**UNIVERSIDADE FEDERAL FLUMINENSE**
**MARCIO AFFONSO RODRIGUES**

# SEGURANÇA DA INFORMAÇÃO EM EMPRESAS

**Niterói**
**2016**

**MARCIO AFFONSO RODRIGUES**

# SEGURANÇA DA INFORMAÇÃO EM EMPRESAS

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

**Orientadora:**
**Helga D. Balbi**

**NITERÓI**
**2016**

**Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF**

R696 Rodrigues, Marcio Affonso
Segurança da informação em empresas / Marcio Affonso Rodrigues. – Niterói, RJ : [s.n.], 2016.
70 f.

Projeto Final (Tecnólogo em Sistemas de Computação) – Universidade Federal Fluminense, 2016.
Orientador: Helga D. Balbi.

1. Segurança da informação. 2. Sistema de computador. I. Título.

CDD 005.8

**MARCIO AFFONSO RODRIGUES**

# SEGURANÇA DA INFORMAÇÃO EM EMPRESAS

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Niterói, ___ de _____ de **2016**.

Banca Examinadora:

_____

Profª. Helga Dolorico Balbi, Msc. – **Orientadora**

UFF - Universidade Federal Fluminense

_____

Prof. Leandro Soares de Sousa, Dsc. – **Avaliador**

UFF - Universidade Federal Fluminense

Dedico este trabalho a minha esposa e a minha estimada filha.

# AGRADECIMENTOS

A Deus, que sempre iluminou a minha caminhada.

Aos meus pais Daniel Cerqueira Rodrigues e Miriam Carvalheira Affonso Rodrigues, que se esforçaram ao longo de suas vidas para proverem minha formação intelectual e de caráter.

As minhas queridas esposa Elaine de Cassia Dantas Rodrigues e filha Júlia Dantas Rodrigues, que me apoiaram e compreenderam meu pouco tempo disponível durante os estudos.

A minha orientadora Helga Dolorico Balbi, pelo estímulo e atenção que me concedeu durante o curso.

Aos Colegas de curso, pelo incentivo e troca de experiências.

**“**O último esforço da razão é reconhecer que existe uma infinidade de coisas que a ultra-passam**”.**

Blaise Pascal

# RESUMO

Atualmente, como fonte de poder, a informação é o bem mais valioso e cobiçado da humanidade. O acesso a ela faz a diferença entre os homens, empresas, estados e governos, merecendo, portanto, um tratamento especial. Nessa busca por vantagens competitivas, muitas empresas e indivíduos tentam obter informações com propósitos escusos. Várias empresas e pessoas já foram vítimas deste tipo de espionagem maliciosa. Tendo isto em vista, é comum a utilização de mecanismos para evitar o roubo de informação. Este estudo procurará descrever as melhores técnicas utilizadas por grandes empresas na tentativa de garantir a segurança de suas informações.

**Palavras-chaves: informação, poder, técnica e segurança.**

# ABSTRACT

Currently, as source of power, the information is the most valuable and coveted property of humanity. Owning it makes difference between men, companies, states and governments, deserving, therefore, a special treatment. In search of competitive advantages, lot of companies and people try to obtain information with bad purposes. Many companies and people had been victims of this kind of malicious espionage. This study intends to describe the best techniques used for big companies trying to guarantee their information safety.



**Key words: information, power, technique and safety.**

# LISTA DE ILUSTRAÇÕES

# LISTA DE TABELAS

# LISTA DE GRÁFICOS

# LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

BS – *British Standart* (Norma Britânica)

CC – *Common Criteria* (Critério Comum)

*CCSC – Comercial Computer Security Centre* (Centro Comercial de Segurança Computacional)

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CETIC.br – Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação

CGI.br – Comitê Gestor da Internet no Brasil

CPU – *Central Process Unit* (Unidade Central de Processamento)

CSIRT – *Computer Secutity Response Team* (Grupo de Resposta a Incidente de Segurança em Computadores)

CTCPEC – Canadian Trusted Computer Product Evaluation Criteria (Critério Canadense de Avaliação de Confiança de Produtos de Computador)

IC – Infraestrutura Crítica

DEC – *Digital Equipment Corporation* (Corporação Equipamento Digital)

DoS – *Denial of Service* (Negação de Serviço)

eMAG – Modelo de Acessibilidade em Governo Eletrônico

ePING – Padrões de Interoperabilidade de Governo Eletrônico

ENIAC – *Electronic Numerical Integrator and Computer* (Computador e Integrador Numérico eletrônico)

IEC – *International Electrotechnical Commission* (Comissão Internacional de Eletrotécnica)

INDA – Infraestrutura Nacional de Dados Abertos

ISO – *International Organization for Standardization* (Organização Internacional para Padronização)

ITSEC – *Information Technology Security Evaluation Criteria* (Critério de Avaliação de Segurança da Tecnologia de Informação)

MPOG – Ministério do Planejamento, Orçamento e Gestão

NIC.br – Núcleo de Informação e Coordenação do Ponto BR

NBS – *National Bureau of Standards* (Agência Nacional de Padrões)

PDP – *Programmed Data Processor* (Processador de Dados Programado)

SGSI – Sistema de Gestão da Segurança da Informação

SI – Segurança da Informação

SISG – Sistema de Administração de Serviços Gerais

SISP – Sistema de Administração dos Recursos de Tecnologia da Informação

SLTI – Secretaria de Logística e Tecnologia da Informação

TCSEC – *Trusted Computer System Evaluation Criteria* (Critério de Avaliação de Confiança em Sistema Computacional)

TIC – Tecnologias da Informação e Comunicação

# SUMÁRIO

# 1 INTRODUÇÃO

A informação é tão importante e fundamental que, desde que começou a ser registrada através da escrita, modificou a história da humanidade, e o período antecessor à sua invenção ficou sendo conhecido como “pré-história”. Neste período, as informações eram transmitidas boca a boca ou por desenhos, permitindo enorme margem para equívocos de interpretação.

Nos últimos anos, assistimos ao desenvolvimento da internet com uma quantidade estrondosa de informação invadindo as telas de nossos computadores, *smartphones* e *tablets*. A facilidade de acesso aos equipamentos também aumentou vertiginosamente e muitas crianças que sequer aprenderam a ler já os possuem.

Processos automatizados e de controles à distância também evoluíram bastante, sendo cada vez mais utilizados para diminuir a burocracia, otimizar custos e garantir a qualidade. Tais informações quase sempre necessitam disponibilização em tempo real e, o que outrora era isolado, passou a estar interligado ao ambiente corporativo das empresas que lançam de sistemas de comunicação sofisticados para transpor ambientes hostis, interferências eletromagnéticas, espectro largo de informação trocada, etc.

Dada a importância das informações tratadas nas empresas, torna-se importante a utilização de técnicas que garantam a confidencialidade, integridade e disponibilidade das mesmas para corroborar o sistema financeiro e a missão empresarial.

Tendo em vista a grande importância do tema, este trabalho fará um estudo sobre a segurança da informação procurando descrever as melhores técnicas utilizadas por grandes empresas na tentativa de garantir que suas informações estejam seguras. O restante do trabalho está organizado da seguinte forma:

- o Capítulo 2 fará uma descrição de alguns eventos de falhas de segurança documentados, mostrando a importância do tema nos dias atuais;

- o terceiro capítulo abordará os desafios da segurança da informação, falando da disponibilidade, confidencialidade e integridade dos sistemas;
- o quarto capítulo é dedicado a identificar as maiores ameaças e vulnerabilidades das redes de dados (físicas e eletrônicas);
- o quinto capítulo apresentará o desenvolvimento das normas de segurança da informação já existentes sobre o assunto; e
- finalmente, no Capítulo 6, serão apresentadas as conclusões do trabalho e propostas para estudos futuros relacionando-os ao tema.

# 2 EVENTOS DE FALHA DE SEGURANÇA DOCUMENTADOS

A Segurança da Informação abrange diversas áreas, como: infraestrutura tecnológica, segurança física e cultura organizacional, cada uma com suas vulnerabilidades, controles e soluções de segurança aplicáveis para minimizar o nível de exposição das empresas, no intuito de preservar o patrimônio cada vez mais valioso: a informação.

> A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos[1]

Para manutenção da operação da empresa, faz-se necessário que ativos físicos, tecnológicos e humanos façam uso de informações. Esses momentos caracterizam o ciclo de vida da informação e correspondem a situações em que a informação é exposta e vulnerável, seja digitalmente ou fisicamente.

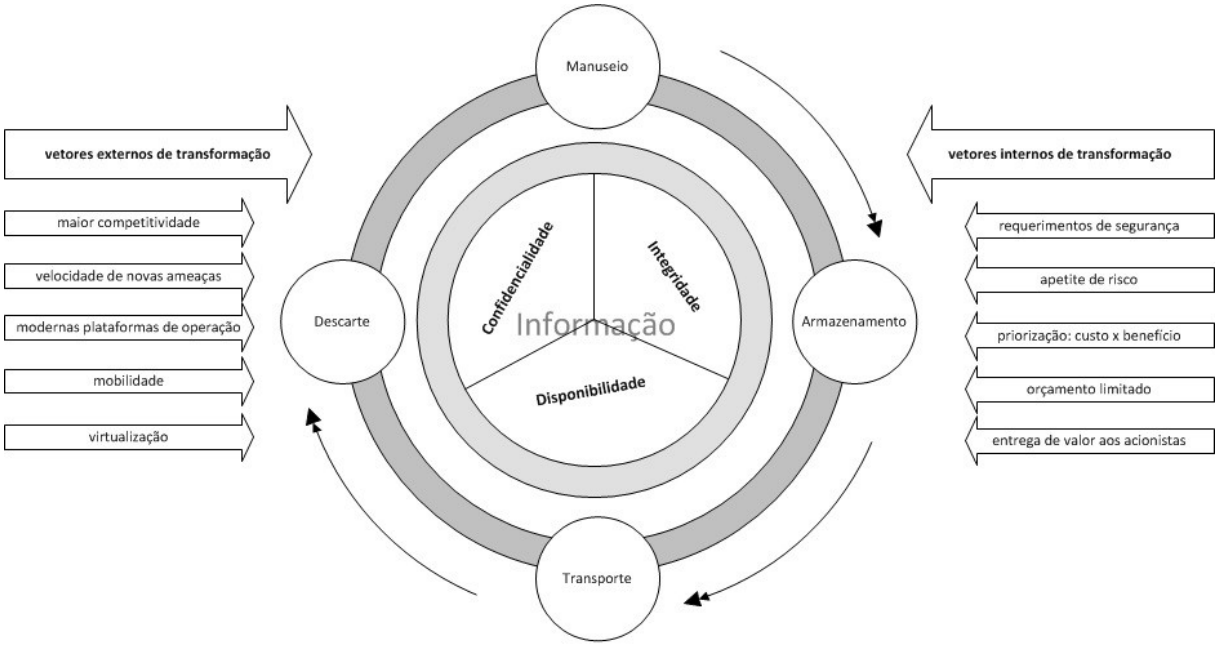
Conforme mostra a Figura Figura 1, destacam-se quatro momentos do ciclo de vida da informação:

- **Manuseio**: momentos em que a informação é criada, consultada ou modificada;
- **Armazenamento**: refere-se ao momento em que a informação é guardada para uso futuro;
- **Transporte**: momento em que a informação é movida/distribuída para outras posições de acesso ou armazenamento;
- **Descarte**: momento em que a informação perde a utilidade e é destruída.

Em uma rede de dados, inevitavelmente existirá um fluxo de informações que trafegarão e serão compartilhadas com usuários. Tal compartilhamento efetuado de forma segura e somente com pessoas autorizadas, corresponde a um conceito básico de segurança chamado confidencialidade.

Uma informação verdadeira fraudada ou a criação de uma falsa pode causar muitos danos às empresas. A criação de controles contra fraudes garantem a integridade da informação que é outro conceito básico de segurança.

A capacidade de acessar as informações no momento em que estas são necessárias caracteriza o conceito de disponibilidade. Uma transação legítima não efetuada pode causar um prejuízo enorme às empresas, muitas vezes superior a um furto de informações.




*"a segurança da informação sempre foi um jogo de risco que requer estratégia inteligente, tecnologia apropriada e atenção aos adversários. Hoje, porém, o jogo em si e os oponentes estão mudados. Para vencer, as empresas devem jogar sob novas regras, recorrer a competências técnicas diferenciadas e adotar estratégias sofisticadas."*

Figura 1: Ciclo de Vida da Informação.

[2]

Este capítulo apresenta quatro eventos de incidentes de segurança da informação. Os incidentes ocorridos serão descritos para demonstrar que o poderio das informações *hackeadas* podem trazer cada vez mais danos às empresas e pessoas, e as consequências podem ser realmente catastróficas.

## 2.1 EXEMPLO DE INCIDENTE n° 1: EMPRESA TEM SISTEMA INVADIDO E BLOQUEADO POR *HACKERS*

Em agosto de 2015, o sistema de computadores de uma empresa de Marília (SP) foi invadido por *hackers* que bloquearam o sistema e deixaram uma mensagem exigindo pagamento de uma taxa para restauração do mesmo.

Chegando ao local de trabalho, o empresário, encontrou as telas dos computadores pretas com a seguinte mensagem em inglês: “Se quiser reaver o sistema envie um *e-mail* com o código 734960800.”[3].

A vítima contatou o *e-mail* informado e recebeu outra mensagem onde os *hackers* exigiam o pagamento de três mil dólares para recuperar o sistema. O valor não foi pago, a empresa acionou a polícia e recuperou o sistema através de *backup,* documentos impressos e muito trabalho.

