Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Aplicadas
Departamento de Computação e Sistemas

Projetos e Avanços que podem Impactar na Segurança Digital

Gildomar Gonçalves Dias

TRABALHO DE CONCLUSÃO DE CURSO

ORIENTAÇÃO:
Diego Zuquim Guimarães Garcia

Janeiro, 2018
João Monlevade–MG

Gildomar Gonçalves Dias

Projetos e Avanços que podem Impactar na Segurança Digital

Orientador: Diego Zuquim Guimarães Garcia

Monografia apresentada ao curso de Sistemas de Informação do Instituto de Ciências Exatas e Aplicadas, da Universidade Federal de Ouro Preto, como requisito parcial para aprovação na Disciplina "Trabalho de Conclusão de Curso II".

Universidade Federal de Ouro Preto

João Monlevade

Janeiro de 2018

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS
COLEGIADO DO CURSO DE SISTEMAS DE INFORMAÇÃO

Curso de Sistemas de Informação

FOLHA DE APROVAÇÃO DA BANCA EXAMINADORA

Projetos e Avanços que podem Impactar na Segurança Digital

Gildomar Gonçalves Dias

Monografia apresentada ao Instituto de Ciências Exatas e Aplicadas da Universidade Federal de Ouro Preto como requisito parcial da disciplina CSI499 – Trabalho de Conclusão de Curso II do curso de Bacharelado em Sistemas de Informação e aprovada pela Banca Examinadora abaixo assinada:

Prof. Dr. Diego Zuquim Guimarães Garcia
Departamento de Computação e Sistemas - UFOP

Prof. Me. Erik de Britto e Silva
Departamento de Computação e Sistemas - UFOP

Prof. Me. Theo Silva Lins
Departamento de Computação e Sistemas - UFOP

João Monlevade, 31 de janeiro de 2018

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS
COLEGIADO DO CURSO DE SISTEMAS DE INFORMAÇÃO

ATA DE DEFESA

Aos 31 dias do mês de janeiro de 2018, às 17 horas e 00 minutos, na sala C203 do Instituto de Ciências Exatas e Aplicadas, foi realizada a defesa de Monografia pelo aluno **Gildomar Gonçalves Dias,** sendo a Comissão Examinadora constituída pelos professores: Prof. Dr. Diego Zuquim Guimarães Garcia, Prof. Me. Erik de Britto e Silva e Prof. Me. Theo Silva Lins.

O candidato apresentou a monografia intitulada: *"Projetos e Avanços que podem Impactar na Segurança Digital"*. A comissão examinadora deliberou, por unanimidade, pela aprovação do candidato, com nota 9,5 (Nove e Meio), concedendo-lhe o prazo de 15 dias para incorporação das alterações sugeridas ao texto final.

Na forma regulamentar, foi lavrada a presente ata que é assinada pelos membros da Comissão Examinadora e pelo graduando.

João Monlevade, 31 de janeiro de 2018.

Prof. Dr. Diego Zuquim Guimarães Garcia
Professor Orientador/Presidente

Prof. Me. Erik de Britto e Silva
Professor Convidado

Prof. Me. Theo Silva Lins
Professor Convidado

Gildomar Gonçalves Dias
Graduando

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS
COLEGIADO DO CURSO DE SISTEMAS DE INFORMAÇÃO

TERMO DE RESPONSABILIDADE

Eu, Gildomar Gonçalves Dias,
declaro que o texto do trabalho de conclusão de curso intitulado "Projetos e Avanços que podem Impactar na Segurança Digital" é de minha inteira responsabilidade e que não há utilização de texto, material fotográfico, código fonte de programa ou qualquer outro material pertencente a terceiros sem as devidas referências ou consentimento dos respectivos autores.

João Monlevade, 31 de janeiro de 2018

Gildomar Gonçalves Dias
Assinatura do aluno

Este trabalho é dedicado à todos os apaixonados pelos avanços em Segurança digital. Em especial a minha Mãe (Terezinha Rodrigues Dias), a minha namorada (Yara Dias), aos meus familiares, amigos e ao professor orientador (Diego Zuquim), pelo apoio e incentivo.

Agradecimentos

Agradeço primeiramente minha Mãe, Terezinha Rodrigues Dias, que me deu todo o apoio, carinho e suporte familiar necessários. Mesmo com todas as dificuldades sempre me fez crer que um dia eu chegaria onde cheguei, tornando esse sonho possível. Agradeço também a minha namorada, Yara Fátima Dias, minha princesa e eterna incentivadora de sucesso. Ao Thales Delfino, funcionário exemplar da Secretaria do Colegiado da UFOP, que me auxiliou no momento em que eu mais precisava na tomada de Decisão me fazendo enxergar que tudo iria dar certo neste trabalho de conclusão de curso. A D. Maria Miranda e familiares, que me cederam moradia durante minha formação acadêmica. Aos meus familiares e amigos, que me acolheram e ampararam sempre que eu precisei. A UFOP pelo ensino público, gratuito e de qualidade oferecido. Ao PRACE/NACE por todo apoio oferecido a mim, como aluno desta instituição. E também a todos que participaram da minha formação, direta ou indiretamente, o meu muito obrigado.

"Nossos esforços nos levará onde os acomodados nunca conseguiram chegar."

— Gildão (2018),
no: Brasil.

Resumo

O trabalho propõe o estudo dos Projetos e Avanços que podem impactar na Segurança Digital, no que diz respeito à realização de avaliações de segurança dos sistemas digitais. Seu objetivo é elaborar um estudo do que tem sido feito para melhorar a eficiência da segurança digital nos sistemas e componentes nela existentes de maneira prática e objetiva. Através da análise dos Princípios de Segurança Física e Lógica em Sistemas Digitais, são estudadas as técnicas e projetos para garantir a segurança, utilizada nesses tipos de sistemas. Essas técnicas podem ser usadas de maneira isolada ou reunida, formando um único conjunto capaz de garantir a segurança. Para que esse estudo seja completo, são apresentados os principais conceitos e aspectos referentes aos Sistemas de Informação quanto à segurança sem falhas e interrupções.Também são definidos os significados de alguns termos técnicos utilizados nessa área. Com isso, espera-se propor uma solução de seguranças físicas e logicas garantindo a efetiva defesa de ameaças futuras.

Palavras-chaves: projetos. avanços. impactar. segurança digital. solução. ameaças.

Abstract

The work proposes the study of the Projects and Advances that can impact in the Digital Security, with respect to the accomplishment of evaluations of security of the digital systems. Its purpose is to elaborate a study of what has been done to improve the efficiency of digital security in systems and components therein in a practical and objective manner. Through the analysis of the Principles of Physical and Logical Security in Digital Systems, the techniques and projects to guarantee the safety used in these types of systems are studied. These techniques can be used in isolation or in combination, forming a single set capable of ensuring safety. In order for this study to be complete, the main concepts and aspects related to Information Systems regarding safety without failures and interruptions are presented. Also the meanings of some technical terms used in this area are defined. With this, it is hoped to propose a solution of physical and logical security, guaranteeing the effective defense of future threats.

Key-words: projects. advances. impacts. security. solution. threats.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ABNT Associação Brasileira de Normas Técnicas

ACPO Associação de Oficiais Chefes de Polícia do Reino Unido

AES *Advanced Encryption Standard*

CD-ROM *Compact Disc Read-Only Memory*

CEH *Certified Ethical Hacker*

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

CISSP *Certified Information Systems Security Professional*

CISA *Certified Information Systems Auditor*

CISM *Certified Information Security Manager*

CobIT *Control Objectives for Information and Related Technology*

CompTIA *Computing Technology Industry Association*

CP Código Penal

CPD Centro de Processamento de Dados

DDoS *Distributed Denial of Service*

3DES *3 Data Encryption Standard*

DNA Ácido Desoxirribonucleico

DSI Departamento de Segurança da Informação

DSL *Digital Subscriber Line*

DVD *Digital Versatile Disc*

ECA Estatuto da Criança e do Adolescente

ECC Criptografia de Curvas Elípticas

EC-Council *International Council of Electronic Commerce Consultants*

GSEC *GIAC Security Essentials*

GSM Sistema Global para Comunicações Móveis

GTI Governança de Tecnologia da Informação

HTML *HyperText Markup Language*

HTTPS *Hyper Text Transfer Protocol Secure*

IDEA *International Data Encryption Algorithm*

IEC Comissão Eletrotécnica Internacional

IoT *Internet of Things*

IRC *Internet Relay Chat*

ISACA *Information Systems Audit and Control Association*

ISO *International Organization for Standardization*

ITGI *IT Governance Institute*

ITIL *Information Technology Infrastructured Library*

LAN *Local Area Network*

MD5 *Message-Digest algorithm 5*

NBR Norma Brasileira

NIC.br Comitê Gestor da Internet no Brasil

P2P *Peer-to-peer*

RAID *Redundant Array of Independent Disk*

RC4 *Rivest Cipher 4*

ROI *Return of Investment*

RSA *Rivest Shamir Adleman*

SGSI Sistema de Gestão em Segurança da Informação

SI Sistemas de Informação

SSH *Secure Shell*

SWGDE Grupo de Trabalho Científico em Evidências Digitais

TCP *Transmission Control Protocol*

TI Tecnologia da Informação

URL *Uniform Resource Locator*

USA *United States of America*

USB *Universal Serial Bus*

WEP *Wired Equivalent Privacy*

WMI Instrumentação de Gerenciamento do Windows

WPA2 *Wi-Fi Protected Access 2*

Sumário

1 Introdução

O presente estudo apresenta um vasto campo para o desenvolvimento de pesquisas, no qual, são apresentados projetos e avanços que podem impactar na Segurança Digital. Diante de tal fato, se fez necessário fornecer ao leitor um texto condensado que permita relacionar os conceitos fundamentais abordados ao que há de mais moderno e avançado em projetos de segurança digital, abrangendo assim, a segurança física e lógica em Sistemas de Informação.

