: representam os aspectos ou temas correlacionados à informação classificada em grau de sigilo, e serão indicadas pela Autoridade Classificadora. Para tanto deverá ser usado, exclusivamente, o primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), definidos no Padrão de Interoperabilidade do Governo Eletrônico (e-Ping), conforme quadro acima.

2. Composição no CIDIC: 2 dígitos = código numérico