Um caso semelhante ocorreu na prefeitura de Pratânia (SP) no dia anterior e mais dois casos com duas empresas de Marília e Vera Cruz (SP).

Esse tipo de invasão representa uma falha na confidencialidade e disponibilidade do sistema de informação. A empresa em questão teve uma grande mão de obra para recuperar os dados “sequestrados” e só conseguiu fazê-lo por ter alguma forma de *backup*. O prejuízo financeiro foi pequeno e compatível com o tamanho do negócio.

No caso da prefeitura, ou evento semelhante em uma empresa de grande porte, o impacto é bem mais grave, pela possibilidade de afetar muitas outras pessoas indiretamente, seja pela exposição de dados pessoais, pelo atraso na concretização de contratos de grande monta, interrupção das prestações de serviços, etc.

## 2.2 EXEMPLO DE INCIDENTE N° 2: FURTO DE COMPUTADORES DA PETROBRAS

Em fevereiro de 2008, foi amplamente divulgado pela mídia o anúncio de que a estatal brasileira Petrobras havia sido vítima de espionagem industrial, por ter tido *notebooks* e *Hds* com informações estratégicas de reservatórios de petróleo roubados.

Segundo a própria Petrobras, dentre as informações roubadas, existiam dados sigilosos sobre o recém-anunciado campo de Tupi, na região pré-sal, com reserva estimada entre cinco a oito bilhões de barris de petróleo.

> Esse tipo de espionagem é bastante comum e, agora que as reservas do Brasil começaram a ficar importantes, isso deve se popularizar por aqui também…
> … fora do país, é comum revistas especializadas trazerem ofertas de dados geológicos não oficiais sobre áreas potenciais de petróleo. Esses relatórios custam no mercado entre US$ 100 mil e US$ 1 milhão[4].

As investigações da Polícia Federal, constataram que os aparelhos foram roubados durante o transporte dos equipamentos em *contêiner* de empresa terceirizada prestadora de serviços.

Ficou comprovado que o sistema de segurança adotado para o transporte dos equipamentos com informações estratégicas era extremamente falho porque várias pessoas tinham acesso aos mesmos indiscriminadamente.

A conclusão da investigação garantiu que o furto foi crime comum e não espionagem industrial. A Polícia Federal culpou vigilantes que trabalhavam no terminal portuário e já vinham praticando pequenos furtos que não foram percebidos pela estatal.

Alguns dos equipamentos foram encontrados ainda com os vigilantes; outros foram vendidos por mil e quinhentos reais e outros foram destruídos. Os ladrões sequer tinham conhecimento das informações que haviam furtado.

> ... independentemente da motivação do crime, as investigações revestem-se de importância, em função da possível fragilidade do sistema de segurança para o transporte de informações reservadas, que o episódio evidenciou[5].

Houve uma grande repercussão do caso na imprensa devido a enorme importância política, econômica e estratégica, após recente anúncio de que as reservas do pré-sal tornariam o país uma superpotência do setor petrolífero.

A situação justificaria um investimento pesado em tecnologia para garantir a segurança das informações na empresa. Quando foi apurado que o roubo foi comum e não espionagem industrial, a imagem da empresa ficou bastante afetada por ter evidenciado um certo desleixo com informações extremamente importantes.

Qualquer aparato tecnológico que a empresa possuísse protegendo à rede de dados seria ineficaz frente a fragilidade imposta pelo desleixado transporte e armazenamento da informação, deixando claro que além das tecnologias aplicáveis, os procedimentos humanos são também essenciais para a segurança.

## 2.3 EXEMPLO DE INCIDENTE N° 3: EXPOSIÇÃO DE DADOS DAS ESTAÇÕES DE TRATAMENTO DE ÁGUA DOS ESTADOS UNIDOS

Em novembro de 2011, na cidade de Ilinóis, ocorreu um evento de quebra de uma bomba de água tratada, que abastecia vários lares americanos, tendo sido especulado como um ataque *hacker.*

As autoridades fizeram um pronunciamento alegando que não havia nenhuma informação confiável que indicasse risco à infraestrutura crítica ou ameaça à segurança pública.

Em resposta ao pronunciamento, um *hacker* intitulado “Pr0f” afirmou ter acesso ao sistema de controle de outra estação de tratamento, esta localizada em Houston.

Para provar o acesso, ele publicou um documento contendo fotos das telas do sistema interno de controle em um *website* chamado Pastebin.

Se o acesso às fotos foi pela internet ou por outros métodos não foi informado pelas autoridades, mas o fato acendeu um alerta de que tais casos devem ser

melhor estudados. “Se cada incidente for visto de forma isolada, será difícil – se não impossível – discernir um padrão ou juntar os pontos.”[6].

O evento descrito chama bastante atenção pelo potencial de risco envolvido, quando sistemas de controle e automação são interligados à internet. A suposta invasão ao sistema representa um risco em Infraestrutura Crítica.

> As Infraestruturas Críticas (IC) - instalações, serviços, bens e sistemas – exercem significativa influência na vida de qualquer pessoa e na operação de setores importantes para o desenvolvimento e manutenção do país, como é o caso do setor industrial. Elas são importantes pelas facilidades e utilidades que fornecem à sociedade e, principalmente, por subsidiarem, na forma de recurso ou serviço, outras Infraestruturas Críticas, mais complexas ou não. Ao passar dos anos, as interdependências verticais das Infraestruturas Críticas, caracterizadas por um baixo acoplamento entre elas, deu lugar às interdependências horizontais altamente acopladas, com muitos pontos de interação em suas dimensões[7].

É inadmissível que um ***hacker*** possa interferir em operações de IC e justificam-se maciços investimentos em tecnologia e procedimentos que impeçam esse tipo de ação para que as sociedades não tornem-se reféns de sistemas comprometidos.

## 2.4 EXEMPLO DE INCIDENTE N° 4: ESPIONAGEM DOS ESTADOS UNIDOS DA AMÉRICA AO BRASIL

Em 2013, um ex-prestador de serviços da *NSA* (Agência Nacional de Segurança dos EUA) chamado Edward Snowden apresentou documentos que revelaram que os EUA monitoravam atividades de outros países e seus líderes.

Conforme as informações de Snowden, a *NSA* possui programas para capturar tudo que o usuário faz na internet, incluindo o conteúdo de *e-mails* e *sites* visitados.

No Brasil, a espionagem norte-americana atingiu as comunicações da presidente Dilma com seus principais assessores, a Petrobras, o Ministério das Minas e Energia, entre outras.

Tal revelação, gerou uma crise diplomática entre Brasil e Estados Unidos, levando ao cancelamento, à época, de uma visita de Estado agendada para Washington.

Indignada, a presidente brasileira condenou duramente as ações de espionagem dos Estados Unidos na Assembleia Geral das Nações Unidas em Nova York.

> “Recentes revelações sobre as atividades de uma rede global de espionagem eletrônica provocaram indignação e repúdio em amplos setores da opinião pública mundial.
> No Brasil, a situação foi ainda mais grave, pois aparecemos como alvo dessa intrusão. Dados pessoais de cidadãos foram indiscriminadamente objeto de interceptação. Informações empresariais – muitas vezes, de alto valor econômico e mesmo estratégico – estiveram na mira da espionagem. Também representações diplomáticas brasileiras, entre elas a Missão Permanente junto às Nações Unidas e a própria Presidência da República tiveram suas comunicações interceptadas.
> Imiscuir-se dessa forma na vida de outros países fere o Direito Internacional e afronta os princípios que devem reger as relações entre eles, sobretudo, entre nações amigas. Jamais pode uma soberania firmar-se em detrimento de outra soberania. Jamais pode o direito à segurança dos cidadãos de um país ser garantido mediante a violação de direitos humanos e civis fundamentais dos cidadãos de outro país…
>
> …O problema, porém, transcende o relacionamento bilateral de dois países. Afeta a própria comunidade internacional e dela exige resposta. As tecnologias de telecomunicação e informação não podem ser o novo campo de batalha entre os Estados. Este é o momento de criarmos as condições para evitar que o espaço cibernético seja instrumentalizado como arma de guerra, por meio da espionagem, da sabotagem, dos ataques contra sistemas e infraestrutura de outros países.
> A ONU deve desempenhar um papel de liderança no esforço de regular o comportamento dos Estados frente a essas tecnologias e a importância da internet, dessa rede social, para construção da democracia no mundo[8].

Nesse evento, é apresentado um cenário caótico, onde o conceito de confidencialidade é descaracterizado e um país espiona qualquer informação que líderes de outro país trafegam na internet.

A crise diplomática gerada poderia facilmente ter evoluído para uma guerra caso as circunstâncias político-econômicas fossem diferentes.

## 2.5 CONCLUSÃO

Como demonstrado nos eventos, a segurança da informação é interesse de toda a sociedade e deve estar cada vez mais presente, tanto quanto a evolução tecnológica.

A humanidade conseguiu uma evolução extraordinária com os avanços tecnológicos, sobretudo com a comunicação em tempo real, principalmente através da internet.

É essencial desenvolver garantias de segurança nesse novo horizonte para que esta fantástica ferramenta seja instrumento de transformação evolutiva. Ignorar a sua potencialidade destruidora pode ser catastrófico.

# 3 DESAFIOS DA SEGURANÇA DA INFORMAÇÃO

O grande objetivo da segurança da informação é proteger a informação. Ocorre que, muitas vezes, as empresas perdem o foco nos ativos tecnológicos pelos quais a informação passa ou onde é armazenada.

Proteger a informação significa prover confidencialidade, integridade e disponibilidade que são conceitos básicos fundamentais da segurança da informação e garanti-los são os principais desafios.

> Confidencial
> [De *confidência* + *-al*[1].]
> Adjetivo de dois gêneros.
> 1. Dito ou escrito em confidência; secreto.
> Substantivo feminino.
> 2. Comunicação ou ordem sob sigilo[9].

Confidencialidade é um substantivo oriundo da palavra confidencial para expressar a ideia de situação confidencial. Seu conceito está relacionado a secreto e sigilo e, na realidade, é o aspecto mais estratégico para as empresas porque protege o capital intelectual e, consequentemente, possibilita vantagens competitivas.

O capital intelectual das empresas é a transformação dos conhecimentos do negócio nas dimensões tecnológicas, processuais e pessoais obtidos pelos funcionários ao longo de suas atividades laborais, propiciando desenvolvimento e destaque às organizações.

Dependendo da complexidade das empresas serão necessários vultuosos investimentos e tempo para atingir resultados de excelência que garantam o destaque necessário ao empreendimento.

A possibilidade de permitir que qualquer concorrente adquira esse "*know-how"* construído através de tanto dispêndio de recursos, para depois perder a vantagem competitiva, justifica um forte investimento para preservação da confidencialidade.

> Integridade
> [Do lat. *integritate*.]

> Substantivo feminino.
> 1. Qualidade de íntegro; inteireza.
> 2. Fig. Retidão, imparcialidade.
> 3. Fig. Inocência, pureza, castidade[9].

Integridade refere-se ao que está inteiro, puro, correto. Todas as empresas e pessoas trocam informações todo o tempo e, para que haja uma comunicação efetiva, é necessário que o receptor interprete e compreenda a mensagem enviada pelo emissor.

> A comunicação eficaz necessita que o conteúdo transmitido seja recebido e entendido por alguém da maneira que era pretendido. Os objetivos da comunicação eficaz incluem a criação de uma percepção comum, mudança de comportamentos e aquisição de informação[10].

Sob esse ponto de vista, percebe-se que a integridade é um conceito extremamente essencial, porque não é fácil atingir essa eficiência com informações íntegras, mas torna-se um processo muito lento, trabalhoso e até impossível quando as mesmas são corrompidas no caminho entre emissor e receptor.

Informação sem integridade pressupõe incertezas, descontinuidades, retrabalho, lentidão e desperdício de recursos que propiciarão prejuízos as empresas.

> Disponibilidade
> [De *disponível* + *-(i)dade*, seg. o padrão erudito.]
> Substantivo feminino.
> 1. Qualidade ou estado do que é disponível.
> 2. Estado de espírito caracterizado pela predisposição a aceitar as solicitações do mundo exterior.
> 5. Qualidade dos valores e títulos integrantes do ativo dum comerciante, que podem ser prontamente convertidos em numerário[9].

Disponibilidade refere-se ao que está disponível, que pode ser utilizado sempre que for necessário. Muitos empreendimentos empresariais dependem da busca ou chegada de uma informação para acontecerem. Se a informação estiver indisponível, o empreendimento poderá ser inviabilizado e consequentemente gerar prejuízos para as empresas.

Em resumo, as empresas precisam prover confidencialidade da informação para não perderem vantagens competitivas, integridade para não perderem lucratividade com desperdício de recursos, e disponibilidade para não perderem a capacidade de operar.

Também é preciso considerar que relacionar segurança da informação apenas à área de informática é um erro pois, na realidade, todos os setores das empresas devem valorizar e proteger este valioso ativo.

As pessoas desempenham um papel fundamental e, por isso, devem ser educadas e capacitadas para a obtenção de um ambiente de compartilhamento seguro das informações.

Investimentos milionários em equipamentos e tecnologia não terão valia se as pessoas simplesmente não protegerem suas chaves de acesso e senhas. Muitos projetos que visam a segurança das informações falham por menosprezarem ou por não considerarem a participação das pessoas como um ponto fundamental. Por isso, investir em educação e treinamento em segurança da informação é fundamental.

Identificar as maiores ameaças e vulnerabilidades das redes de dados é primordial para desenvolver critérios mitigadores de incidentes e será o assunto do próximo capítulo.