A partir do aprofundamento dos conceitos fundamentais e seus aspectos, dos princípios de Segurança Física e Lógica, das técnicas de garantia da segurança utilizadas nos sistemas digitais, é possível ainda, identificar pontos essenciais e distintos, que viabilizem o auxílio às necessidades do atual cenário corporativo, uma vez, que nota-se, a imprescindibilidade quanto à implantação de ferramentas eficazes na identificação, quantificação e até mesmo a minimização de possíveis falhas de segurança.

Para isto, se fazem necessários investimentos mais eficazes em relação aos recursos humanos, técnicos e econômicos que incidirão de maneira direta em aspectos essenciais à implantação de projetos, quanto à definição de requisitos de segurança, implementação dos sistemas e análise de segurança.

Desta forma, o presente estudo tem como objetivo abordar os principais conceitos e aspectos dos Sistemas de Informação, bem como apresentar as terminologias utilizadas, explanar sobre as técnicas de proteção que inviabilizam as possíveis fragilidades do sistema, os mecanismos de redundância no controle, cuja finalidade é manter o sistema em constante funcionamento, através do emprego de circuitos comparadores de saída.

Outros fatores relevantes a serem considerados como objetos deste estudo, são: a importância do desenvolvimento de softwares que utilizam de maneira intensiva os diagnósticos de programação defensiva, cujo intuito é a eliminação de erros e a produção de um programa mais robusto, e discorre ainda, sobre técnicas avançadas de identificação, codificação e autenticação e técnicas de segurança na comunicação das informações através de protocolos, criptografia e firewalls.

A realização deste estudo justifica-se, portanto, devido à relevância da segurança quanto às atividades desenvolvidas e disponibilizadas pela área de tecnologia da informação, considerando que mesmo as ferramentas de segurança utilizadas atualmente, ainda apresentam certa fragilidade.

Sendo assim, as justificativas deste documento estão diretamente ligadas aos Princípios de Segurança Física e Lógica em Sistemas de Informação, ou seja, quais Projetos

e Avanços que podem Impactar na Segurança Digital.

A motivação quanto a este tema, está relacionado à importância de implantação de Sistemas de Informação mais seguros, pois esses sistemas computacionais não podem apresentar falhas, visto que essa tecnologia aliada a especialistas altamente capacitados, torna-se uma ferramenta de potencial elevado, capaz de evitar erros que possam comprometer as atividades organizacionais, sustentáveis e por que não dizer a própria vida, reduzindo assim, o risco de aplicação a um nível aceitável.

Um fator de grande relevância refere-se aos Sistemas de Informação Critico, no qual, uma mínima falha pode ocasionar um desastre, gerando inúmeras mortes e prejuízos econômicos. Como exemplo de Sistemas de Informação Critico podem ser citadas usinas nucleares, plantas químicas e petroquímicas, aviação (aeroviários), sistemas ferroviários e metroferroviários, armas de guerra, equipamentos médicos utilizados para tratamento de pacientes e sistemas financeiros (bancários, bolsas de valores).

Por esta razão, são descritos ao longo deste estudo os principais conceitos envolvidos na segurança dos sistemas, a importância da existência de uma cultura organizacional voltada ao tema em questão e o aspecto vital de se desenvolver requisitos diretamente relacionados à segurança.

Em seguida, são descritas as tecnologias utilizadas para sua implementação, bem como os principais tipos de aplicação desses sistemas, citando as técnicas de armazenamento, recuperação de dados e backup, utilização das normas internacionais e nacionais de segurança da informação, considerando que os objetivos de segurança variam de acordo com o tipo de ambiente computacional e a natureza do sistema seja administrativo, financeiro, militar.

Segundo (DIAS, 2000) os principais objetivos de segurança aos quais os usuários e profissionais da área de inforática devem estar atentos são:

- **Confidencialidade ou privacidade** - proteger as informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação, isto é, as informações e processos são liberados apenas a pessoas autorizadas;
- **Integridade de dados** - evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação;
- **Disponibilidade** - proteger os serviços de informática de tal forma que não sejam degradados ou tornados indisponíveis sem a devida autorização. Para um usuário autorizado, um sistema não disponível, quando se necessita dele, pode ser tão ruim quanto um sistema inexistente ou destruído;
- **Consistência** - certificar-se de que o sistema atua de acordo com as expectativas dos usuários autorizados;

- **Isolamento ou uso legítimo** - regular o acesso ao sistema. O acesso não autorizado é sempre um problema, pois além de ser necessário identificar quem acessou e como, é preciso se certificar de que nada importante do sistema foi adulterado ou apagado;
- **Auditoria** - proteger os sistemas contra erros e atos maliciosos cometidos por usuários autorizados. Para identificar os autores e suas ações, são utilizadas trilhas de auditoria e logs, que registram tudo que foi executado no sistema, por quem e quando;
- **Confiabilidade** - garantir que, mesmo em condições adversas, o sistema atuará conforme o esperado.

1.1 O problema de pesquisa

A problemática deste estudo está no aumento das ocorrências de ataques aos sistemas digitais, e em quais os avanços e aprimoramentos em relação às medidas e projetos quanto à defesa patrimonial, uma vez que inicialmente os ataques cibernéticos eram realizados apenas por diversão ou simplesmente para provar algum tipo de conhecimento técnico, cenário este que sofreu uma grande alteração, visto que, atualmente grande parte dos ataques tem como objetivo a obtenção de vantagens financeiras, além de serem realizados por criminosos especializados.

A Segurança da Informação é uma preocupação constante tanto para as organizações quanto para os usuários comuns. Uma das possíveis consequências para a evolução tecnológica está associada ao crescimento de ataques cibernéticos, pois, os processos e recursos tornam-se alvos de grande interesse.

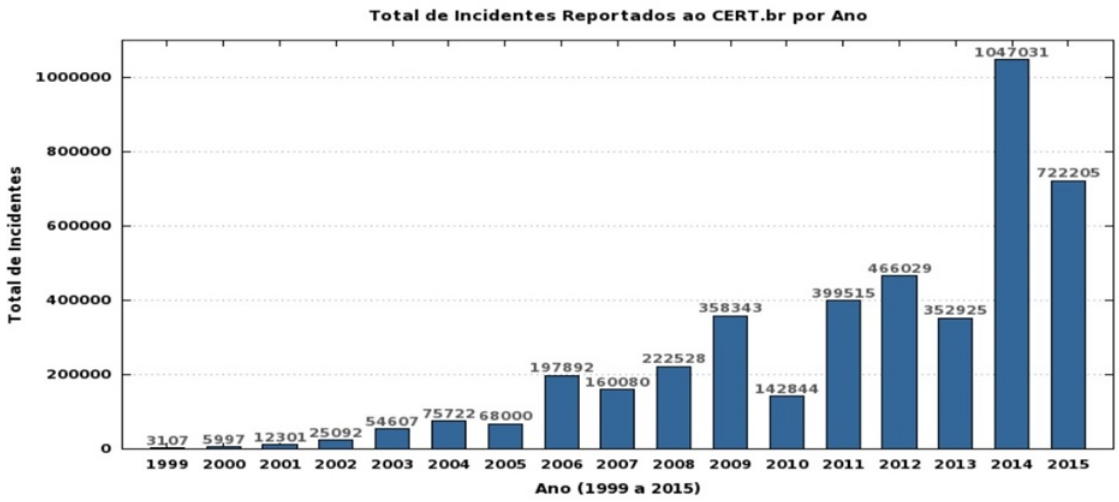
No entanto, mesmo diante desta evolução, os ativos tecnológicos podem conter vulnerabilidades e as informações podem ser roubadas sem que ninguém tome ciência, por isso, a proteção dos dados e a utilização de ferramentas que impossibilitem qualquer tipo de invasão se fazem tão necessárias.

As organizações estão sujeitas a ataques constantemente, o que pode ser visualizado através da figura 1, que apresenta o gráfico de Estatísticas dos Incidentes Reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), mantido pelo Comitê Gestor da Internet no Brasil (NIC.br), e que atende a qualquer rede brasileira conectada à Internet.

É possível observar que os incidentes tendem a crescer a cada ano e que o ano de 2014 foi o mais significativo. Em virtude disso, é provável que a redução no ano de 2015 seja justificada pela alta incidência no ano anterior.

Os ataques ou invasões são inerentes a todo e qualquer sistema, como é possível observar em sites que monitoram em tempo real os diversos ataques *hackers* no mundo,

Figura 1 – Estatísticas dos Incidentes Reportados ao CERT.br



Fonte: CERT.br (2017)

como por exemplo, pode-se citar a Norse Corp <http://map.norsecorp.com> na figura 2, da HP <http://hp.ipviking.com/>, da Karpersky <https://cybermap.kaspersky.com/>, da operadora de telefonia Deutsche Telekom <http://www.sicherheitstacho.eu/>, dentre outros.

Figura 2 – Pagina da Norse Corp, registrando os ataques vituais em tempo real

Fonte: Norse Corp (2017)

Essas organizações dispõem de diferentes tipos de avaliações ou auditorias de segurança para avaliar o nível de segurança de seus sistemas, dentre elas podemos citar:

- Aquisição de Informações;
- Análise de Tráfego;
- Análise de Senhas;
- *Wireless Hacking*;
- *Scanner* de Vulnerabilidades;
- *Scanner* de Aplicação Web;
- *Scanner* de rede.

Sendo assim, a proposta a ser discutida é a criação e avaliação de situações relacionadas a projetos e avanços que podem impactar na segurança digital, bem como definir quais as decisões a ser tomadas e em tempo hábil. Além disso, serão demonstradas possíveis soluções a serem adotadas na segurança dos sistemas, cujo intuito é evitar os problemas ocasionados pelas falhas de segurança, correlacionando-os aos ganhos econômicos gerados por sistemas mais seguros.