# 4 MAIORES AMEAÇAS E VULNERABILIDADES DAS REDES DE DADOS

Ameaça refere-se a qualquer fator, ação ou evento físico, tecnológico ou humano que represente um risco à integridade, disponibilidade e confidencialidade da informação. As ameaças podem ser caracterizadas de várias formas: quanto ao tipo, quanto ao grau de risco, entre outras.

Vulnerabilidade é uma falha ou fraqueza do sistema que pode ser explorada propositalmente ou acidentalmente por um agente interno ou externo, ou seja, é uma incapacidade do sistema em proteger-se de ameaças.

Sabotagem, vandalismo, enchentes, terremotos, incêndios e explosões são exemplos de ameaças à segurança. A integração dos sistemas à Internet acrescenta novas possibilidades de exposição das informações. Além da preocupação com as ameaças citadas, as empresas desbravam um novo horizonte com *hackers*, vírus e invasões.

Ameaças e vulnerabilidades não eliminadas podem levar à ocorrência de um incidente. Por exemplo, o uso de senhas simples é uma ameaça à Segurança da Informação, pois algum indivíduo mal intencionado poderá deduzir estas senhas e obter acesso a informações sensíveis, gerando um incidente de segurança.

> Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas[11].

Conforme o pensamento do General Sun Tzu, é possível entender que o primeiro passo para que as empresas obtenham sucesso nessa “batalha” pela segurança das informações é o conhecimento do seu negócio e seus reais problemas tecnológicos, processuais ou pessoais, capazes de afetar e/ou fragilizar a organização.

As empresas precisam preparar-se para reagir e analisar o comportamento de adversários de tal maneira que se tornem capazes de melhor se posicionarem e destinarem investimentos de forma inteligente em prevenção e detecção.

> Uma ameaça, consiste em uma possível violação de um sistema computacional, que pode ser acidental ou intencional. Uma ameaça acidental é aquela que não foi planejada, podendo ser, por exemplo, uma falha no *hardware* ou no *software*. Já uma ameaça intencional está associada à intencionalidade premeditada. Podendo ser desde um monitoramento não autorizado do sistema até ataques sofisticados, como os realizados por *Hackers*. Estes ocorrem por vários motivos. Variam desde a pura curiosidade, interesse em adquirir maior conhecimento sobre os sistemas, intenção em conseguir ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial ou venda de informações confidenciais. Outro tipo de interesse é o de ferir a imagem de um governo ou uma determinada empresa ou serviço, e quando isso acontece, a notícia da invasão é proporcional à fama de quem a sofreu e normalmente representa um desastre em termos de repercussão pública[12].

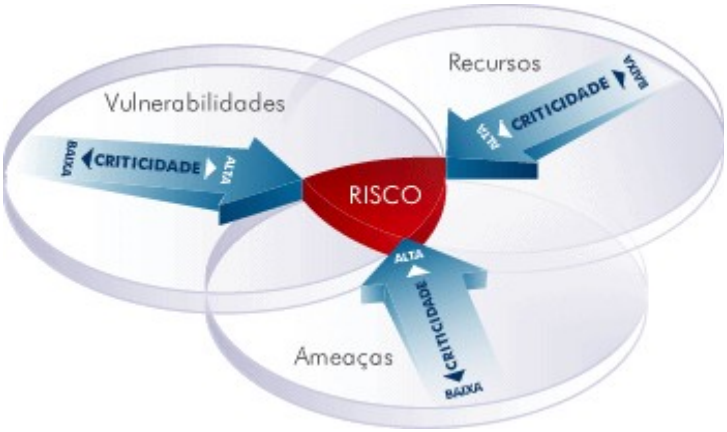



Figura 2: Recursos, Ameaças, Vulnerabilidades e Risco.

[13]

Na Figura 2, uma ilustração que retrata o aumento dos riscos de uma empresa dadas a criticidade das ameaças e vulnerabilidades é apresentada. Mais detalhes sobre estas ameaças e vulnerabilidades estão apresentadas no “ANEXO A - EXEMPLOS DE VULNERABILIDADES E AMEAÇAS”, cujos alguns elementos referentes à preservação dos dispositivos serão destacados a seguir. Estes elementos devem ter prioridade quando se pensa em segurança da informação dentro das empresas, uma vez que os dispositivos devem ser preservados buscando a conservação de dados e demais elementos. A preservação é uma prática importante, já que seus benefícios são imensuráveis para a empresa e a mesma deve preservar seu patrimônio em toda a sua abrangência.

- ***HARDWARE***

No que diz respeito aos *hardwares* pode-se destacar que a ausência de manutenção e de cuidados com os elementos escolhidos para se realizar as atividades cotidianas podem comprometer e trazer problemas significativos não apenas para os usuários, mas também para a organização como um todo. Em determinados casos, ocorre a opção por aparelhos que sejam de menor custo e que, assim, tragam o mesmo resultado que elementos de maior valor pudessem acarretar para os seus usuários. Entretanto, o gasto será superior caso algo dê errado e seja necessário acionar assistências técnicas especializadas que, talvez, possam não se encontrar próximo da instituição e haver a necessidade de um período de espera mais prolongado. Estes inconvenientes, consequentemente, prejudicarão o andamento das atividades da instituição e, assim, poderão acarretar prejuízos para os órgãos que a utilizam.

Enfim, a escolha de um elemento que seja um pouco mais caro, porém que tenha assistência técnica consideravelmente mais próxima e que possua uma qualidade superior daquele *hardware* que seria mais “em conta” traz benefícios bem consideráveis e, por sua vez, evitam gastos desnecessários que comprometeriam a lucratividade da empresa além, é claro, de causar transtornos e preocupações desnecessários.

> Vulnerabilidades de hardware: São aquelas relacionadas aos equipamentos, vistos de modo individual. São exemplos de vulnerabilidades de *hardware* a ausência de atualizações de *firmware* pelos fabricantes, incompatibilidade com alguns *softwares*, dimensionamento inadequado (muitas informações para poucos dispositivos de armazenamento), muitas transações para pou-

> co processamento (número insuficiente de *CPU*), muito tráfego de dados para pouca banda de transmissão, desgaste natural, entre outros[14].

Ainda no que diz respeito ao hardware e/ou máquina escolhida pela instituição organizacional para que seus colaboradores desempenhem suas funções, encontra-se a preocupação com as ameaças externas. Estas ameaças seriam, basicamente, os elementos de origem natural, como forças meteorológicas, ou ainda, de questão de segurança, haja vista os frequentes furtos registrados em aparelhos de tal natureza, devido a sua facilidade de transporte e de compra nos mercados informais que estimulam essa prática.

Ou seja, além de se preocupar com os elementos de cunho interno, que são referentes à qualidade do produto, automaticamente quando a empresa adquire um aparelho de maior qualidade e, por vezes, de um valor elevado, existe também a necessidade de se ter o cuidado com a segurança física, haja vista a alta taxa de roubos e furtos que tem ocorrido nas instituições.

- ***SOFTWARE***

Deve-se optar por soluções de *software* que possibilitem um rastreamento mais facilitado de vírus, haja vista que, uma vulnerabilidade comum é a inexistência de procedimentos de testes de *softwares* para monitoramento frequente de forma a garantir a segurança de tais equipamentos.

> Vulnerabilidades de Software: São aquelas relacionadas às falhas de desenvolvimento e implantação dos aplicativos, sistemas operacionais e protocolos de comunicação, comumente conhecidos como *softwares*. Essas vulnerabilidades são muito comuns e poderosas, permitem que um invasor domine um sistema informatizado ou o faça deixar de responder a solicitações. São exemplos dessa vulnerabilidade o transbordamento de dados (*buffer overflow*), inundação de sincronia (*SYN flood*), ponteiros pendentes (*dangling pointers*), entre outros[14].

Também é fundamental a consciência de que não apenas as aplicações (programas) de uma máquina devem passar por uma prevenção frequente, mas também todos os elementos que se encontram em seu sistema, tais como, as imagens, textos e dados diversos, considerando que, mesmo que sejam arquivos internos, os mesmos podem ser corrompidos e comprometer a segurança da informação, além de possibilitar ataque que também prejudiquem a comunicação das organizações.

Ameaças como o comprometimento de dados e o aparecimento de erros durante a execução dos programas também são igualmente preocupantes, pois trazem inúmeros malefícios para as organizações, haja vista o risco de se perder informações de suma importância para as empresas e, consequentemente, trazer a possibilidade e o risco de invasão do sistema por indivíduos maliciosos que podem quebrar a comunicação e acarretar percas inestimáveis para as instituições.

- **REDE**

O acesso à rede é um elemento de grande contribuição para que existam ataques aos computadores. Dentre as suas vulnerabilidades destacam-se o uso de senhas que podem ser descobertas por outros indivíduos não autorizados com facilidade e riscos em decorrência da inexistência de mecanismos de autenticação e identificação. Tais vulnerabilidades trazem enormes preocupações às instituições empresariais, tendo em vista a possibilidade de invasão do sistema por *hackers* através da internet, que buscam realizar alterações maléficas nos sistemas da organização.

> Vulnerabilidades de transmissão: São aquelas relacionadas aos aspectos da comunicação de dados, abrangendo os meios físicos de transmissão (cabeamento, ondas de rádio, micro- -ondas, etc.) e os meios onde estes estão assentados (postes, tubulações, etc.). São exemplos desse tipo de vulnerabilidade: proximidade a florestas (quedas de árvores sobre o cabeamento), tráfego intenso de veículos (postes derrubados por acidentes de trânsito), tráfego de caminhões (podem romper o cabeamento que atravessa a via), obras de saneamento básico (podem destruir o cabeamento subterrâneo), grampeamento da transmissão (para furtar ou alterar informações), utilização indevida de canais de transmissão (rádios piratas), ratos (podem roer o cabeamento), entre outros[14].

As vulnerabilidades de rede, e a consequente ocorrência de uma invasão, podem ocasionar defeitos nos mais diversos *softwares* instalados na organização. As ameaças envolvem, principalmente, o forjamento dos direitos de acesso às informações, possibilitando que sejam acessadas de maneiras indevida. Consequentemente, também corroboram para que os riscos se ampliem e os invasores se sintam mais à vontade para realizar uma série de malefícios às instituições.

- **RECURSOS HUMANOS**

As vulnerabilidades encontradas nesse quesito, basicamente, consistem na gestão da instituição em escolher, de maneira mais bem específica, os seus cola-

boradores, de forma que os mesmos sejam plenamente confiáveis para a organização, não apenas para a sua segurança física, mas também para que seus dados e informações virtuais possam ser plenamente bem preservadas e não possibilitarem as invasões.

> Vulnerabilidades humanas: São aquelas decorrentes da ação ou omissão dos seres humanos. Em geral, são causadas pelo desconhecimento das normas básicas de segurança durante a utilização do ambiente de tecnologia da informação. Essas vulnerabilidades também podem decorrer de ações ou omissões intencionais. Como exemplos de vulnerabilidades humanas, podemos citar a falta de capacitação do usuário, a ignorância às normas de segurança, a insatisfação com o ambiente de trabalho, erros, falta de cuidado com os equipamentos, escolha de senhas fracas, compartilhamento de senhas de acesso, entre outros[14].

Além disso, outro elemento fundamental para prevenir tais vulnerabilidades é a contratação de mão de obra capacitada para lidar com os riscos e ameaças que norteiam as corporações nos dias atuais. Há algum tempo, a maior preocupação das empresas era de que os funcionários fossem confiáveis no que diz respeito à questão financeira. Entretanto, atualmente, existe essa prioridade em se ter uma capacitação e aprimoramento profissional, também na área tecnológica, para que, assim, sejam reduzidos gastos com manutenções e consertos desnecessários para as empresas.

Desta maneira, para evitar as ameaças como uso não autorizado de recursos, bem como, ocorrências de erros durante os usos da informação da instituição, existe a necessidade de se escolher e treinar bem especificamente o indivíduo que irá se instaurar na organização e ter acesso a todos os dados e informações contidas ali, desde o início de suas atividades.

Nesse sentido, é de suma importâncias que os Recursos Humanos sejam considerados como elementos imprescindíveis para que as empresas alcancem seus respectivos objetivos e tenham sucesso no decorrer de suas caminhadas profissionais.

- **INSTALAÇÕES/LOCALIZAÇÃO**

Esse aspecto é o mais elementar da instituição e, portanto, deve ser um dos primordiais quando se imagina a implementação de uma empresa de determinado ramo de atuação. Deve-se considerar que, caso ocorra uma escolha errada do local onde a instituição realizará as suas atividades, podem surgir imprevistos e vulne-

rabilidades tais como riscos de inundações, ausência de acesso a determinados mecanismos tecnológicos, tais como a incidência frequente de ausência de sinal de internet, dentre outros aspectos que, por ventura, venham a desestabilizar as funcionalidades da empresa. O objetivo é, assim, evitar incoerências e preocupações desnecessárias, haja vista que existe a possibilidade de se realizar uma pesquisa de localização que possa determinar um local mais bem adequado para serem realizadas as instalações da instituição.

> Vulnerabilidades ambientais: São aquelas relacionadas ao meio ambiente e à geografia do local onde a infraestrutura de tecnologia da informação da empresa está instalada. Exemplos: proximidade a refinarias de petróleo (explosões e corrosão de componentes pela poluição), proximidade a rios (inundações), locais muito distantes de usinas elétricas ou que possuam apenas uma unidade de geração de energia (desabastecimento), proximidade do litoral (tsunamis, maremotos, corrosão de componentes pela maresia), instalações em áreas de atividade sísmica (terremotos, erupções vulcânicas), instalações em áreas hostis (furacões, tornados, tempestades), entre outras[14].

Dentre as ameaças frequentes encontradas em tal quesito encontra-se a má utilização de equipamentos, devido ao espaço reduzido ou ausência de ventilação que, ocasionalmente, podem incorrer na destruição contínua de equipamentos de mídia e materiais diversos da empresa.

Também pode ocorrer interrupção do fornecimento de energia, inundações e demais ameaças que não apenas prejudicam financeiramente a empresa, haja vista que influem sobre a necessidade de trocar equipamentos com menor intervalo de tempo, mas também influenciam sobre o tempo de realização das atividades. A questão influencia também as formas como os colaboradores irão se posicionar frente a tais dificuldades encontradas sendo, inclusive, necessária a substituição de recursos humanos que são essenciais para o funcionamento da empresa.

- **ORGANIZAÇÃO**

A organização é o elemento mais importante da empresa, uma vez que seus aspectos, bem como planejamentos variados e instalações de políticas empresariais são norteadores das atividades da organização desde a sua implementação e, portanto, contribuem para fomentar as bases que estruturam todos os serviços realizados pela empresa.

Quando se fala em organização, inicialmente tem-se a ideia de planejamento de atividades, com a definição de objetivos e metas a serem alcançadas que,

por sua vez, são de suma importância para os trabalhos cotidianos e, também, para as expectativas esperadas pela empresa que são determinadas e definidas em longo prazo. Para estabelecer tais metas, é preciso que a instituição esteja organizada não apenas no que diz respeito aos seus aspectos estruturais, mas também no que se refere aos posicionamentos, ideais e a missão da organização frente ao seu mercado competitivo.

> Quando se analisa a segurança em sistemas de informação, é necessário ter em mente duas premissas: Primeiro, a segurança não é uma tecnologia. Não é um dispositivo que se possa comprar e que torne uma rede 100% segura, assim como não é possível também, comprar ou criar um software capaz de tornar um computador 100% seguro. E segundo, a segurança não é um estado que se pode atingir. A segurança é uma direção em que se pode viajar, porém, nunca se chegar de fato ao destino. O que se pode fazer é administrar um nível aceitável de risco[12].

Portanto, dentre as principais vulnerabilidades percebidas com a ausência de organização, destacam-se a inexistência de padrões adequados para o funcionamento da organização, passando pela falta de segurança e da ausência de planos de contenção de gastos, implementação de faturamento, dentre outros.

Também nessa perspectiva existem as ameaças que são ocasionadas por abuso de direitos, considerando a não existência de uma hierarquia bem estabelecida e de os colaboradores se encontrarem perdidos em meio à tomada de decisões. Também existe a questão do comprometimento com os dados, quebra de sigilos, falha nos serviços, enfim, uma gama de ameaças que insistentemente norteiam a empresa que não detém uma organização bem estabelecida dentro de suas limitações diárias. A organização é, assim, um aspecto importante que, caso não esteja presente em uma empresa, se torna um dos elementos de vulnerabilidade e de ameaças. Desta forma, deve ter uma atenção mais direta e especial, haja vista, que tais elementos são norteadores de todas as demais atividades da instituição empresarial.

## 4.1 O CGI.br

Os problemas pelos quais não apenas o usuário comum dos computadores pode enfrentar são muito mais complexos quando se imagina a utilização de

uma série de dados filtrados por empresas e, também, as informações de cunho sigiloso que podem ser afetadas pelo vazamento dos dados das máquinas das instituições empresariais. Ou seja, os perigos não são apenas físicos e tampouco se restringem a preocupações com roubos e/ou furtos de equipamentos, mas também é preciso ter essa consciência de que os ataques virtuais são relativamente preocupantes e, por isso, podem se traduzir em riscos potenciais para a perda de trabalhos que levaram anos para serem construídos, além de, é claro, trazer infortúnios consideráveis para as organizações.

> O Comitê Gestor da Internet – CGI.br é uma experiência pioneira e única. Composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, o CGI.br representa um modelo de governança democrático e plural, em que os representantes de cada segmento não governamental são eleitos para compor um órgão colegiado que exerce o papel de coordenar e integrar as iniciativas de serviços de Internet no país[15].

Um dos elementos, que buscam frequentes soluções para os problemas tecnológicos no que diz respeito aos riscos sofridos pela segurança da informação, é o CGI (Comitê Gestor de Internet), norteado pelo Decreto Presidencial nº 4.829 [16], de 03 de setembro de 2003 que configura, dentre as suas especificidades, regulamentar o uso da internet no país e, assim, garantir que normas e procedimentos sejam adequados para que se respeitem as leis de segurança no âmbito da TIC.

> A implantação de políticas de governo eletrônico avança guiada por instrumentos e processos de gestão dos recursos de TIC. Nesse sentido, a Secretaria de Logística e Tecnologia da Informação (SLTI), do Ministério do Planejamento, Orçamento e Gestão (MPOG), é responsável por propor políticas, planejar, coordenar, supervisionar e orientar normativamente as atividades de: gestão dos recursos de tecnologia da informação, no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP); gestão dos recursos de logística sustentável, no âmbito do Sistema de Administração de Serviços Gerais (SISG); gestão de convênios e contratos de repasse; governo eletrônico, relacionadas à padronização e à disponibilização de serviços eletrônicos interoperáveis, acessibilidade digital e abertura de dados. Destacam-se, entre as ações de governo eletrônico implementadas pela SLTI, o Guia de Serviços Públicos do Governo Federal (servicos.gov.br) e a Infraestrutura Nacional de Dados Abertos (INDA) (dados.gov.br), além do Modelo de Acessibilidade em Governo Eletrônico (eMAG) e dos Padrões de Interoperabilidade de Governo Eletrônico (ePING)[17].

Tal ferramenta, mais do que determinar normas rígidas a serem seguidas, também busca as frequentes atualizações de seus padrões de segurança, considerando que se possibilite a preservação das redes, por meio de monitoramento dos registros que utilizam o final “.br”, além de realizar frequentes estudos e pesquisas

na área de tecnologia da informação e comunicação com o intuito de estabelecer parâmetros adequados para o acesso seguro à internet.

> Entende-se, portanto, imprescindível a produção de dados e informações confiáveis que permitam compreender como as TIC estão sendo utilizadas pela administração pública com o objetivo de transformar o seu relacionamento com a sociedade. O Cetic.br, que já mede anualmente, desde 2005, o uso do governo eletrônico pelos cidadãos e empresas por meio das pesquisas TIC Domicílios e TIC. Empresas, que fornecem informações a respeito da demanda por esse serviço, passa a produzir regularmente estatísticas e indicadores também do lado da oferta de serviços eletrônicos por parte dos órgãos públicos brasileiros. Medir esses avanços em ambos os lados é fundamental para a implementação de políticas efetivas e eficazes tanto para os usuários de governo eletrônico quanto para as organizações públicas que são responsáveis pela implantação de ações nessa área[17].

O comitê, em decorrência de tais responsabilidades automaticamente efetiva coleta de informações que demonstram a situação real do uso da rede no Brasil, destacando quais os principais riscos que tem surgido no mercado, os indicadores de ataques sofridos por organizações e estatísticas que contribuem para o conhecimento mais detalhado dos aspectos de segurança da informação, com vistas a garantir o mínimo de qualidade no momento em que o usuário se dispõe a acessar a internet.

> O Comitê Gestor da Internet no Brasil (CGI.br) produz anualmente dados e informações estratégicas sobre o acesso e uso das tecnologias de informação e comunicação (TIC), visando a subsidiar a sociedade com dados confiáveis e atualizados sobre os impactos das TIC e, particularmente, da Internet, na sociedade e na economia. A Internet é hoje um meio importante para o desenvolvimento social e pessoal, bem como para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos. Assim, nosso principal objetivo é contribuir para que se possa desenvolver políticas públicas efetivas e eficazes, além de gerar informações que possam ser utilizadas tanto para o desenvolvimento da Internet no Brasil, quanto para o suporte a pesquisas acadêmicas que contribuam para a construção de conhecimento sobre o tema[18].

O CGI.br (Comitê Gestor de Internet no Brasil) divulgou, em 2012, uma cartilha de segurança para a internet[19] que tinha como intuito analisar os principais riscos e ataques aos quais os computadores estariam expostos, assim como disseminar as informações a respeito de tais elementos que poderiam prejudicar o funcionamento das máquinas.

> A Cartilha de Segurança para Internet e um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. O documento apresenta o significado de diversos termos e conceitos utilizados na Internet, aborda os riscos de uso desta tecnologia e fornece uma série de dicas e cuidados a serem tomados pelos usuários para se protegerem destas ameaças[19].

Tal estudo já havia sido realizado em anos anteriores, com o CERT.br que também é um instrumento fundamental para a manutenção da segurança da informação no país e que será melhor detalhado e vislumbrado no capítulo a seguir.

## 4.2 O CERT.br

As transformações que ocorreram com a internet no decorrer das décadas, desde o seu surgimento a partir da década de 70 por meio de redes limitadas que apenas objetivavam servir como instrumento reserva de troca de informações durante a Guerra Fria, até os dias atuais também foram de suma importância para que os sistemas de informação e comunicação evoluíssem para algo mais rápido, dinâmico e eficiente ao ponto de que a troca de informações se tornarem algo imediato e livre de atrasos, até mesmo porque na sociedade contemporânea o imediatismo e eficácia são características importantes e valorizadas para que se mantenha e garanta a comunicação de uma maneira plena e satisfatória.

> A rápida disseminação das tecnologias de informação e comunicação (TIC), especialmente a Internet, está no centro das mudanças sociais, econômicas e culturais que ocorrem em todo o mundo. Um dos atores afetados por estas mudanças são os governos, cada vez mais atentos quanto à necessidade de transformar o modo como se relacionam com indivíduos e organizações[17].

Esse mecanismo, mais do que uma evolução do sistema de redes é um instrumento que fornece aos seus usuários se comunicarem, em tempo real, utilizando ferramentas que viabilizem o contato com o outro a partir do computador, demonstrando que a tecnologia pode ir além da mera transmissão de dados e contribuir efetivamente para a construção de uma cultura que vise uma real transformação social por meio de instrumentos tecnológicos que, acima de tudo serão utilizados de forma democrática e partilhados por todos os cidadãos.

> Os crescentes efeitos de fenômenos como as redes sociais na Internet e da tendência irreversível à mobilidade no acesso à Internet são incontestáveis. O avanço no uso de dispositivos como *notebooks*, *tablets* e celulares, que

> passam a fazer parte da vida cotidiana de uma parcela considerável da população e da grande maioria das empresas brasileiras, mostra o fato[20].

Entretanto na medida em que ocorrem as evoluções e as facilidades de vida se transfiguram de maneiras mais específica, junto com elas surgem também os problemas, como se pode perceber pela citação dos riscos decorrentes de tais utilizações da tecnologia, sendo necessária a criação de uma série de fatores e normas de regulamentação que tenham o foco na segurança do acesso aos dados dos indivíduos, haja vista a intensa utilização de instrumentos que podem se tornar alvos para ataques virtuais.

O CERT (*Computer Emergency Response Team*)[21] foi criado em 1988, porém o CERT.br, que é o responsável por tais atividades no Brasil, surgiu apenas em 1997 e, em suma, tem o intuito de realizar atividades no âmbito da Tecnologia da Informação e Comunicação, mais especificamente no que diz respeito à utilização da internet no Brasil, assim, ele se subdivide em 3 categorias principais que representam suas atividades mais frequentes, que consistem no tratamento de incidentes, treinamento e análise de tendências.

> • Tratamento de Incidentes: Dar suporte ao processo de recuperação e análise de ataques e de sistemas comprometidos; Estabelecer um trabalho colaborativo com outras entidades, como outros CSIRTs, empresas, universidades, provedores de acesso e serviços Internet e *backbones*; Manter estatísticas públicas dos incidentes tratados e das reclamações de spam recebidas.
> • Treinamento e Conscientização: Oferecer treinamentos na área de tratamento de incidentes de segurança, especialmente para membros de CSIRTs e para instituições que estejam criando seu próprio grupo; Desenvolver documentação de apoio para administradores de redes Internet e usuários; Realizar reuniões com setores diversos da Internet no Brasil, de modo a articular a cooperação e implantação de boas práticas de segurança.
> • Análise de Tendências de Ataques: Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro, através da manutenção de uma rede de *honeypots* distribuídos em diversas redes do país; Obter, através de *honeypots* de baixa interatividade, dados sobre o abuso da infraestrutura de redes conectadas à Internet para envio de *spam*[22].

O tratamento de incidentes, por assim dizer, busca o aprimoramento das ferramentas que impedem o acesso de pessoas não autorizadas aos dados particulares, seja de um indivíduo ou de uma organização, assim, tal etapa tem a responsabilidade de articulação, ou seja, capacidade de responder aos ataques com o máximo de rapidez e precisão possível, de maneira que sejam alternativas eficientes

para o solucionamento dos problemas, bem como, também a busca e detecção dos responsáveis pela invasão.

Portanto, além de estimular essa resposta aos riscos, também é imprescindível que existam apoios às recuperações, ou seja, que sejam disponibilizados os mecanismos capazes de reforçar a segurança do uso da internet, bem como, de oferecer suporte aos usuários, para que os mesmos se sintam mais confortáveis ao realizar os seus acessos e, portanto, como existe a necessidade dessa ligação é fundamental o registro das ocorrências, a fim de se realizar levantamentos estatísticos que, mais do que apenas informar a respeito das intercorrências também estimulam a busca contínua por uma melhor qualidade no acesso à rede.

No que diz respeito ao treinamento, a abordagem do comitê é mais ativa com os usuários de sistemas da internet, uma vez que esse elemento traz uma maior qualidade nas formas que as pessoas têm de acessar o computador, destacando a primazia pelas seguranças e destacando que o uso cauteloso de seus softwares proporciona uma melhor utilização da rede como um todo, evitando-se a disseminação de novos ataques.