1.2 Objetivos

O presente estudo consiste no desenvolvimento de análises acerca das condutas adotadas quanto a realização de projetos e avanços voltados a defesa e mecanismos que proporcionem a segurança digital. Diversas são as categorias de avaliações de segurança dos sistemas digitais, e por isso, optou se por um estudo mais apurado da defesa e impactos de ameaças de maneira prática e objetiva.

Este trabalho possui aos seguintes objetivos específicos:

- Observar dos critérios particulares dos projetos ligados a segurança digital acerca de parâmetros e resultados da segurança dos sistemas digitais;
- Planejar e realizar pesquisas nos avanços da aplicações de segurança;
- Definir as estratégias para que as empresas possam defender seus bens de possíveis ataques ou ameaça;
- Analisar e discutir os resultados obtidos, além de identificar possíveis melhorias e considerações gerais sobre o processo.

1.3 Metodologia

O objeto de pesquisa deste trabalho é propor o estudo dos projetos e avanços que podem impactar na segurança digital, cuja finalidade é a realização de avaliações de segurança dos sistemas digitais. O objetivo é elaborar um estudo das ações adotadas para melhorar a eficácia da segurança digital nos sistemas e componentes nela existentes de maneira prática e objetiva.

Para isso, se fez necessário saber quais são os ataques mais frequentes utilizados pelos hackers na exploração de vulnerabilidade digital. Com isso, espera-se propor uma solução de seguranças físicas e logicas garantindo a efetiva defesa de ameaças futuras.

Os passos para execução deste trabalho são assim definidos:

- Revisão da literatura: apresenta uma revisão da literatura, bem como trabalhos correlatos;
- Desenvolvimento: mostra e descrever o desenvolvimento deste trabalho;
- Resultados: descrever os resultados obtidos relacionados a esse estudo;
- Conclusão: por meio de Análise e discussão do tema apresentado;

1.4 Organização do trabalho

O restante deste trabalho é organizado como se segue: O Capítulo 2 apresenta uma revisão da literatura, bem como trabalhos correlatos, aliados aos projetos e avanços que podem impactar na segurança digital. Discorre ainda, sobre a **Análise Forense**, através da qual, são expostos os princípios e boas práticas sugeridos pela Associação de Oficiais Chefes de Polícia do Reino Unido (ACPO) e pelo Grupo de Trabalho Científico em Evidências Digitais (SWGDE).

São realizadas análises sobre a **Segurança Digital** e as três tecnologias estratégicas: inteligência, digitalização e rede mesh ou rede de malha, sendo abordados ainda, os tipos de ataques mais comuns e os *Cybercrimes* ou Crimes Digitais demostrados com alguns relatos de ocorrências.

E por fim, como complemento foi anexado um Estudo de caso realizado pelo (OLHAR DIGITAL, 2016), que retrata detalhadamente sobre o interior e procedimentos adotados pelo Data Center da empresa de tecnologia **Level 3**, localizado em Cotia.

O Capítulo 3 descreve o desenvolvimento do trabalho mostrando os projetos e avanços que podem impactar na segurança digital, observamdo os critérios particulares dos projetos ligados a segurança e os parâmetros e resultados alcançados. Mostra também os

avanços da aplicações de segurança proposta e define as estratégias para que as empresas possam defender seus bens de possíveis ataques ou ameaças. Abordando temas ligados a:

- Seção 3.1, Controle de Acesso realizados de duas maneira (segurança lógica e física),
- Seção 3.2, Criptografia (de chave simétrica e de chaves assimétricas) e ataques *Cryptomalware*.
- Seção 3.3, Controle de Informações em Sistemas, com gerenciamento de volumes crescentes de dados e conteúdos, combinados com a necessidade de fornecer informações confiáveis
- Seção 3.4, *Backups* na recuperação e conservação das informações. E os tipos ou maneiras mais modernas de realização dos *Backups*, tipos: *Redundant Array of Independent Disk* (RAID) e *Cloud Storage*.
- Seção 3.5, Estudo da Programação Defensiva, onde são realizados testes na busca de defeitos e falhas de implementação e/ou especificação visando garantir a funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade dos sistemas e portais.
- Seção 3.6, Redundância, onde usa-se módulos redundantes, na arquitetura dos projetos em segurança digital, que apresenta quatro formas distintas que são: a **redundância de *hardware***, **de *software***, **de informação** e **redundância temporal**.
- Seção 3.7, Análises e medidas a serem adotadas, na criação um Manual de Normas e Procedimentos de Segurança Física e Lógicas em Sistemas de Informação.
- Seção 3.8, Estudo das Ferramenta para *PenTests* e Auditorias.
- Seção 3.9, Certificações de segurança mais exigidas pelas empresas e profissionais de Segurança da Informação.
- Seção 3.10, Estudo das Normas técnicas de segurança digitais brasileiras e internacionais mais utilizadas. Como auxiliadoras das normas técnicas temos também as melhores práticas que trazem Benefícios gerando impacto na Segurança Digital e retratando temas contemplados na Governança de Tecnologia da Informação (GTI), onde destacam-se o **CobIT** - *framework* e o **ITIL** - Composta por 5 livros.
- Seção 3.11, Projetos e Avanços das leis voltadas aos *Cybercrimes* no Brasil, que podem impactar na Segurança Digital.

No Capítulo 4, são analisados e discutidos os resultados obtidos nesse trabalho, além de identificar possíveis melhorias e considerações gerais sobre os Projetos e Avanços que podem impactar na Segurança Digital.

E por fim, o Capítulo 5, apresenta a conclusão que esse estudo apresentou em relação aos Projetos e Avanços que podem impactar na Segurança Digital.

2 Revisão bibliográfica

Neste capítulo, é apresentada uma revisão da literatura, bem como trabalhos correlatos, em que foram realizados estudos sobre os Projetos e Avanços que podem impactar na Segurança Digital. Para isso, foram coletados todos os pontos de maior relevância, através de pesquisas realizadas em livros, artigos e sites, cujos levantamentos mais pertinentes serão apresentados a seguir.

2.1 Análise Forense

Os Projetos e Avanços que podem impactar na Segurança Digital, na Análise Forense, podem ser evidenciados nos procedimentos adotados pelos peritos digitais, na conservação das provas ou evidencias digitais. Segundo (REIS; GEUS, 2002), "o processo de investigação forense, seja para fins judiciais ou corporativos, deve garantir a autenticidade e integridade das evidências coletadas e dos resultados produzidos", ou seja, a investigação forense deve assegurar que as informações obtidas não sejam alteradas ou contaminadas pelo processo de investigação.

Segundo (REIS; GEUS, 2002) os arquivos de log potencialmente representam a fonte de informação mais valiosa sobre as atividades do sistema. Tais arquivos podem registrar, entre outras informações, as atividades dos usuários, dos processos e do sistema, as conexões e atividades da rede, e informações específicas dos aplicativos e serviços.

Conforme as considerações de (REIS; GEUS, 2002), alguns princípios e boas práticas são sugeridos pela Associação de Oficiais Chefes de Polícia do Reino Unido (ACPO) e pelo Grupo de Trabalho Científico em Evidências Digitais (SWGDE). Alguns desses princípios, são:

- As ações tomadas durante a investigação forense não devem alterar as evidências;
- Qualquer ação que tenha o potencial de alterar, danificar ou destruir qualquer aspecto da evidência original deve ser conduzida por uma pessoa qualificada (por exemplo, quando a evidência original precisa ser acessada para coleta de informações voláteis ou para a criação de imagens);
- O investigador não deve confiar cegamente no sistema invadido, nem nos programas e bibliotecas dinâmicas nele encontrados;
- cópias das evidências originais devem ser produzidas e, sempre que possível, a investigação deve ser conduzida sobre as cópias. Tais cópias devem ser idênticas às evidências originais, contendo toda a informação em seu estado original;

- todas as evidências digitais coletadas e as cópias produzidas devem ser autenticadas por meio de assinaturas criptográficas, permitindo a verificação de sua integridade;
- toda evidência coletada deve ser identificada, contendo o número do caso investigado, uma breve descrição da evidência e a data e horário da coleta;
- toda evidência coletada deve ser preservada em local de acesso controlado e livre de alterações;
- todas as informações relativas à investigação (atividades relacionadas à aquisição, armazenamento, análise ou transferência das evidências, anotações e observações do investigador e os resultados produzidos) devem ser documentadas de maneira permanente e devem estar disponíveis para revisão. A documentação das ações executadas e dos resultados obtidos deve ser feita em relatórios minuciosos, contendo detalhes que incluem as versões das ferramentas utilizadas, os métodos empregados para coleta e análise das evidências e explicações que fundamentam a utilização desses métodos. Desse modo, outro investigador deve ser capaz de examinar as informações documentadas e chegar as mesmas conclusões;
- A cadeia de custódia das evidências coletadas deve ser mantida, documentando a jornada completa de cada evidência durante a investigação. Devem ser relatadas, entre outras informações, o nome da pessoa que coletou a evidência, como, onde e quando foi feita a coleta, o nome do investigador que está a de posse da evidência, data e horário de retirada e devolução da evidência e as atividades executadas pelo investigador;
- As ferramentas usadas na investigação (hardware e software) devem ser amplamente aceitas na área e testadas para garantir sua operação correta e confiável. Além disso, elas devem ser conhecidas em cada detalhe para evitar implicações inesperadas na evidência analisada;
- Os procedimentos devem ser aceitos pela comunidade científica relevante ou suportados por demonstrações da precisão e confiabilidade das técnicas aplicadas;
- Os procedimentos devem ser revistos periodicamente para garantir sua contínua adaptabilidade e eficácia em relação às evoluções tecnológicas;
- O investigador deve ser responsável pelos resultados da investigação e pelas evidências enquanto estiverem em sua posse;
- A pessoa responsável pela investigação deve assegurar o cumprimento dos procedimentos e protocolos estabelecidos.