Por último, mas não menos importante, no que diz respeito a análise de tendências, basicamente consiste em uma análise frequente de softwares maliciosos da internet, de maneira que se possa realizar um filtro e realizar uma espécie de medição no que concerne aos ataques e riscos aos quais os computadores encontram-se expostos continuamente para que, assim, seja possível realizar intervenções positivas que priorizem a prevenção e seja possível a minimização do impactos e a busca constante por uma solução viável de tais problemas, uma vez que surgem cotidianamente novas ameaças.

> O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.
> Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.
> Além do processo de tratamento a incidentes em si, o CERT.br também atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos CSIRTs no Brasil[22].

Dentre as principais atividades do CERT.br, está a manutenção de estatísticas públicas dos incidentes tratados e das reclamações de *spams* recebidas. Ob-

serva-se, no Gráfico 1, que o quantitativo de incidentes reportados deu um “grande salto” em 2014 e possui uma tendência de aumento ao longo dos anos.

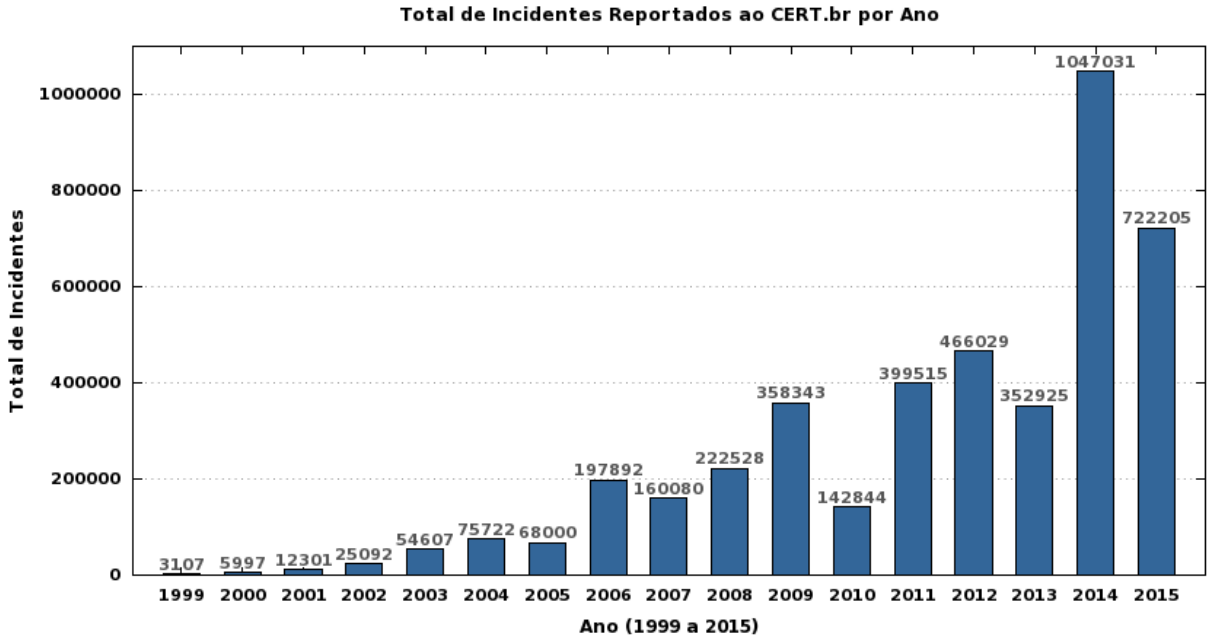



Gráfico 1: Total de incidentes reportados ao CERT.br por ano.

[23]

Os dados registrados nesse período demonstram, assim, que apesar da existência de uma série de controles, tanto estabelecidos pelo CGI, quanto pelos demais órgãos responsáveis por essas especificidades, também ocorre um crescimento progressivo dos incidentes, com o passar dos tempos, isso ocorre, primordialmente, em decorrência do aperfeiçoamento dos ataques e, conforme o avanço tecnológico acontece, automaticamente, também ocorrem aprimoramentos com os ataques que provocam tais incidentes, por isso é preciso que exista uma busca frequente por melhoramentos nas maneiras de se combater esses riscos, uma vez que os *softwares* mal intencionados também estão cada vez mais preparados para invadir os sistemas independentemente do *hardware* que ali se encontra, sendo necessário o aperfeiçoamento do software e dos sistemas operacionais.

No ano de 2014, por exemplo, houve um avanço bem significativo que foi reduzido significativamente em 2015, decorrente do aprimoramento das ferramentas que impediam os ataques e da disseminação de riscos dos mesmos que, por sua

vez, também demonstrar uma maior cautela na utilização e isso, por si só, já reduz drasticamente as chances de maior disseminação do problema, uma vez que os usuários se valem de mais mecanismos que impedem os taques e minimizam a ocorrência de incidentes.

No Gráfico 2, os incidentes reportados no ano de 2015 são relacionados percentualmente e podem servir como parâmetro para que as empresas desenvolvam uma política de segurança prevenindo, principalmente, os principais eventos registrados na internet brasileira.

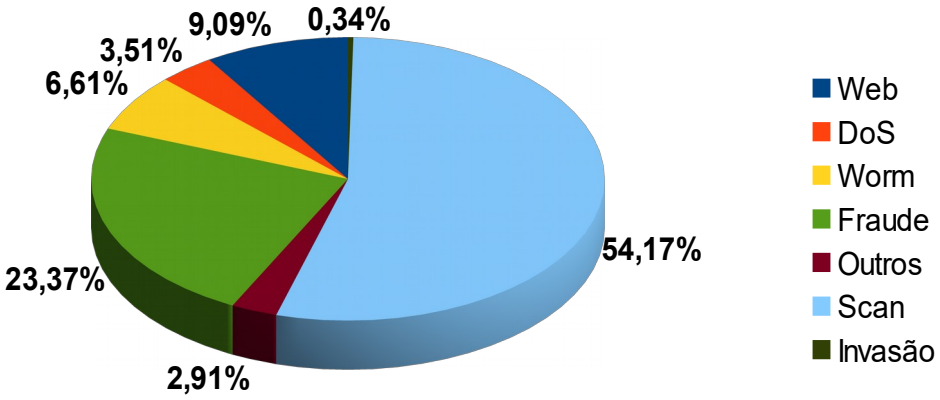



Gráfico 2: Tipos de Incidentes Reportados ao CERT.br em 2015.

Legenda:

- *worm*: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- dos (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- *web*: um caso particular de ataque visando, especificamente, o comprometimento de servidores *Web* ou desfigurações de páginas na Internet.
- *scan*: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- outros: notificações de incidentes que não se enquadram nas categorias anteriores.

[24]

Percebe-se que a maior quantidade de incidentes, em 2015 ocorreu com a utilização de *scans*, desta maneira, valendo-se de tal informação é possível estabelecer um paralelo com a empresa demonstrando que o reforço de barreiras e restrição de acessos no momento das varreduras e, também, durante toda a utilização do sistema é uma alternativa que proporciona um impedimento mais substancializado que, por sua vez, mesmo que não impeça 100% dos ataques, somando-se alguns outros cuidados, pode-se tornar possível um controle mais específico de usuários que acessam o sistema e, assim, garantir uma maior segurança.

Possuir uma visibilidade do que ocorre realmente em sua rede e seu negócio é a melhor maneira para atingir uma resposta adequada aos incidentes, posto que, por maior que sejam os investimentos em prevenção e detecção, crimes e acidentes continuarão ocorrendo.

Na busca por uma maior compreensão e criação de defesas para essas infinidades de ameaças concorrentes à constante e crescente evolução tecnológica, a humanidade despende grandiosos esforços para encontrar alternativas que possam garantir a Segurança da Informação. Com este objetivo, as empresas buscam suporte em normas reconhecidas mundialmente que estão em constante desenvolvimento. Tais normas serão abordadas no próximo capítulo.

# 5 DESENVOLVIMENTO DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO

> Norma é o documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece regras, diretrizes ou características mínimas para atividades ou para seus resultados, visando à obtenção de um grau ótimo de ordenação em um dado contexto.
> A norma é, por princípio, de uso voluntário, mas quase sempre é usada por representar o consenso sobre o estado da arte de determinado assunto, obtido entre especialistas das partes interessadas[25].

De acordo com o desenvolvimento tecnológico humano, conforme visto ao longo de todo o trabalho, quanto mais útil for a informação, mais necessária, e quanto mais preciosa, mais cobiçada. Portanto, é cada vez mais necessário compreender a informação como um bem.

Tal facilidade que a web remete traz incontáveis evoluções para todas as áreas de conhecimento humano, não apenas para os saberes relacionados à Análise de Sistemas e de Informática, como também para diversas outras vertentes tais como: a educação, por meio do aperfeiçoamento das ferramentas tecnológicas do ensino; o fortalecimento das relações sociais, pois cada vez mais, as pessoas tendem a se comunicar utilizando a tecnologia e, assim, aproximar-se mais do outro que se encontra distante geograficamente e, também, construir novas relações; o comércio, através da evolução e especificação dos sites de compra coletiva que, cada vez mais, se estabelecem como práticos e objetivos, facilitando a vida dos cidadãos e conquistando seu espaço no mercado.

Nesse sentido, esse mecanismo não apenas colaborou para o desenvolvimento de um caráter mais social da internet, como também serviu, direta ou indiretamente, como instrumento que ultrapassa a rapidez na troca de informações.

Há algum tempo, a utilização das facilidades da *web* só era possível em computadores enormes que, em geral, ficavam dentro das residências ou empresas. Estes computadores utilizavam metros e metros de fios para conseguir conectar em uma conexão de discagem que era lenta, por vezes demorava horas para se conse-

guir baixar uma imagem e, imagine ter uma comunicação imediata e um sistema de informações que economizasse espaço e tempo. O suporte dos *e-mails* era limitado, e não era possível, tampouco imaginável, o que hoje pode ser visto e realizado com o uso da internet.

Atualmente, a internet está em todos os aparelhos, dos mais simples até os mais modernos. Onde quer que se vá, encontram-se crianças, jovens, adultos e idosos com seus *smartphones*, *tablets*, dentre tantos outros mecanismos da era tecnológica que fica difícil até mesmo de enumerá-los por completo. Pode-se dizer que, na atual época contemporânea na qual encontramo-nos inseridos, alguns não sabem como é viver sem esses aparelhos eletrônicos e das mais diversificadas mídias, pois, quando nasceram, os mesmos já existiam e sempre estiveram presentes em suas vidas desde muito cedo.

Analisando a história dos computadores tendo o ENIAC (1946) como o principal exemplo da primeira geração de computadores, até a construção do DEC PDP-8 em 1965, considerado o primeiro computador portátil e tendo atingido vendas acima de 50 mil unidades no ano de lançamento, pode-se afirmar que o problema da segurança dos sistemas não demorou a ser abordado, tendo sido elaborado um documento chamado "*Security Controls for Computer System*"[26] já em 1967, que marcou o passo inicial para a criação de um conjunto de regras para segurança de computadores.

Livre tradução de trecho do prefácio do documento "*Security Controls for Computer System* (U) – Relatório da Força Tarefa de Segurança de Computador do Conselho de Defesa e Ciência":

> A questão do controle de segurança em sistemas de recursos compartilhados foi trazido à tona pelo Departamento de Defesa (EUA) por uma série de eventos (de incidentes de segurança) ocorridos na primavera e verão de 1967. Tais sistemas têm sido corrompidos em número crescente nas instalações governamentais; os problemas de segurança desses sistemas tornaram-se interesse prioritário tanto para contratos de defesa quanto para operações militares; os Administradores de Pesquisa em Segurança encaminharam um documento através da Agência de Suprimentos de Defesa para o diretor de Políticas de Segurança no escritório da Secretaria de Defesa (Administração) solicitando uma ação. Como o problema envolvia questões técnicas, o documento foi remetido para o escritório do diretor de Defesa Pesquisa e Engenharia para parecer[26].

Com maior utilização de sistemas informatizados, ocorreu a elevação no número de incidentes de segurança em âmbito mundial, e destacou-se a possibilida-

de de perdas financeiras substanciais pela ausência de estruturação de processos capazes de garantir a Segurança da Informação.

Embora a questão tenha sido “levantada” em 1967 no âmbito do Departamento de Defesa dos Estados Unidos da América, somente em 11 de fevereiro de 1970 o relatório da “Força Tarefa” foi publicado com recomendações políticas e técnicas para a redução de ameaças às informações sigilosas processadas em sistemas de computadores.

É interessante destacar algumas conclusões alcançadas pela “Força Tarefa”:

> 1) Prover controle de segurança satisfatório em um sistema de computadores é intrinsecamente um problema de *design*. Uma combinação de *hardware*, *software*, comunicações, espaço físico, pessoas e procedimentos administrativos de salva guarda são necessários para prover segurança. Em particular, *softwares* de segurança isolados não são suficientes.
> 2) A tecnologia contemporânea pode prover um sistema de segurança aceitável, resistente a ataque externo, divulgação acidental, subversão interna, e negação de uso para legitimar usuários em ambientes fechados (usuários idôneos trabalhando com informação classificada em consoles fisicamente protegidos conectados ao sistema por circuitos de comunicação protegidos).
> 3) A tecnologia contemporânea não pode prover um sistema de segurança em um ambiente aberto, que inclui usuários inidôneos trabalhando em consoles fisicamente desprotegidos conectados ao sistema por comunicações desprotegidas.
> 4) É imprudente incorporar informação classificada ou sigilosa em um sistema funcionando em ambiente aberto a menos que um risco significante de divulgação acidental possa ser aceitável.
> 5) Procedimentos aceitáveis e salva guardas existem e podem ser implementadas para que um sistema funcione alternadamente em ambiente fechado e em ambiente aberto.
> 6) *Designers* de sistemas de segurança ainda estão na parte inicial da curva de aprendizado e muito discernimento e experiência operacional com vários sistemas serão necessários.
> 7) Aperfeiçoamento substancial (exemplo: custo, performance) em sistemas de controle de segurança podem ser esperados se algumas áreas de pesquisa puderem ser seguidas com sucesso[26].