2.2 Segurança Digital

Em relação as tendencias do tema em questão, tem-se como preocupação o grande aumento de dispositivos na rede de computadores. Como visto na publicação "Como três tendências estratégicas vão impactar a Segurança da Informação", no site <http://www.datacenterdynamics.com.br>, no site (DATACENTER DYNAMICS, 2017), onde o sócio-diretor da (IBLISS DIGITAL SECURITY, 2017) Leonardo Militelli, fala sobre as três tecnologias estratégicas: inteligência, digitalização e rede mesh ou rede de malha (padrão 802.11, tráfego de dados e voz, a cabo ou infraestrutura *wireless*), que deverão impactar os investimentos em segurança nos anos atuais.

"Os líderes de segurança terão de criar *frameworks* de segurança estratégicos para superar as necessidades relacionadas às tecnologias em ascensão. As soluções mais tradicionais de segurança de proteção do perímetro, mesmo sendo importantes, não são suficientes para garantir a continuidade do negócio nesse cenário", afirma Leonardo Militelli, (IBLISS DIGITAL SECURITY, 2017), no site (DATACENTER DYNAMICS, 2017).

Inteligência artificial e aprendizado de máquina: "O aprendizado de máquina permite que ferramentas de segurança coletem e analisem dados de outras soluções de segurança e fontes diversas para criar imagens de ataque e prever as próximas ações maliciosas. No setor financeiro, por exemplo, as empresas poderão usar isso para acompanhar transações e estabelecer modelos preditivos para identificar fraudes", Leonardo Militelli, (IBLISS DIGITAL SECURITY, 2017), no site (DATACENTER DYNAMICS, 2017).

Digitalização ou Gêmeos digitais: como citado por (DATACENTER DYNAMICS, 2017) no site <http://www.datacenterdynamics.com.br>, os gêmeos digitais usam dados físicos de objetos que operam e respondem ao ambiente, bem como informações de sensores, para analisar e simular condições do mundo real, responder a mudanças, melhorar operações e agregar valor ao negócio.

"Imagine, por exemplo, uma empresa responsável por peças de aeronaves. A organização pode coletar dados de voos para prever os danos em seus componentes e a necessidade de manutenção sem ter que se dar ao trabalho de inspecionar as peças com tanta frequência", explica Leonardo Militelli, (IBLISS DIGITAL SECURITY, 2017), no site (DATACENTER DYNAMICS, 2017).

Arquitetura de segurança adaptativa (rede mesh): "As empresas não podem mais depender apenas de mecanismos de prevenção, pois os hackers estão aumentando seu nível de sofisticação para encontrar novas vulnerabilidades. Uma arquitetura adaptativa vai além, pois consiste em múltiplas camadas de segurança, das quais o monitoramento e as ferramentas de analytics são os principais componentes", explica Leonardo Militelli, (IBLISS DIGITAL SECURITY, 2017), no site (DATACENTER DYNAMICS, 2017).

2.3 Tipos de Ataques

Os Projetos e Avanços que podem impactar na Segurança Digital, sempre estão direcionados a todos os possíveis tipos de ataques para que seja possível criar sistemas mais seguros e dentro de um padrão de qualidade que possa garantir a segurança nos dados dos usuários.

Segundo o (ITGI, 2017), O *IT Governance Institute* (ITGI), <www.itgi.org> foi criado em 1998 para promover o pensamento internacional e padrões de direção e controle de tecnologia de informação de uma empresa. Uma governança de TI eficaz ajuda a garantir que A Tecnologia da Informação (TI) suporta os objetivos comerciais, otimiza o investimento empresarial em TI e administra adequadamente os riscos relacionados à TI e oportunidades. O IT Governance Institute oferece simpósios, pesquisas originais e estudos de caso para ajudar líderes empresariais e conselhos de administração nas suas responsabilidades de governança de TI.

Conforme (ITGI, 2017), o IT Governance Institute (ITGI) é o autor de ***COBIT Security Baseline — An Information Security Survival Kit***, ou seja, um Kit de Sobrevivência de Segurança da Informação, que cobre assuntos de segurança relacionados à: Usuários domésticos, Usuários Profissionais, Gerentes, Executivos, Executivos seniores e Boards of Direct. Onde o (ITGI, 2017), faz um resumo dos riscos de segurança técnica aos quais estamos expostos aos ataques:

- ***Trojan***: Programas de cavalo de Tróia são uma maneira comum para os intrusos enganar o usuário (às vezes referido como "**Engenharia social**") para instalar programas de "*back door*" ou "porta traseira", que podem permitir acesso intrusos de fácil acesso para o computador do usuário sem o seu conhecimento, mudando as configurações do sistema ou infectando o computador.

- **Programas de porta traseira e administração remota** (*Back door and remote administration programs*): Nos computadores que utilizam um sistema operacional *Windows*, os invasores costumam usar três ferramentas - *Back Orifice, Netbus e SubSeven* - para obter acesso remoto ao computador. Estes programas de porta traseira ou de administração remota, uma vez instalados, permitem que outras pessoas acessem e controlem o computador.

- **Ataques de negação de serviço** (*Denial-of-service attacks*): Este tipo de ataque faz com que o computador falhe ou se torne tão ocupado processando dados que o usuário não consegue usá-lo.

- **Ser um intermediário para outro ataque** (*Being an intermediary for another attack*): Os intrusos frequentemente usam computadores comprometidos para atacar outros sistemas. O uso de ferramentas distribuídas de negação de serviço,

Distributed Denial of Service (DDoS), é um exemplo disso. Os intrusos instalariam um "agente"(frequentemente através de um programa de cavalo de *Tróia*) que é executado no computador comprometido, aguardando instruções adicionais. Então, quando muitos agentes estão sendo executados em diferentes computadores, um único "manipulador"pode instruí-los a lançar um ataque de negação de serviço em outro sistema. Assim, o alvo final do ataque não é o computador do usuário original, que é apenas uma ferramenta conveniente em um ataque maior.

- **Partilhas de redes *Windows* desprotegidas** (*Unprotected Windows networking shares*): Os intrusos podem explorar compartilhamentos de rede de *Windows* desprotegidos de forma automática para colocar ferramentas em um grande número de computadores baseados no *Windows* conectados à Internet. Como a segurança do site na Internet é interdependente, um computador comprometido não só cria problemas para o proprietário do computador, mas também é uma ameaça para outros sites na Internet.

- **Código móvel** (*Java/JavaScript/ActiveX*) - Mobile code: Houve relatos de problemas com "código móvel"(por exemplo, *Java, JavaScript e ActiveX*). Essas linguagens de programação permitem que os desenvolvedores da *web* escrevam o código que é executado pelo navegador da organização. Embora esse código seja geralmente útil para a organização, os intrusos também o usam para coletar informações (como quais sites o usuário visita) ou executar código malicioso no computador. É possível desativar *Java, JavaScript e ActiveX* no navegador da *Web*, mas o usuário deve estar ciente que isso pode limitar a funcionalidade legítima do navegador. Além disso, o usuário deve estar ciente dos riscos envolvidos no uso do código móvel nos programas de *e-mail*. Muitos programas de *e-mail* usam o mesmo código que os navegadores da *Web* para exibir *HTML*. Assim, as vulnerabilidades que afetam o *Java, o JavaScript e o ActiveX* são muitas vezes aplicáveis ao *e-mail* e às páginas da *Web*.

- **Scripts entre sites** (*Cross-site scripting*): Um desenvolvedor *web* malicioso pode anexar um *script* a algo enviado para um *site*, como um *Uniform Resource Locator* (URL), um elemento em um formulário ou um inquérito de banco de dados. Mais tarde, quando o site responde, o *script* malicioso é transferido para o navegador. Isso pode potencialmente expor o navegador da *Web* a *scripts* maliciosos por: - Seguindo *links* em páginas da *Web*, mensagens de *e-mail* ou postagens de grupos de notícias sem saber onde eles ligam - Usando formulários interativos em um *site* não confiável - Visualizando grupos de discussão, fóruns ou outras páginas geradas dinamicamente, onde os usuários podem postar texto contendo *tags HyperText Markup Language* (HTML), Linguagem de Marcação de Hipertexto.

- ***Spoofing* por *e-mail***: É quando uma mensagem de *e-mail* parece ter se originado

de uma fonte quando ela realmente foi enviada de outra fonte. O *spoofing* por *e-mail* geralmente é uma tentativa de enganar o usuário para fazer uma declaração prejudicial ou liberar informações confidenciais (como senhas). O *e-mail* falsificado pode variar de brincadeiras inofensivas a estratagemas de engenharia social. Exemplos disso incluem: - *E-mail* reivindicando ser de um administrador de sistema solicitando aos usuários que alterem suas senhas para uma *string* especificada e ameaçando suspender sua conta se eles não cumprirem - *E-mail* alegando ser de uma pessoa na autoridade que solicita aos usuários para enviar uma cópia de um arquivo de senha ou outra informação sensível

- **Vírus transmitidos por *e-mail*** (*E-mail-borne viruses*): Vírus e outros tipos de códigos maliciosos geralmente são distribuídos como anexos para mensagens de *e-mail*. Antes de abrir quaisquer anexos, o usuário deve estar ciente da fonte do anexo. Não basta que o *e-mail* seja originário de um endereço reconhecido. Por exemplo, o vírus Melissa se espalhou precisamente porque se originou de um endereço familiar. Além disso, o código malicioso pode ser distribuído em programas divertidos ou sedutores. Muitos vírus recentes utilizam essas técnicas de engenharia social para se espalhar. Exemplos incluem *W32/Sircam* e *W32/Goner*.

- **Extensões de arquivo escondidas** (*Hidden file extensions*): Os sistemas operacionais *Windows* possuem uma opção para ocultar extensões de arquivos para tipos de arquivos conhecidos. A opção está habilitada por padrão, mas um usuário pode optar por desativar esta opção para ter extensões de arquivo exibidas pelo *Windows*. Vários vírus transmitidos por *e-mail* são conhecidos por explorar extensões de arquivo escondidas. O primeiro grande ataque que aproveitou uma extensão de arquivo oculta foi o verme *VBS/LoveLetter* que continha um anexo de *e-mail* chamado *LOVE-LETTER-FOR-YOU.TXT.vbs*. Outros exemplos incluem *Downloader* (*MySis*.avi.exe ou *QuickFlick*.mpg.exe), *VBS/CoolNote* (*COOL_NOTEPAD_DEMO.TXT.vbs*) e *VBS/OnTheFly* (*AnnaKournikova*.jpg.vbs). Os arquivos anexados às mensagens de *e-mail* enviadas por esses vírus podem parecer textos inofensivos (.txt), MPEG (.mpg), AVI (.avi) ou outros tipos de arquivos, quando de fato o arquivo é um *script* malicioso ou executável (.vbs ou .exe).

- **Clientes de bate-papo** (*Chat clients*): Os aplicativos de bate-papo na Internet, como aplicativos de mensagens instantâneas e redes de conversação de Internet, *Internet Relay Chat* (IRC) - protocolo de comunicação utilizado na Internet, fornecem um mecanismo para que a informação seja transmitida bidirecionalmente entre os computadores na Internet. Os clientes de bate-papo fornecem grupos de indivíduos com os meios para trocar diálogo, *Uniform Resource Locator* (URL)s da *web* e, em muitos casos, arquivos de qualquer tipo. Como muitos clientes de bate-papo permitem a troca de código executável, eles apresentam riscos semelhantes aos dos

clientes de *e-mail*. Tal como acontece com os clientes de *e-mail*, a capacidade dos clientes de chat de executar arquivos baixados deve ser limitada. Como sempre, o usuário deve desconfiar da troca de arquivos com partes desconhecidas.

- ***Sniffing* pacotes** (*Packet sniffing*): É um programa que captura dados de pacotes de informações à medida que eles viajam pela rede. Esses dados podem incluir nomes de usuários, senhas e informações proprietárias que viajam pela rede em texto claro. Com talvez centenas ou milhares de senhas capturadas pelo *sniffer* de pacotes, os intrusos podem lançar ataques generalizados em sistemas. A instalação de um *sniffer* de pacotes não necessita necessariamente de acesso ao nível do administrador. Em relação aos usuários *Digital Subscriber Line* (DSL) - Linha Digital de Assinante e *dial-up* tradicionais, os usuários de modem a cabo têm maior risco de exposição a cheiros de pacotes, já que todo o bairro de usuários de modem a cabo faz parte efetivamente da mesma *Local Area Network* (LAN) - Rede de área local. Um *sniffer* de pacotes instalado em qualquer computador do usuário do modem a cabo em um bairro pode ser capaz de capturar dados transmitidos por qualquer outro modem a cabo no mesmo bairro.

- **Roubo de identidade** (*Identity theft*): As informações armazenadas em um computador doméstico podem fornecer um *hacker* dados pessoais suficientes para solicitar um cartão de crédito ou identificação em nome do usuário.

- **Túnel** (*Tunneling*): Quando os funcionários trabalham em casa e transferem arquivos para um computador no escritório, há potencial para que alguém possa obter acesso remoto ao computador doméstico e colocar um arquivo secreto em um documento que acaba no sistema da empresa.

- **Zumbis** (*Zombies*): Os programas automáticos procuram sistemas que estão conectados à Internet, mas estão desprotegidos; levá-los sem o conhecimento do proprietário; e use-os para fins maliciosos.

- ***Spyware***: O software de pesquisa inocente (por exemplo, o software do agente *Peer-to-peer* (P2P) usado em software de comunicação *peer-to-peer* popular) pode incluir ou ocultar software que colete informações sobre o sistema e o usuário e pode enviar essas informações para terceiros sem o conhecimento legítimo do usuário.

2.4 *Cybercrimes* ou Crimes Digitais

Cybercrime ou Crimes Digitais são termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, uma base de ataque ou como meio de crime. Temos logo abaixo alguns relatos

de vulnerabilidades em dispositivos que podem ser utilizados para cometer crimes graves, simplesmente utilizando uma conexão de internet com acesso remoto.

Hacker invade babá eletrônica: "O caso, ocorrido em 2013, foi um ataque a família de Marc e Lauren Gilbert, um casal de Houston, Texas. Um hacker conseguiu invadir o circuito eletrônico de uma babá eletrônica da marca Foscam na residência do casal e começou a gritar insultos à criança de 2 anos de idade. Marc e Lauren ouviram um sotaque "britânico ou europeu"gritando ofensas e obcenidades e foram ver o que ocorria. Pela câmera, o hacker foi capaz de ver o nome da criança escrito na parede do quarto. "A sensação era de que tinham invadido a nossa casa", disse Marc. A criança por sorte estava dormindo. O jornal BBC diz ter encontrado provas de que hackers compartilham informações sobre como acessar câmeras não protegidas em fóruns online."(BBC - NOTÍCIAS, 2013)

Hacker invade sistema de carro: "Engenheiros de segurança *hackers* descobriram que eles poderiam sequestrar o sistema de entretenimento informativo de um *Jeep Cherokee* usando uma simples conexão de internet. Através de uma vulnerabilidade no *Uconnect* – um software que permite que veículos *Chrysler* se conectem a Internet e também controlem as funções de navegação e de entretenimento – os dois obtiveram acesso as funções mais críticas do carro e remotamente assumiram o controle delas. No experimento feito, conseguiram ate mesmo girar o volante, mudaram a estação de rádio, aumentaram o volume e acionaram os limpadores de para-brisas. Depois, desativaram a transmissão e o acelerador enquanto o carro estava em movimento, bloquear as travas de segurança e desativar ou travar os freios do carro remotamente. Aparentemente, o experimento pode ser replicado em outros modelos da *Fiat Chrysler*. Vale ressaltar que os hackers estavam a mais de 15 quilômetros de distância da estrada por onde circulava o motorista."(UOL - CARROS, 2015)

Hacker invade Smart TV: "A gravação apareceu em um site. Amigos viram as imagens e alertaram o casal. Eles não haviam feito qualquer vídeo particular. Pelo ângulo, o vídeo foi feito pela câmera da smart TV. Não houve contato com o casal, não houve chantagem ou ameaça. Concluímos que deve ter sido um ataque aleatório", disse Laura. O hacker em questão conseguiu ativar a câmera do aparelho a distância.(O GLOBO, 2016)

2.5 Estudo de Caso

O estudo de caso realizado pelo (OLHAR DIGITAL, 2016), constante no Anexo A, apresenta todos os detalhes de um Data Center da empresa de tecnologia **Level 3**, localizado em Cotia, e demonstra todos os mecanismos adotados em segurança física e logica mais atuais relacionados a tecnologia. Desta forma, este estudo de caso, tem como principal objetivo fundamentar, comprovar e ilustrar todo o embasamento teórico.

3 Desenvolvimento

Este capítulo descreve os Projetos e Avanços que podem Impactar na Segurança Digital, observando os critérios particulares dos projetos ligados a segurança acerca de parâmetros e resultados dos sistemas virtuais. Demonstra ainda, os avanços das aplicações de segurança propostas e define as estratégias para que as empresas possam defender seus bens de possíveis ataques ou ameaças.

3.1 Controle de Acesso

Deve haver um controle de quem entra e de quem sai de um Sistema de Informação ou mesmo de uma instalação física, é um projeto que pode impactar consideravelmente na Segurança Digital, pois não basta ter um firewall rodando em servidores, ou no caso de ambientes físicos, um guarda na entrada para obrigar todos os visitantes a se identificarem. É preciso desenvolver um projeto de política no controle de acessos eficiente, para caso haja um incidente, ser possível identificar o seu autor.

De acordo com (KOTONYA; SOMMERVILLE, 1998) as principais características do conjunto básico de requisitos de Sistemas são:

- **Requisitos de Confiabilidade** - São os requisitos diretamente ligados à disponibilidade e à taxa de falhas (quão frequentemente o sistema deixa de desempenhar sua função). Ambos, disponibilidade e taxa de falhas, são expressos de forma quantitativa.
- **Requisitos de Desempenho** - Os tipos de requisitos de desempenho especificados são os tempos de resposta aceitáveis por usuários e por outros sistemas que possuam interfaces com o sistema sob estudo, a quantidade de dados processados em um determinado período de tempo e os períodos determinados para a obtenção de sinais de entrada e para a geração de sinais de saída. Estes parâmetros são do tipo quantitativo;
- **Requisitos de Segurança Crítica** - Nesta categoria de requisitos, os objetivos são assegurar uma operação sem a ocorrência de situações consideradas perigosas e determinar a adequação de sistemas de proteção. Informalmente, pode-se dizer que são requisitos que estabelecem o que o sistema não pode fazer, restringindo a liberdade do projetista. São ainda determinadas todas as condições inaceitáveis ou indesejáveis para o sistema. Os requisitos de segurança crítica são considerados do tipo qualitativo.

- **Requisitos de Segurança de Informação** - Tais requisitos têm como objetivo garantir que não seja feito o acesso ao sistema e a seus dados, por pessoas ou sistemas não autorizados. Exemplos de requisitos deste tipo são, manter permissões de acesso sob controle do administrador do sistema, efetuar cópias de segurança a determinados períodos e armazená-las em local seguro ou ainda efetuar a criptografia em todas comunicações externas realizadas. A Segurança de Informação é vital para a manutenção da Segurança Crítica.

- **Requisitos de Usabilidade** - Referem-se à interface do usuário e suas interações com o sistema. Exemplos de requisitos deste tipo são o tempo de aprendizado de uso do sistema e a gravidade ou importância de erros na operação.