Simultaneamente aos esforços do Departamento de Defesa dos Estados Unidos, a NBS (*National Bureau of Standards*) iniciou trabalhos para definição de problemas e soluções para construção, avaliação e auditoria de sistemas de computadores seguros.

Foram promovidos dois *workshops* pela NBS, o primeiro em março de 1977 e o segundo em novembro de 1978 que produziu um documento intitulado como *Trusted Computer System Evaluation Criteria*[27]*,* que teve sua versão final impressa somente em 26 de dezembro de 1985.

O documento também ficou conhecido como *The Orange Book* devido à cor laranja da capa e é considerado o início da busca mundial pela qualificação de um ambiente computacional seguro, por especificar implementações necessárias aos *softwares* e classificando-os em níveis de segurança.

Outros documentos derivaram do *Orange Book*, contendo adaptações e/ou complementações para especificação e classificação de diversos requisitos computacionais, como redes de computadores, banco de dados e gerenciamento de senhas; e, por possuírem diferentes cores de capas, essa série de livros ficou conhecida como *Rainbow Series* ou *Rainbow Books.*

A preocupação com a Segurança da Informação devido à possibilidade de prejuízos substanciais não era exclusividade dos Estados Unidos da América e, em 1987, o departamento de comércio e indústria do Reino Unido criou o CCSC (*Comercial Computer Security Centre*) com a tarefa de criar uma norma de SI através da criação de critérios para avaliação da segurança.

O CCSC também tinha como objetivo a criação de um código de segurança para os usuários das informações e, em 1989 publicou o documento chamado PD0003 – Código para Gerenciamento da Segurança da Informação, que passou por revisões e foi finalmente publicado como norma em 1995, a norma britânica BS7799:1995[28].

Dando prosseguimento aos trabalhos, foi publicado em 1997 uma segunda parte do documento, vindo tornar-se norma em 1998, a BS7799-2:1998, que sofreu revisão e foi publicada junto com a primeira parte em abril de 1999 como BS7799:1999[29].

A primeira parte desse documento foi encaminhada à ISO (*International Organization for Standardization*) e homologada em dezembro de 2000, passando a chamar-se ISO/IEC 17799:2000[30].

Vários países também tentavam desenvolver padrões para desenvolvimento de sistemas seguros. Nos Estados Unidos da América desenvolviam o TCSEC (*Trusted Computer System Evaluation Criteria*), no Canadá o CTCPEC (*Canadian Trusted Computer Product Evaluation Criteria*), nos países europeus os critérios foram unificados desenvolvendo o ITSEC (*Information Technology Security Evaluation Criteria*).

Em 1996, houve a unificação dos padrões europeu e norte-americano, gerando o CC (*Common Criteria*) que, em dezembro de 1999, na versão 2.1, tornou-se a norma ISO/IEC 15408-1:1999[31].

A norma ISO/IEC 15408-1, apresenta critérios para a definição e avaliação de requisitos de segurança de sistemas, enquanto a norma ISO/IEC 17799 apresenta critérios para a definição e avaliação de requisitos de segurança de organizações.

Após um período de ampla revisão, a norma ISO/IEC 17799:2000 foi publicada em junho de 2005 como a versão ISO/IEC 17799:2005. Também em 2005, a segunda parte da norma BS7799 foi adaptada pela ISO/IEC e publicada como a norma ISO/IEC 27001:2005.

A partir da ISO/IEC 27001, foi iniciada uma série direcionada à padronização de normas para a segurança da informação. Em julho de 2007, a ISO/IEC 17799:2005 passou a ter outra numeração, tornando-se a norma ISO/IEC 27002:2005. A “família” 27000 para SGSI[32] possui atualmente as seguintes normas:

- **ISO/IEC 27000:2016**: Sistema de Gestão de Segurança da Informação — Visão geral e vocabulário;
- **ISO/IEC 27001:2013**: Sistema de Gestão de Segurança da Informação — Requisitos;
- **ISO/IEC 27002:2013**: Boas práticas para controles de segurança da informação;
- **ISO/IEC 27003:2010**: Guia de implantação do Sistema de Gestão de Segurança da Informação;
- **ISO/IEC 27004:2009**: Gestão da segurança da informação — Medição;
- **ISO/IEC 27005:2011**: Gestão de risco em segurança da informação;
- **ISO/IEC 27006:2015**: Requisitos para empresas de auditoria e certificação de Sistemas de Gestão de Segurança da Informação;
- **ISO/IEC 27007:2011**: Diretrizes para auditoria em Sistemas de Gestão de Segurança da Informação;
- **ISO/IEC TR 27008:2011**: Diretrizes para auditores sobre controle de segurança da informação;

- **ISO/IEC 27009:2016**: Seção específica de aplicação da ISO/IEC 27001— Requisitos;
- **ISO/IEC 27010:2015**: Gestão de segurança da informação para comunicação inter-setorial e inter-organizacional;
- **ISO/IEC 27011:2008**: Diretrizes para gestão de segurança da informação em organizações de telecomunicação com base na ISO/IEC 27002
- **ISO/IEC 27013:2015**: Diretrizes para a implementação integrada da ISO/IEC 27001 e ISO/IEC 20000-1;
- **ISO/IEC 27014:2013**: Governança de segurança da informação
- **ISO/IEC TR 27015:2012**: Diretrizes para a gestão de segurança da informação em serviços financeiros;
- **ISO/IEC TR 27016:2014**: Diretrizes para a gestão de segurança da informação – Empresas de economia;
- **ISO/IEC 27017:2015**: Boas práticas para controles de segurança da informação baseadas na ISO/IEC 27002 para serviços na nuvem;
- **ISO/IEC 27018:2014**: Boas práticas para proteção de informação de identificação pessoal em nuvem;
- **ISO/IEC 27019:2014**: Diretrizes para gestão de segurança da informação baseadas na ISO/IEC 27002 para sistemas de controle de processos específico para indústria de energia;
- **ISO 27799:2008**: Informática em saúde – Gestão da segurança da informação na saúde usando ISO/IEC 27002.

Nota-se que uma considerável evolução ocorreu com as normas de seguranças das instituições empresariais, assim como também percebe-se que, conforme as necessidades de segurança, se aprimoraram, em paralelo, inovadoras maneiras de indivíduos mal-intencionados realizarem seus ataques.

Indubitavelmente, a busca constante pela segurança encontra seu maior revés na ameaça humana que, com toda criatividade e intelecto acaba, sempre descobrindo maneiras para transpor quantas barreiras forem implementadas. Tais ameaças, motivações e possíveis consequências conhecidas até o momento, encontram-se elencadas no “ANEXO B – FONTES DE AMEAÇAS REPRESENTADAS POR SERES HUMANOS.”

Portanto, as normatizações devem estar em frequente evolução, carregando aspectos que impeçam tais mecanismos de agirem nos sistemas, na intenção de se garantir o sigilo durante os acessos, considerando que as missões das empresas devem priorizar o zelo por seus clientes e, assim, exaltar os aspectos da segurança nos seus acessos.

> O crescente uso da tecnologia nas empresas brasileiras deixou de ser artigo de luxo, tornou-se uma questão de sobrevivência no mercado. E não apenas pelo aspecto da competitividade, mas também para atender às exigências legais: o empresário precisa implementar ferramentas tecnológicas para cumprir obrigações fiscais e trabalhistas, por exemplo.
> Neste cenário, junto com o impulso na demanda por produtos tecnológicos, aumentou também a prática de ilícitos, tais como obtenção indevida de dados, propagação maliciosa de vírus e diversos tipos de estelionatos[33].

Sendo assim, mais do que demonstrar o histórico de evoluções e do desenvolvimento das normas de segurança da informação cabe, aqui, destacar o caráter essencial de uma constante busca por um aprimoramento adequado das medidas de seguridade. Tais medidas são fundamentais e imprescindíveis para a utilização das tecnologias e, talvez com elas, as empresas consigam alcançar suas metas com responsabilidade, respeitando não apenas os seus usuários, mas todos os que se encontram envolvidos, direta ou indiretamente, no decorrer do exercício de seus processos, desde o início até o público final.

A preocupação com a segurança surgiu bem antes de os sistemas informacionais terem sido implementados pela sociedade inovadora que estimulou a propagação da cultura nessa nova era digital, trazendo, consigo, elementos tecnológicos que, igualmente aos elementos que são físicos e palpáveis, podem também sofrer ataques virtuais e, por isso, terem informações de caráter particular e/ou sigiloso comprometidos, trazendo a insegurança também para essa área da vida do cidadão.

O desenvolvimento de ferramentas que tinham o intuito de favorecer o cidadão e manter a segurança de seu acesso na rede virtual, iniciou-se com alternativas de restringir a informação a um pequeno grupo de indivíduos, ou apenas a uma única pessoa e, com isso, fazer com que as normas mínimas de segurança fossem respeitadas, consagrando, desta maneira, o mínimo possível de falhas nos sistemas e trazendo uma certa garantia, ou seja, uma sensação de que os dados estavam seguros e devidamente resguardados.

Com isso surgiu uma normatização mais específica para a área tecnológica garantindo que os usuários não apenas resguardassem seus dados de forma

mais segura, mas também que tornasse possível o tráfego seguro de informações pela rede. Ou seja, não apenas restringia o acesso de indivíduos maliciosos àquela determinada máquina em específico, como também possibilitava que a navegação na rede se configurasse de uma maneira mais bem delimitada, garantindo que não apenas o sistema operacional se tornasse mais seguro, como também o acesso à internet.

> Esta norma (27001) foi publicada pelo ISO e pelo IEC em Outubro de 2005. Foi elaborada para especificar os requisitos para o estabelecimento, implementação, operacionalização, monitorização, revisão, manutenção e melhoria de um SGSI, dentro do contexto dos riscos de negócio de uma organização.
> A certificação não é um requisito obrigatório da norma ISO 27001, é uma decisão da organização. No entanto, dezoito meses após a sua publicação mais de 2000 organizações de mais de 50 países foram certificadas e o crescimento nesta área tem vindo a aumentar[34].

Isso, por sua vez, também aumentou as expectativas de uso quanto à rede e, assim, a popularização da navegação também se intensificou. Ao passo em que os indivíduos, bem como empresas públicas e privadas, também reconhecessem esse potencial e houvesse um maior investimento no uso dos elementos computacionais, uma dedicação dos governos em trazer o mínimo de segurança para seus usuários seria consequente.

Na Tabela 1, fica demonstrada a evolução na utilização da certificação ISO/IEC 27001 nos dois países com maiores números de certificações de cada região do mundo. Os números apresentados representam o número de certificações. Conforme mostram os dados, um grande aumento na utilização desta norma pode ser observado, principalmente nos EUA, Japão, China, Reino Unido e Índia. No Brasil, a utilização de tal norma não é muito comum, porém, observa-se uma tendência ao crescimento no número de certificações no decorrer dos anos.

| REGIÃO | PAÍS | ANO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
| ÁFRICA | África do Sul | 5 | 8 | 10 | 14 | 14 | 14 | 22 | 35 | 22 |
| | Nigéria | 0 | 0 | 0 | 0 | 0 | 5 | 9 | 12 | 16 |
| AMÉRICA DO SUL E CENTRAL | Brasil | 10 | 25 | 40 | 48 | 41 | 50 | 53 | 82 | 86 |
| | Colômbia | 3 | 8 | 11 | 14 | 23 | 27 | 58 | 82 | 80 |
| AMÉRICA DO NORTE | EUA | 69 | 94 | 168 | 252 | 247 | 315 | 415 | 566 | 664 |
| | Canadá | 1 | 5 | 13 | 21 | 26 | 50 | 62 | 66 | 76 |
| ÁSIA ORIENTAL E PACÍFICO | Japão | 3790 | 4896 | 4425 | 5508 | 6237 | 6914 | 7199 | 7140 | 7181 |
| | China | 75 | 146 | 236 | 459 | 957 | 1219 | 1490 | 1710 | 2002 |
| EUROPA | Reino Unido | 486 | 519 | 738 | 946 | 1157 | 1464 | 1701 | 1923 | 2261 |
| | Itália | 175 | 148 | 233 | 297 | 374 | 425 | 495 | 901 | 970 |
| ÁSIA CENTRAL E SUL | Índia | 369 | 508 | 813 | 1240 | 1281 | 1427 | 1611 | 1931 | 2170 |
| | Sri Lanka | 13 | 6 | 10 | 23 | 21 | 42 | 27 | 37 | 33 |
| ORIENTE MÉDIO | Israel | 0 | 24 | 61 | 78 | 86 | 110 | 130 | 185 | 201 |
| | Emirados Árabes | 14 | 15 | 27 | 53 | 57 | 73 | 96 | 123 | 131 |

Tabela 1: Evolução da certificação ISO/IEC 27001 pelo mundo – Crescimento do fim de 2006 até o fim de 2014.

[35]

Cabe ressaltar que, aqui, pode-se considerar um marco na utilização da internet, não por ter se dedicado a sua evolução em particular, mas devido ao fato dessa busca pela segurança do acesso ter intensificado a qualificação, aperfeiçoamento e evolução dos fatores de proteção de acesso que, hoje, são fundamentais dentro de uma política e uma visão mais social da sociedade tecnológica na qual encontramo-nos inseridos.