Conforme podemos perceber os projetos e avanços que podem impactar na Segurança Digital, relacionados ao controle de acesso pode ser realizado por meio de Segurança Lógica e Física:

- **Segurança lógica** é a forma como o Sistema de Informação é protegido no nível de sistema operacional e de aplicação. Proteção de sistemas contra ataques e erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação. Atentando contra ameaças ocasionadas por vírus, acessos remotos à rede, backup desatualizados, violação de senhas, etc.

- **A segurança física** deverá ser pensada em profundidade, visando aumentar o nível de proteção contra acessos não autorizados ao o Sistema de Informação. Os bens mais importantes deverão ficar mais perto do centro das instalações, obrigando à passagem por diversos níveis de validação (proporcionais ao tipo de informação que protegem, para também não haver exageros. Exemplo: ninguém vai proteger o depósito de materiais de limpeza com um leitor de retina).

3.1.1 Controle de Acesso Lógico

O controle de acesso lógico é um projeto ou maneira utilizada para autenticar usuários nos Sistema de Informação ou em sistemas físicos que envolvam todas as tecnologias utilizadas. Existem três maneiras básicas de se autenticar um usuário em um sistema:

- **Primeiro Método**: O que você sabe - senha de acesso.

- **Segundo Método**: O que você tem - um *smart card*, USB *flash* ou *token*.

- **Terceiro Método**: O que você é - É o método mais seguro dos três, utilizando biometria, tipos: impressão digital, íris, retina, voz, facial, geometria da mão, etc.

3.1.1.1 Primeiro Método: O que você sabe

Como exemplo, pode-se citar as senhas que é a forma mais utilizada e de melhor custo benefício. O mais importante, antes de tudo, é possuir uma senha que possa ser considerada segura, no entanto, ainda que nada seja perfeitamente seguro, o ideal é que essa senha seja tão difícil de ser quebrada (por métodos como o de força bruta) que se torne inviável para o atacante. Algumas dicas são importantes para isso:

- Não utilize nomes que possam ser encontrados em um dicionário;
- Misture caracteres estendidos, letras e números (u=S-!m?045ktrhiyotp);
- Nunca utilize nomes ao contrário, ou palavras com apenas um número na frente;
- Utilize uma senha que seja, de preferência, maior que oito dígitos;
- Não repita senhas para diferentes;
- Troque suas senhas com certa frequência, pelo menos, uma vez por mês.

Nos *smartphones* com sistema *android*, observa-se mecanismos de acessos por senha ou desenhos de grafos interligando pontos, onde o usuário cadastra esse padrão anteriormente. Essas proteções conseguem ser eficazes pelo numero de tentativas serem limitados, chegando até a bloquear o *smartphone*, por algum tempo.

Nos computadores com sistemas *windows* e *linux*, tem-se o login de acesso, onde cada usuário, possue seu nome e senha de login. Geralmente pode ser cadastrada uma pergunta padrão para recuperar a senha cadastrada pelo usuário do computador.

Para manter seguros os serviços rodados nos navegadores, são realizados login, com o número de tentativa limitada que se expirada provoca o bloqueio da conta (evita força bruta), fornecendo algum mecanismo de recuperação da senha (podendo ser por um outro e-mail cadastrado na conta ou por uma mensagem via celular). Em alguns casos além de pedir o login (nome e senha) pode ser pedido ao usuário que transcreva alguns caracteres mostrados em imagens ou solicitar a identificação de alguns objetos dentro das imagens dadas.

3.1.1.2 Segundo Método: O que você tem

Como exemplo, tem-se o Certificado Digital, onde as chaves privadas e as informações referentes ao seu certificado de autentificação de acesso ficam armazenadas em um hardware criptográfico - cartão inteligente (*smart card*) ou cartão de memória *(token* USB ou *pen drive* ou *USB flash*).

Segundo (RIBEIRO, 2015) a Certificação digital é um conjunto de processos e técnicas que dão maior segurança às comunicações e às transações eletrônicas. Ela evita

que os dados transmitidos sejam interceptados ou adulterados no trajeto entre a máquina do remetente e a do destinatário e identifica o autor da mensagem. Os dois principais elementos da certificação digital são o certificado e a assinatura digitais, que têm como base a criptografia, técnica usada para codificar dados que trafegam pela Internet. Juntos, esses dois elementos comprovam a identidade de uma pessoa ou site e evitam fraudes nas transações eletrônicas.

Alguns órgãos do Governo Federal e empresas privadas já estão exigindo a adoção do certificado para acessar alguns de seus serviços online, conforme exemplos a seguir:

- Tribunal de Justiça, que disponibiliza acesso aos processos jurídicos online, onde cada advogado registra seu token de identificação.

- Secretaria da Receita Federal, que disponibiliza para o contribuinte brasileiro os certificados digitais **e-CNPJ** e **e-CPF** com acesso a vários de seus serviços.

  O **e-CPF**: Criado para identificar o contribuinte pessoa física na Internet, o e-CPF é emitido pelas seguintes autoridades certificadoras Serasa, Certisign, Prodemg, Serpro, Imesp e Sincor.

  O **e-CNPJ**: para diversos serviços online disponibilizados pelos governos Federal, Estadual e Municipal. É possível, por exemplo: Emitir comprovantes de arrecadação de pagamento de tributos; Retificar possíveis erros no preenchimento de Darf (Documento de Arrecadação de Receitas Federais); Parcelar débitos fiscais; Realizar todas as transações relativas ao comércio exterior e Emitir nota fiscal eletrônica.

  Na Figura 3, temos os cartões inteligente é feito de plástico semi-rígido e mede 8,5cm x 5,4cm. Na frente do cartão ficam Nome e CPF do titular ou inscrição no CNPJ, o chip criptográfico onde estão armazenados os dados do titular e a chave privada associada àquele certificado, e o logo da autoridade certificadora. No verso estão os logos da Receita Federal e da ICP-Brasil, além da mensagem de alerta que orienta o titular a revogar o certificado em caso de perda ou roubo do cartão.

- Empresas Privadas, que disponibiliza acessos aos seus servidores remotamente para devidas manutenções, por pessoas autorizadas com esses tipos de privilégios.

Segundo (RIBEIRO, 2015) o certificado digital (similar ao RG) é um documento eletrônico que contém informações que identificam uma pessoa, uma máquina ou uma instituição na Internet. Para fazer isso, ele usa um software como intermediário - pode ser o navegador, o cliente de e-mail ou outro programa qualquer que reconheça essa informação. O certificado digital é emitido a pessoas físicas (cidadão comum) e jurídicas (empresas ou municípios), equipamentos e aplicações.

Figura 3 – e-CPF e e-CNPJ

O e-CPF em cartão inteligente **O e-CNPJ em cartão inteligente**

Fonte: Ribeiro (2015, p. 10-11)

Conforme (RIBEIRO, 2015) a emissão é feita por uma entidade considerada confiável, chamada Autoridade Certificadora. É ela quem vai associar ao usuário um par de chaves criptográficas (pública e privada). Essas chaves, emitidas e geradas pelo próprio usuário no momento da aquisição do certificado, transformam um documento eletrônico em códigos indecifráveis que trafegam de um ponto a outro sigilosamente.

Enquanto a chave pública codifica o documento, a chave privada associada à ela decodifica. E vice-versa. Um certificado pode ser usado em conjunto com uma assinatura digital. Neste caso, a assinatura digital (carimbo dos cartórios, para reconhecer firma) fica de tal modo vinculada ao documento eletrônico que qualquer alteração o torna inválido.

Juntos, esses dois elementos, aliados à criptografia, garantem a confiabilidade, a autenticidade, a integridade (combina o uso de chaves públicas com uma assinatura digital), o não repúdio à transação e a confidencialidade da informação, ou seja, as partes são mesmo quem dizem ser, e a transação online é legítima, autêntica, segura e não sofreu alterações ao longo do caminho.

De acordo com (RIBEIRO, 2015) a assinatura digital assim como a criptografia assimétrica é uma sequência de bits resultante de uma operação matemática conhecida como função hashing. Essa função analisa todo o documento ou arquivo e, com base no algoritmo matemático, gera um valor de tamanho fixo para ele.

Esse valor varia de acordo com a sequência de bits do documento, e como cada caractere tem uma composição binária, qualquer mudança no arquivo original fará com que o valor hash seja diferente e a assinatura se torne inválida.

3.1.1.3 Terceiro Método: O que você é

Como exemplo de Projetos e Avanços que podem Impactar na Segurança Digital, relacionado a esse terceiro método, temos os **Mecanismos de Biometria** que é um dos métodos de segurança mais avançados e seguros atualmente, e será descrito da mais simples até a mais moderna Biometria existente. Esse método pode ser utilizado como complemento dos dois métodos vistos anteriormente, a fim de criar níveis de segurança mais fortes.

Segundo (BONATO; NETO, 2010) **Biometria** é a ciência que procura identificar indivíduos baseando-se em características únicas. Essas características podem ser de caráter físico, químico ou comportamental. Seu principal uso é controlar o acesso de pessoas a um local que exige um nível de segurança.

O uso desse método biométrico evita perdas de objetos identificadores como cartões ou o esquecimento de senhas, já que a identificação é feita por meio de "**O que você é**". Nos últimos tempos essa área vem se desenvolvimento e novas tecnologias surgem, com isso muitos são os interesses em pesquisas fazendo com que o setor de Controle de Acesso Lógico, torne mais seguro o acesso somente as pessoas autorizadas.

Conforme (BONATO; NETO, 2010) para conseguimos utilizar os recursos da Biometria devemos seguir algumas as etapas:

- 1. **Registro**: A amostra coletada é analisada, verificar se sua qualidade é aceitável, se for, a amostra é armazenada após um processo de criptografia, para proteger os dados.
- 2. **Extração de características**: o template é processado por alguns filtros para separar a imagem importante (algoritmo que faz a extração das características), melhor observável e armazenável, transforma essa imagem em uma matriz. Alguns desses algoritmos podem ser visto na Figura 4 na próxima página.
- 3. **Identificação ou verificação do usuário**: o dispositivo coleta uma nova amostra do usuário, extrai suas características e compara com o template. Se as características forem iguais, o usuário é aceito.

Alguns dos tipos de Biometria existentes atualmente são apresentados na Tabela 1 abaixo, no estudo desenvolvido por (BONATO; NETO, 2010), que apresenta suas vantagens, desvantagens e custo benefício. Através destas informações se torna possível ao

usuário visualisar a real necessidade de cada sistemas nos quais pretende empregar tais recursos Biométricos a fim de evitar gastos desnecessários na implantação do projeto de segurança.

Figura 4 – Algoritmos usado na Etapa de Extração de Características

Tipos	Algoritmos
Impressão digital	Baseado em Minutiae, baseado em correlação;
Retina	LCC;
Íris	Daugman, Li Ma, Boles;
Reconhecimento facial	PCA, LDA, ICA, LFA, EBGM;
Reconhecimento por voz	FFT, HMM com Baum-Welch;
DNA	P. Zhang;

Fonte: Bonato e Neto (2010, p. 04)

Tabela 1 – Tipos Biométricos.

Tipos Biométricos	**Vantagens**	**Desvantagens**
Impressão digital	Simples, barato;	Fácil de ser fraudado;
Retina	Precisão;	Caro, difícil de treinar os usuários;
Íris	Fácil aquisição,melhor precisão de todos os métodos;	Custo, baixa aceitabilidade;
Reconhecimento facial	Similar ao processo humano;	Pode ser difícil de adquirir, baixa precisão;
Reconhecimento por voz	Fácil aquisição;	Fácil de ser fraudado;
DNA	Determinístico e precisão;	Necessita de muito tempo para processar;
Assinatura Digital	Simples, barato, caligrafia;	Ainda em implantação
Mãos	Simples;	Ainda em pesquisas
Veias	Precisão, posições;	Caro, difícil de treinar os usuários;

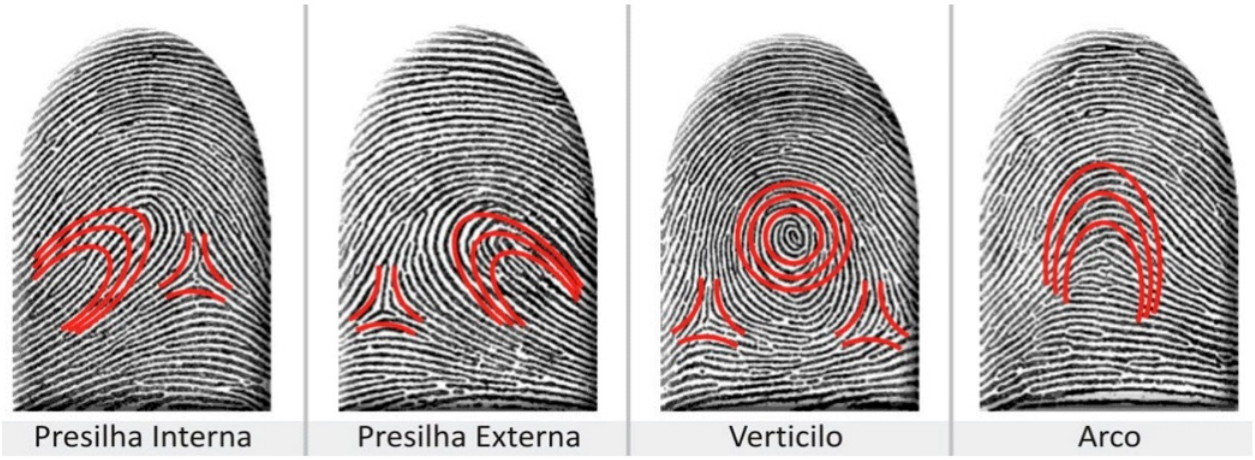
Fonte: Bonato e Neto (2010)

Através da analise dos Projetos e Avanços, será realizada uma breve descrição das principais Características, dos tipos de biometria, que podem impactar na Segurança Digital:

- **Impressão Digital**: é a mais antiga e utilizada até os dias atuais nos documentos de identidade. Os principais riscos estão em torno da polemica dos dedos de silicone,

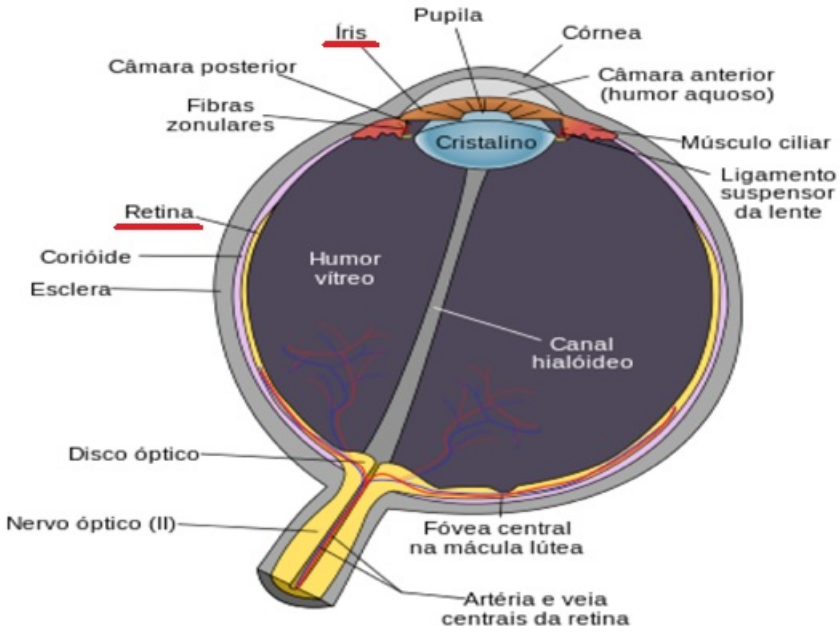
que podem tentar violar a autenticação. Na Figura 5 serão demonstradas algumas impressões digitais:

Figura 5 – Algumas Impressões Digitais



Fonte: Sportslab (2017)

Figura 6 – Componentes do Olho



Fonte: IORJ - Instituto de Oftalmologia do Rio de Janeiro (2017)

- **Retina**: é uma camada fina de tecido nervoso sensível à luz localizada no interior do olho. Projeta as imagens enxergadas, traduzindo para o cérebro através dos impulsos elétricos. Como pode ser observado na Figura 6.

- **Íris**: parte colorida do olho, como observado na Figura 6; Pode revelar até mesmo as condições de saúde de uma pessoa. Usa câmera CCD com resolução de 512 dpi, iridologia.

- **Reconhecimento Facial**: é muito desafiador desenvolver uma técnica de reconhecimento de rosto que pode tolerar os efeitos do envelhecimento, expressões faciais, ligeiras variações na imagiologia ambiente e a posição do rosto em relação à câmera.

- **Reconhecimento por voz**: Emissões acústicas que em alguns casos podem ser burladas por equipamentos de gravações. Risco: o sinal de voz pode ser degradada em qualidade pelo microfone, comunicação canal, digitalizador, saúde de uma pessoa (ex: resfriado), o stress, emoções, permitindo ainda, a identificação de uma pessoa em uma conversa telefônica (muito utilizada por operadoras telefônicas, forçando o cliente a aceitar alguns planos de telefonia só pelo simples fato de quem está na linha dizer um "Sim").

- **DNA**: Ácido Desoxirribonucleico (DNA), é uma molécula presente no núcleo das células com informação genética. Esse mecanismo biométrico faz comparação de códigos genéticos.

- **Assinaturas Digitais**: Redução de custos e tempo. Possibilita maior mobilidade; maneira como uma pessoa assina seu nome. Permite a agilidade na tramitação e resolução de processos; Responsabilidade social (Meio ambiente – lixo papel). É utilizada em carteiras de habilitações e títulos de eleitores.

- **Mãos**: Mede traços, linhas e tamanho da mão, bem como, o comprimento dos dedos e articulações envolvidas. É obtida uma imagem da mão para comparação com a imagem cadastrada.

- **Veias**: Identificação pelo padrão de veias; É realizada leitura por infravermelho para identificar o padrão único por pessoa.

3.1.2 Controle de Acesso Físico

Envolve toda a infraestrutura da empresa e de seus sistemas, onde são criadas regras de conduta a todos os profissionais envolvidos e ou usuários do sistema. Como exemplo, pode-se citar os visitantes ou funcionários não poderão levar materiais da empresa sem autorização expressa do responsável por esses equipamentos de Sistema de Informação.

O controle de acessos físico além de portaria com guardas e um sistema de vídeo em circuito fechado, no imóvel ou sala em que ficam os servidores dos Sistemas de Informação, devem ser registrados os acessos de todos os operadores e administradores, incluindo as identificação por cartões magnéticos e um livro com registro de acessos, onde devem ser colocadas as datas e horas de entrada e saída, bem como a assinatura da pessoa.

3.1.2.1 Sensores

Nos últimos tempos tem se tornado cada vez mais frequente a adição de sensores nos diversos tipos de dispositivos de segurança física, a fim de dar-lhes maior autonomia sem a necessidade de intervenção humana. Como exemplo pode-se citar os sensores de presença (ou movimentos), aquecimento (ou temperatura), fumaça e sensores no piso.

As câmeras de vigilância nos dias atuais passaram a ter **sensores de presença** para acionamento automático de gravações (com isso temos uma economia de espaços de armazenamentos de imagens), imagem colorida (de alta definição) e **sensores de visão noturna**, sendo indicada para qualquer sistema de monitoramento.