> A primeira fase do processo envolve as organizações, o facto de estarem preparadas para a certificação do seu SGSI: desenvolvimento e implementação do seu SGSI, utilização e integração do seu SGSI no seu dia-a-dia e nos seus processos de negócio, formação da sua equipe e estabelecimento de um programa contínuo de manutenção do SGSI. A segunda fase envolve uma auditoria do SGSI da organização, envolvendo os organismos de certificação acreditados. O certificado concedido tem a duração de três anos, pelo que a terceira fase do processo passa pelo acompanhamento por parte das entidades certificadoras[34].

No que concerne ao âmbito nacional, a ABNT (Associação Brasileira de Normas Técnicas), é uma das responsáveis por trazer os elementos de seguridade da informação para o Brasil e, com isso, atentar às particularidades do país e elaborar normatizações técnicas que visem o bom andamento das atividades diárias reali-

zadas com o uso da internet, sejam elas particulares, públicas, empresariais, domésticas, dentre outras.

As normas nacionais “NBR ISO/IEC” da “família” 27000, são traduções idênticas em conteúdo técnico, estrutura e redação das normas “ISO/IEC” e se baseiam, basicamente, em catorze elementos que tangem e norteiam o uso dos computadores e da internet de uma maneira geral, a saber: política de segurança; organização da segurança; segurança em recursos humanos; gestão de ativos da informação; controle de acesso; criptografia; segurança física e do ambiente; segurança nas operações; segurança nas comunicações; aquisição, desenvolvimento e manutenção de sistemas; relacionamento na cadeia de suprimento; gestão de incidentes; gestão da continuidade do negócio; conformidade com as legislações vigentes.

Além das traduções da “família” 27000, outras normas também fazem parte do catálogo da ABNT[36] para segurança/tecnologia da informação, são elas:

- **ABNT NBR 16167:2013**: Segurança da informação — Diretrizes para classificação, rotulação e tratamento da informação;
- **ABNT NBR 16386:2015**: Tecnologia da informação — Diretrizes para o processamento de interceptação telemática judicial;
- **ABNT NBR ISO 22301:2013**: Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos;
- **ABNT NBR ISO/IEC 27031:2015**; Tecnologia da informação — Técnicas de segurança — Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação;
- **ABNT NBR ISO/IEC 27032:2015**: Tecnologia da Informação — Técnicas de segurança — Diretrizes para segurança cibernética;
- **ABNT NBR ISO/IEC 27037:2013**: Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital;
- **ABNT NBR ISO/IEC 27038:2014**: Tecnologia da informação — Técnicas de segurança — Especificação para redação digital;
- **ABNT ISO/IEC TR 20000-5:2011**: Tecnologia da informação — Gerenciamento de Serviços;
- **ABNT NBR 12896:1993**: Tecnologia de informação — Gerência de senhas — Procedimento;

- **ABNT NBR 12964:1993**: Tecnologia de informação — Técnicas criptográficas de dados — Modos de operação de um algoritmo de cifração de blocos padrão — Padronização;
- **ABNT NBR 9611:1991**: Tecnologia de informação — Código Brasileiro para Intercâmbio de Informação — Padronização;
- **ABNT NBR ISO/IEC 14598-5:2001**: Tecnologia de informação — Avaliação de produto de software;
- **ABNT NBR ISO/IEC 15504-1:2008**: Tecnologia da informação — Avaliação de processo;
- **ABNT NBR ISO/IEC 15504-3:2008**: Tecnologia da informação — Avaliação de processo;
- **ABNT NBR ISO/IEC 15504-4:2008**: Tecnologia da informação — Avaliação de processo;
- **ABNT NBR ISO/IEC 17788:2015**: Tecnologia da informação — Computação em nuvem — Visão geral e vocabulário;
- **ABNT NBR ISO/IEC 20000-1:2011**: Tecnologia da informação — Gestão de serviços;
- **ABNT NBR ISO/IEC 20000-2:2013**: Tecnologia da informação — Gerenciamento de serviços;
- **ABNT NBR ISO/IEC 26300:2008**: Tecnologia da informação — Formato aberto de documento para aplicações de escritório (OpenDocument) v1.0;
- **ABNT NBR ISO/IEC 38500:2009**: Governança corporativa de tecnologia da informação.

A normatização nacional, portanto, prevê que uma determinada desenvolvedora de *softwares*, *hardwares*, aplicativos, enfim, qualquer elemento que venha a produzir algo físico, programa ou conteúdo digital deve se adequar a tais normativas, haja vista que as mesmas são garantidoras de um mínimo padrão de segurança tanto para o usuário, quanto para a empresa ou pessoa que desenvolve um projeto.

Nesse sentido, uma das maneiras de se perceber se um programa ou aparelho é confiável e pode ser adquirido ou instalado com maior segurança dentro das empresas, é a busca ativa pelo número de registro, percepção e análise junto à padronização para saber se a empresa segue adequadamente as normas de segurança estabelecidas pela ABNT, ou seja, essa é uma das garantias imprescindíveis

para que se possam evitar os riscos e trazer uma qualidade maior na prestação de serviços ou produção de insumos para o público.

# CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho demonstrou que a segurança da informação de empresas é uma temática, de fato, essencial e deve ser considerada no planejamento das organizações, para que seja possível estabelecer uma maior segurança por parte das instituições. Esta questão se torna ainda mais importante, considerando que os incidentes ameaçam não apenas pessoas físicas, mas também órgãos importantes para a sociedade, sem os quais seria impossível a adoção das práticas diárias dos cidadãos, tais como as realizações de pagamentos em instituições bancárias, acesso aos dados cadastrais em veículos organizacionais, dentre outros.

Foram destacados aspectos primordiais de alguns incidentes ocorridos, mostrando-se que o comprometimento de informações ocasionou abalo a grandes estruturas locais e a invasão de sistemas comprometeu, também, os sistemas operacionais das empresas. Além disso, todos os envolvidos, direta ou indiretamente, com o exercício da atividade da organização também foram afetados pelas catástrofes, mesmo que não estivessem relacionados diretamente às empresas, o que define que as falhas afetam não apenas uma estrutura comercial, mas também a sociedade que a circunda.

O trabalho apresentou, também, uma breve conceituação a respeito das maiores ameaças e vulnerabilidades das redes de dados, demonstrando quais são os principais riscos e quais as formas de ataques que mais se intensificam na atualidade. Tais informações são de extremo valor uma vez que a maneira mais efetiva de se combater tais ameaças é reconhecendo-as e minimizando seus impactos dentro das organizações.

O CERT.br foi apresentado no decorrer do trabalho, tendo em vista a sua importância para a segurança da informação no Brasil. Dentre as suas responsabilidades, destaca-se a busca frequente por soluções dos principais incidentes que podem vir a surgir e prejudicar o andamento das atividades realizadas a partir do uso dos computadores. Assim, a partir da compreensão dos mecanismos que norteiam o CERT.br, bem como, de suas pesquisas frequentes realizadas na área, as instituições se tornam capazes de reconhecer os desafios da segurança da informação,

bem como, as melhores maneiras de se contornar os problemas detectados pelos riscos de invasões aos sistemas operacionais das organizações.

O trabalho também dissertou a respeito do desenvolvimento das normas de segurança da informação que, por sua vez, permitiu uma análise histórica acerca do tema, bem como, de suas principais características e evoluções. Além disso, também destacou a necessidade de se aperfeiçoar as barreiras contra os ataques que podem prejudicar drasticamente as instituições empresariais.

Considera-se, portanto, que este trabalho é de relevância para o cenário da segurança da informação ao destacar os aspectos fundamentais que devem ser considerados a cerca da segurança da informação em empresas. Técnicas de qualidade que tragam benefícios consideráveis não apenas para uma área restrita da instituição, mas também para todas as etapas de suas atividades, devem ser estabelecidas desde o planejamento até ao fornecimento de seus produtos e/ou serviços aos seus utilizadores/consumidores.

O estudo também é de grande relevância no âmbito acadêmico, considerando que aborda um tema de grande importância e bastante exigido em concursos públicos e demais mecanismos de acesso ao mercado de trabalho. Tendo em vista que o tema é de suma importância para a formação profissional dos estudantes que tem a intenção de atuar nos mais diversos ramos, tal conteúdo é essencial para prepará-los, tanto para o seu prosseguimento na vida estudantil, como também para exercer sua profissão fora dos muros das instituições educacionais, favorecendo uma formação completa do aluno.

Uma proposta para trabalho futuro seriam pesquisas que vislumbrassem o solucionamento das principais vulnerabilidades e ameaças que regem os sistemas digitais da atualidade, trazendo, consigo, a valorização de aspectos que são elementares para que os usuários possam ter plena segurança ao acessar a internet, suas contas bancárias, enfim, todos esses conteúdos digitais sem grandes preocupações com *softwares* e/ou indivíduos maliciosos.

Assim, a temática seria trabalhada, tendo por base os dados levantados por essa pesquisa e, em conjunto, abordariam também alternativas que fossem de encontro com tais necessidades de mercado, uma vez que os utilizadores da rede virtual, também conhecida como internet, não se restringem ao público composto por cidadãos que, basicamente, acessam as redes sociais, mas também estão presen-

tes grandes instituições, governamentais, não governamentais, empresariais, enfim, corporações que necessitam de pesquisas e, inclusive, realizam investimentos para que a segurança de suas informações seja mais bem tratada, de forma que garanta o seu controle tecnológico.

# REFERÊNCIAS BIBLIOGRÁFICAS


1. ESPIRÍTO SANTO, Adrielle F. S. **Segurança da Informação**, 2010, http://www.ice.edu.br/TNX/encontrocomputacao/artigos- internos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf, Acesso em 07 jun. 2013.
2. SÊMOLA, Marcos. **Gestão de riscos da informação é para os fortes**, 2014, http://segurancadainformacao.modulo.com.br/gestao-de-riscos-da-informacao-e-para-os-fortes, Acesso em 08 jun. 2016.
3. G1. **Empresa de Marília tem sistema invadido e bloqueado por Hackers**, 2015, http://g1.globo.com/sp/bauru-marilia/noticia/2015/09/empresa-de-marilia-tem-sistema-invadido-e-bloqueado-por-hackers.html, Acesso em 07 set. 2015.
4. BACOCCOLI, Giuseppe. Geólogo e Professor da Universidade Federal do Rio de Janeiro (UFRJ). **Para analistas, Petrobras sofreu espionagem industrial**, 2008, http://g1.globo.com/Noticias/Economia_Negocios/0,,MUL299380-9356,00-PARA+ANALISTAS+PETROBRAS+SOFREU+ESPIONAGEM+INDUSTRIAL.html, Acesso em 07 set. 2015.
5. GENRO, Tarso. Ministro da Jústiça. **Nota do Ministério da Justiça**, 2008, http://g1.globo.com/Noticias/Mundo/0,,MUL304209-5602,00-ABIN+INVESTIGARA+COM+PF+ROUBO+DE+DADOS+GEOLOGICOS+DA+PETROBRAS.html, Acesso em 08 set. 2015.
6. KASS, Lani. Ex-conselheira do Joint Chiefs of Staff dos EUA sobre questões de segurança. **Hackers 'hit' US water treatment systems**, 2011, http://www.bbc.com/news/technology-15817335, Acesso em 11 set. 2015.
7. PRESIDÊNCIA DA REPÚBLICA. **GUIA DE REFERÊNCIA PARA ASEGURANÇA DAS INFRAESTRUTURASCRÍTICAS DA INFORMAÇÃO**, 2010, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Brazil_2010_Orig_2_Guia_SICI.pdf, Acesso em 10 set. 2015.

8. ROUSSEF, Dilma. Presidente da República. **Discurso em Assembleia-Geral da ONU**, 2013, http://g1.globo.com/mundo/noticia/2013/09/dilma-diz-na-onu-que-espionagem-fere-soberania-e-direito-internacional.html, Acesso em 10 set. 2015.
9. FERREIRA, Aurélio Buarque de Holanda. **Novo Dicionário da Língua Portuguesa, 2ª edição, Editora Nova Fronteira**, 1986.
10. BROWN, Barbara. **O que é comunicação efetiva?**, , http://www.ehow.com.-br/comunicacao-efetiva-sobre_6642/, Acesso em 25 mar. 2016.
11. TZU, Sun. General e Estrategista Chinês. **A Arte da Guerra**, ~ano 400 a.C..
12. LIEIRA, Julio Fernando. **Segurança de Redes - Apostila segurança de Redes de Computadores, Fatec Lins, Lins - SP**, 2012.
13. ARAÚJO, José Iago Pereira. **Integridade, disponibilidade e confidencialidade da informação**, 2011, http://www.dsc.ufcg.edu.br/~pet/jornal/outubro2011/materias/profissoes.html, Acesso em 08 jun. 2016.
14. NOVO, Jorge Procópio da Costa. **Softwares de Segurança da Informação - Curso Técnico em Manutenção e Suporte em Informática**, 2010, http://ead.ifap.edu.br/netsys/public/livros/LIVRO%20MANUTEN %C3%87%C3%83O/Modulo%20III/software_seguran%C3%A7a_informa %C3%A7%C3%A3o.pdf, Acesso em 08 jun. 2016.
15. CGI.br. **Relatório de Políticas de Internet**, 2012, http://www.cgi.br/media/docs/publicacoes/1/relatorio-politicas-internet-pt.pdf, Acesso em 08 jun. 2016.
16. PRESIDÊNCIA DA REPÚBLICA. **DECRETO Nº 4.829, DE 3 DE SETEMBRO DE 2003**, 2003, http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm, Acesso em 08 jun. 2016.
17. CGI.br. **TIC Governo Eletrônico 2013 - Pesquisa Sobre o Uso das Tecnologias da Informação e Comunicação no Setor Público Brasileiro**, , http://cgi.br/media/docs/publicacoes/2/TIC_eGOV_2013_LIVRO_ELETRONICO.pdf, Acesso em 08 jun. 2016.
18. CETIC.br. **TIC Educação 2013 - Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação nas Escolas Brasileiras**, , http://www.cetic.br/media/docs/publicacoes/2/tic-educacao-2013.pdf, Acesso em 08 jun. 2016.

19. CERT.br. **Cartilha de Segurança para Internet**, , http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf, Acesso em 04 abr. 2016.
20. CETIC.br. **TIC Domicílios e Empresas 2013 - Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Brasil**, 2014, http://www.cetic.br/media/docs/publicacoes/2/TIC_DOM_EMP_2013_livro_eletronico.pdf, Acesso em 08 jun. 2016.
21. CARNEGIE MELLON UNIVERSITY. **CERT - Computer Emergency Response Team**, 1988, http://www.cert.org/, Acesso em 08 jun. 2016.
22. CERT.br. **Sobre o CERT.br**, 2016, http://www.cert.br/sobre/, Acesso em 20 mar. 2016.
23. CERT.br. **Estatísticas dos Incidentes Reportados ao CERT.br**, 2016, http://http://www.cert.br/stats/incidentes/, Acesso em 20 mar. 2016.
24. CERT.br. **Incidentes Reportados ao CERT.br - Janeiro a Dezembro de 2015**, 2016, http://http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque.html, Acesso em 20 mar. 2016.
25. ABNT, Associação Brasileira de Normas Técnicas. **Normalização**, , http://www.abnt.org.br/normalizacao/o-que-e/o-que-e, Acesso em 27 mai. 2016.
26. Força Tarefa de Segurança de Computador do Conselho de Defesa e Ciência. **Security Controls for Computer System (U) – Relatório da Força Tarefa de Segurança de Computador do Conselho de Defesa e Ciência**, 1970.
27. DEPARTAMENTO DE DEFESA DOS ESTADOS UNIDOS DA AMÉRICA. **Trusted Computer System Evaluation Criteria**, 1985.
28. BSI, British Standards Institution. **BS7799:1995**, 1995.
29. BSI, British Standards Institution. **BS7799:1999**, 1999.
30. ISO/IEC, International Organization for Standardization / International Electrotechnical Commision. **ISO/IEC 17799:2000 - Information Technology - Code of practice for information security management**, 2000.
31. ISO/IEC, International Organization for Standardization / International Electrotechnical Commision. **ISO/IEC 15408-1:1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model**, 1999.

32. ISO/IEC, International Organization for Standardization / International Electrotechnical Commision. **ISO/IEC 27000:2016(en)Information technology — Security techniques — Information security management systems — Overview and vocabulary**, 2016, https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en, Acesso em 08 jun. 2016.
33. FECOMERCIOSP. **Cartilha - Segurança da Informação para Empresas - Soluções Simples - Grandes Resultados**, , http://www.coaliza.org.br/wp-content/uploads/2014/05/Cartilha-Seguran%C3%A7a-da-Informa %C3%A7%C3%A3o-para-pequenas-empresas.pdf, Acesso em 08 jun. 2016.
34. SANTOS, Diana Luísa Rocha e Silva, Rita Maria Santos. **Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001**, 2012, https://web.-fe.up.pt/~jmcruz/seginf/seginf.1314/trabs-als/final/G4-ISO.27000.final.pdf, Acesso em 08 jun. 2016.
35. ISO, International Organization for Standardization. **ISO Survey 2014**, 2014, http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=BR#standardpick, Acesso em 08 jun. 2016.
36. ABNT, Associação Brasileira de Normas Técnicas. **Pesquise por normas, cursos e publicações ABNT**, , http://www.abnt.org.br/pesquisas/?searchword=seguran%C3%A7a+da+informa%C3%A7%C3%A3o&x=0&y=0, Acesso em 08 jun.2016.
37. ABNT, Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27005 - Tecnologia da Informação - Técnicas de segurança - Gestão de riscos de segurança da informação**, 2011. NORMA BRASILEIRA..

# ANEXO A – EXEMPLOS DE VULNERABILIDADES E AMEAÇAS.

[37]

A tabela abaixo fornece exemplos de vulnerabilidades e possíveis ameaças em diversas áreas de segurança e pode servir de auxílio durante o processo de identificação de potenciais ameaças e vulnerabilidades, assunto abordado no Capítulo 4.

| Tipos | Exemplos de vulnerabilidades | Exemplos de ameaças |
|---|---|---|
| *Hardware* | Manutenção insuficiente ou instalação defeituosa de mídia de armazenamento | Violação das condições de uso do sistema de informação que possibilitam sua manutenção |
| | Falta de uma rotina de substituição periódica | Destruição de equipamento ou mídia |
| | Sensibilidade à umidade, poeira ou sujeira | Poeira, corrosão, congelamento. |
| | Sensibilidade à radiação eletromagnética | Radiação eletromagnética |
| | Inexistência de um controle de mudanças de configuração | Erro durante o uso |
| | Sensibilidade a variações de voltagem | Interrupção do suprimento de energia |
| | Sensibilidade a variações de temperatura | Fenômeno meteorológico |
| | Armazenamento não protegido | Furto de mídia ou documentos |
| | Descuidado durante o descarte | Furto de mídia ou documentos |
| | Utilização de cópias não controladas | Furto de mídias ou documentos |
| *Software* | Inexistência de procedimentos de teste de *softwares*. | Abuso de direitos |

| | | |
|---|---|---|
| *Software* | Falhas conhecidas no *software* | Abuso de diretos |
| | Não execução do "*logout*" ao se deixar uma estação de trabalho | Abuso de direitos |
| | Descarte ou reutilização de mídia de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados | Abuso de direitos |
| | Inexistência de uma trilha de auditoria | Abuso de direitos |
| | Atribuição errônea de direitos de acesso | Abuso de diretos |
| | *Software* amplamente distribuído | Comprometimento dos dados |
| | Utilizar programas aplicativos com um conjunto errado de dados | Comprometimento dos dados |
| | Interface de usuário complexa | Erro durante uso |
| | Inexistência de documentação | Erro durante uso |
| | Parâmetros Incorretos | Erro durante uso |
| | Datas incorretas | Erro durante uso |
| Rede | Inexistência de mecanismos de autenticação e identificação | Forjamento de direitos |
| | Tabelas de senhas desprotegidas | Forjamento de diretos |
| | Gerenciamento mal feito de senhas | Forjamento de direitos |
| | Serviços desnecessários habilitados | Processamento ilegal de dados |
| | *Software* novo ou imaturo | Defeito de *software* |
| | Especificações confusas o incompletas para os desenvolvedores | Defeito de *software* |

| | | |
|---|---|---|
| Rede | Inexistência de um controle eficaz de mudança | Defeito de *software* |
| | *Download* e uso não controlado de *software* | Alteração do *software* |
| | Inexistência de cópias de segurança | Alteração do *software* |
| | Inexistência de mecanismos de proteção física no prédio, portas e janelas | Furto de mídia ou documentos |
| | Inexistência de relatórios de gerenciamento | Uso não autorizado de equipamento |
| | Inexistência de evidências que comprovem o envio ou recebimento de mensagens | Repúdio de ações |
| | Linhas de Comunicação desprotegidas | Escuta não autorizada |
| | Tráfego sensível desprotegido | Escuta não autorizada |
| | Junções de cabeamento mal feitas | Falha do equipamento de telecomunicação |
| | Ponto único de falha | Falha do equipamento de telecomunicação |
| | Não identificação e não autenticação do emissor ou receptor | Forjamento de diretos |
| | Arquitetura insegura da rede | Espionagem à distância |
| | Transferências de senhas em claro | Espionagem a distância |
| | Gerenciamento de rede inadequado, quanto à configuração de roteamentos | Saturação do sistema de informação |
| | Conexões de redes públicas desprotegidas | Uso não autorizado de equipamento |
| Recursos humanos | Ausência de recursos humanos | Indisponibilidade de recursos humanos |

| | | |
|---|---|---|
| Recursos humanos | Procedimentos de recrutamento inadequados | Indisponibilidade de recursos humanos |
| | Treinamento insuficiente em segurança | Erro durante o uso |
| | Uso incorreto de *software* e *hardware* | Erro durante o uso |
| | Falta de conscientização em segurança | Erro durante o uso |
| | Inexistência de mecanismos de monitoramento | Processamento ilegal dos dados |
| | Trabalho não supervisionado de pessoal de limpeza ou de terceirizados | Furto de mídia ou documentos |
| | Inexistência de políticas pra o uso correto de meios de telecomunicação e de troca de mensagens | Uso não autorizado de recurso |
| Local ou instalações | Uso inadequado de mecanismos de controle de acesso físico a locais sensíveis | Destruição de equipamento ou mídia |
| | Localização em área suscetível a inundações | Inundação |
| | Fornecimento de energia instável | Interrupção de suprimento de energia |
| | Inexistência de mecanismos de proteção física no prédio portas e janelas | Furto de equipamentos |
| Organização | Inexistência de um procedimento formal para o registro de remoção de usuários | Abuso de direitos |
| | Inexistência de processo formal para a análise crítica dos direitos de acesso | Abuso de direitos |

| | | |
|---|---|---|
| Organização | Provisões de segurança insuficientes o inexistentes em contratos com clientes e/ou terceiros | Abuso de direitos |
| | Inexistência de procedimentos de monitoramento das instalações de processamento de informações | Abuso de direitos |
| | Inexistência de auditorias periódicas | Abuso de direitos |
| | Inexistência de procedimentos para a identificação e análise/avaliação de riscos | Abuso de direitos |
| | Inexistência de relatos de falha nos arquivos de auditoria das atividades de administradores e operações | Abuso de direitos |
| | Resposta inadequada do serviço de manutenção | Violação das condições de uso do sistema de informação |
| | Acordo de nível de serviço (SLA) inexistência ou ineficaz | Violação das condições de uso do sistema de informação |
| | Controle de mudanças inexistente ou ineficaz | Violação das condições de uso do sistema de informação |
| | Procedimento e controle de sistemas de gerenciamento de segurança inexistentes | Comprometimento dos dados |
| | Atribuição inadequada das responsabilidades pela segurança da informação | Repúdio de ações |
| | Plano de continuidade de serviços inexistente | Falha nos serviços |

| | | |
|---|---|---|
| Organização | Política de uso de e-mail inexistente | Erro durante o uso |
| | Ausência de registros de auditoria (*logs*) | Erro durante o uso |
| | Processo disciplinar no caso de incidentes de segurança inexistente | Furto de equipamentos ou dados |
| | Política de uso de recursos de informática inexistente | Furto de equipamentos ou dados |
| | Inexistência de controle de ativos fora da organização | Furto de equipamentos ou dados |
| | Inexistência de procedimentos de direitos de propriedade intelectual | Uso de cópias de aplicativos falsificadas ou ilegais. |

ANEXO B – FONTES DE AMEAÇAS REPRESENTADAS POR SERES HUMANOS.

[37]

| Fontes de ameaça | Motivação | Possíveis Consequências |
|---|---|---|
| *Hacher*, *cracker* | Desafio<br>Egocentrismo<br>Protesto<br>Rebeldia<br>*Status*<br>Dinheiro | • *Hacking*;<br>• Engenharia social;<br>• Negação de serviço;<br>• Pichação de *sites*;<br>• Invasão de sistemas, infiltrações;<br>• Acesso não autorizado. |
| Criminosos digitais | Destruição de informações<br>Acesso a dados sigilosos<br>Divulgação ilegal de informações<br>Ganho monetário<br>Alterações não autorizadas de dados | • Atos virtuais fraudulentos (interceptação de dados, ataque homem-no-meio, IP *spoofing*, etc.);<br>• Intrusão de sistemas.<br>• Suborno por informação;<br>• Ataques a sistemas (negação de serviço); |
| Terroristas | Chantagem<br>Destruição<br>Vingança<br>Exploração<br>Ganho político<br>Cobertura da mídia | • Ataques com bombas;<br>• Guerra de informação;<br>• Ataques a sistemas (negação de serviço distribuído);<br>• Invasão e dominação de sistemas;<br>• Alteração de sistemas. |
| Espiões | Vantagem competitiva<br>Espionagem econômica | • Garantir vantagem de um posicionamento defensivo;<br>• Garantir uma vantagem política;<br>• Exploração econômica;<br>• Furto de informações;<br>• Violação da privacidade das pessoas; |

| | | |
|---|---|---|
| Espiões | | • Engenharia social;<br>• Invasão de sistemas;<br>• Invasão de privacidade;<br>• Acessos não autorizados em sistemas (acesso a informação restrita, de propriedade exclusiva, e/ou relativa à tecnologia). |
| Pessoas: mal treinadas, insatisfeitas, mal-intencionadas, negligentes, imprudentes, desonestas, demitidas. | Curiosidade<br>Egocentrismo<br>Informações para serviço de Inteligência<br>Ganhos financeiros<br>Vingança<br>Ações não intencionais ou omissões (erro na entrada de dados, erro na programação). | • Agressão a funcionário;<br>• Chantagem;<br>• Busca de informação sensível;<br>• Abuso dos recursos computacionais;<br>• Fraudes;<br>• Furto de ativos;<br>• Suborno de informação;<br>• Inclusão de dados falsos;<br>• Corrupção de dados;<br>• Interceptação de informação;<br>• Desvio de informação;<br>• Uso de programas ou códigos maliciosos;<br>• Sabotagens;<br>• Invasão de sistemas;<br>• Acessos não autorizados a sistemas. |