Já os **sensores de temperatura** são muito utilizados nos interiores de salas onde estão armazenados os Centro de Processamento de Dados (CPD), servidores ou Data Center, e sua principal função é monitorar em tempo integral os limites admitidos de temperatura destas salas que variam entre 17°C a 20°C. Sua sensibiliade é capaz até mesmo de acionar um sistema anti-incêndio caso houver uma elevação da temperatura ocasionado pelo aumento do número de pessoas dentro do ambiente no qual o sensor esteja instalado.

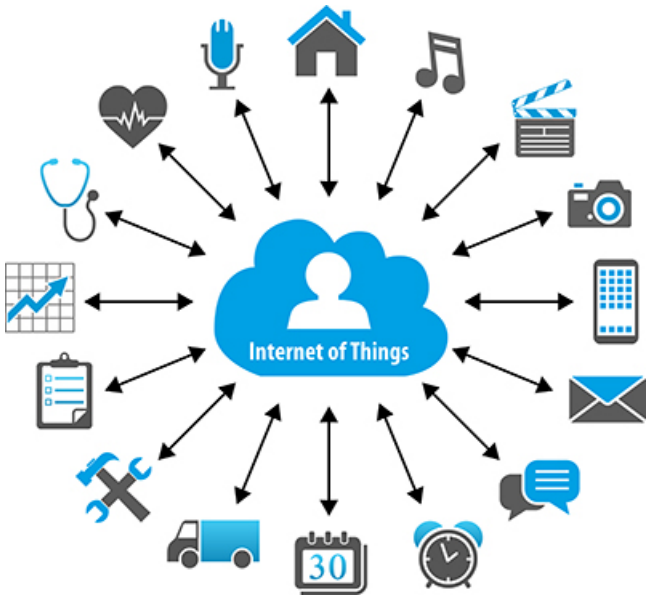
O **sensor ou detector de presença de fumaça** em um determinado ambiente pode salvar vidas, proteger patrimônios, equipamentos, computadores e servidores dentro da empresa. A presença de fumaça pode ser originada de um início de incêndio, então ele aciona um sistema de alarme, que avisará as pessoas que estão no local sobre o incidente, permitindo que elas escapem sem ferimentos. Ao mesmo tempo, o aparelho permite que brigadas de incêndio ou bombeiros militares sejam acionados, a fim de evitar maiores problemas e prejuízos ao patrimônio.

O **sensor encontrado no piso** geralmente é encontrado em portas de acesso que permitem que apenas uma pessoas passe por vez, evitando que várias pessoas tenham acesso ao local utilizando apenas uma identificação, desta maneira a porta secundária só tem seu acesso liberado se for detectada apenas uma pessoa entre as portas.

Uma outra curiosidade relacionadas aos sensores, está no fato de serem muito utilizados, como mostrado na Figura 7 em *Internet of Things* (IoT) ou seja, **Internet das Coisas** que são usados para designar objetos físicos usados no cotidiano interconectados a Internet de maneira a dotá-los com inteligência necessária para interagir com o meio em que

se encontram, a qualquer hora e em qualquer lugar através de atuadores eletromecânicos.

Figura 7 – Representação de aplicações da IoT



Fonte: Weatherby, E. (2016)

Essa nova forma de comunicação de **Internet das Coisas**, torna-se uma ferramenta fundamental para aplicações ubíquas, tais como: monitoramento da saúde, segurança pessoal, logística, jogos, redes sociais, casas inteligentes, cidades inteligentes, entre muitas outras. Devido ao baixo custo de sensores e comunicação *wireless*, a rede de tecnologia de sensores apresenta uma nova demanda a tecnologia Internet. Ela ira trazer grandes mudanças para a sociedade no futuro, alem de mudar a maneira de viver e trabalhar.

Segundo o (WOOTTON, 2016), um exemplo seria o do fabricante que oferece um sistema que meça o consumo de energia de uma residência ou estabelecimento de sensores instalados na fiação elétrica que medem em tempo real o consumo em *Amperes* de vários circuitos.

Estes dados são enviados pelos sensores a um *gateway* (ou ponte de ligação) que, por sua vez, os envia a um servidor deste fabricante em algum lugar do mundo e o cliente visualiza através de algum aplicativo, seja em seu tablete, *smartphone* ou energia elétrica que cada sensor esta medindo.

Um *Gateway*, ou ponte de ligação, é um dispositivo intermediário que interliga redes, separa os domínios de colisão, traduz protocolos. Por Exemplo, os *routers* (ou roteadores) e *firewalls*.

O *Internet of Things* (IoT) pode detectar por meios de gráficos ao longo do tempo o consumo, e assim detectar anomalias que podem indicar algum problema com algum

equipamento ou comportamento.

Alem dos benefícios da *Internet of Things* (IoT), há muita preocupação com segurança e privacidade em diferentes camadas: *Front end*, *Back end* e rede, portanto além dos estudos sendo desenvolvidos para criação de novas aplicações que se enquadrem nessa nova era tecnológica, e preciso também investir em segurança de infraestrutura. A medida que a Internet das Coisas começa a transformar industrias inteiras, as ameaças evoluem rapidamente para atacar esse novo e rico cenário, extremamente vulnerável.

Conforme a (SYMANTEC, 2016) com a expansão da conectividade para uma quantidade maior de dispositivos (automoveis, motores de jatos, robôs de fabricas, equipamentos médicos e controladores industriais lógicos programáveis), as consequências causadas por problemas em segurança estão cada vez mais sérios.

As consequências agora incluem danos físicos a indivíduos, inatividade prolongada e danos irreparáveis a equipamentos de capital, como tubulações, alto-forno e recursos para a geração de energia, principalmente na *Internet of Things* (IoT) industrial.

Há diversos relatos pela *Web*, em que confirmam no contexto de *Internet of Things* (IoT) de redes que possuem ameaças de acessos aos dados não autorizados, acesso não autorizado a serviços, roubo ou mudança das informações usadas na comunicação, vírus ou ataques de *malware* e segurança de rede.

As brechas de segurança, de permissão ou de criptografia existem e foram documentadas em diversos dispositivos conectados a web, desde carros, aparelhos médicos, brinquedos, baba eletrônica, *Smart* TVs da *Samsung* (é possível monitorar usuários), dispositivos esses que conectados a uma rede internet podem ser acessados e controlados de qualquer lugar do mundo.

Essa preocupação em manter dispositivos conectados e mais seguros é muito estudada já que a *Internet of Things* (IoT) em um espaço de tempo não muito grande já estará em vários dispositivos de uso cotidiano. Com isso mais soluções em segurança devem ser pensadas, pois com o nascimento da tecnologia surgem também ameaças de ataques que podem ser feitos utilizando brechas deixadas no sistema. A ideia é que junto com a tecnologia cresçam também as estratégias para proteger e manter os dados dos usuários mais seguros, uma vez que o quantitativo de informações armazenadas na nuvem tem sido crescente.

3.1.2.2 Acesso aos Servidores ou *Data Center*

Para a elaboração dos Projetos de acesso aos Servidores algumas medidas rotineiras de segurança deverão ser seguidas a risca, para a proteção de áreas restritas às pessoas autorizadas.

Segundo o estudo de caso realizado pelo (OLHAR DIGITAL, 2016) a um data

center da empresa de tecnologia **Level 3**, em Cotia, no Anexo A (**??**). A preocupação com a segurança deve já começar logo na entrada do terreno do *Data Center*, exigindo que todos se identifique mostrando seus documentos com foto aos seguranças. Uma vez liberada a entrada, precisam ser cadastrados na portaria do Data Center. Nesse momento é decidido o nível de acesso que as pessoas terão: esse nível determina quais áreas do espaço serão acessíveis com o crachá. O segurança irá acompanhar passando por uma porta dupla que garante a passagem de uma única pessoa por vez. A primeira porta é aberta com o crachá e se fecha atrás dele. Para abrir a porta seguinte, a pessoa posiciona seus pés em retângulos no chão e em seguida aperta um botão à sua frente. Se mais de uma pessoa tentar passar com apenas um crachá, o sensor no piso detectaria a presença de mais de uma pessoa e não abriria a segunda porta. Ao chegar a porta da sala com os *racks* de servidores só pode ser aberta por meio de identificação biométrica de um segurança ou de pessoas com alto nível de acesso.

Existem várias orientações que deverão ser seguidas para a criação de um local que possa ser realmente seguro ao Centro de Processamento de Dados (CPD), dentre elas podemos citar (SENAC, 2011):

- O Centro de Processamento de Dados (CPD) não deverá ficar nem no piso térreo nem no último andar.
- Não devem existir acessos diretos vindos do exterior (janelas, portas, etc.);
- Os acessos feitos ao Centro de Processamento de Dados (CPD) deverão poder ser facilmente monitorizados;
- Não é recomendável que tenha canos de água ou esgoto próximos ao local;
- Os locais deverão ter chão e teto falsos, tendo cabos de energia e refrigeração;
- A alimentação elétrica deve ser redundante;
- Os sistemas de detecção e combate a incêndios por supressão por gás inerte;
- Está de acordo com a maioria das normas de segurança internacionais.

3.2 Criptografia

Do grego: *kryptós* (escondido) + *gráphein* (escrita), a criptografia significa escrita escondida. É uma técnica de escrever mensagens em forma cifrada (cifras) com caracteres secretos ou em códigos, cuja finalidade é a proteção da informação.

A criptografia vem sendo utilizada por um público diverso, como militares, empresas preocupadas com o seu patrimônio ou até mesmo pessoas físicas com interesses individuais.

Essa escrita secreta é de extrema importância aos Sistemas de Informação, por garantir de maneira segura a confidencialidade, integridade, autenticidade e não-repúdio (evitar negação da mensagem) das informações manipuladas nesses sistemas dificultando que estas informações sejam decifradas por pessoas erradas.

Os mecanismos de funcionamento básicos de criptografia são:

- Pegar um texto legível, não criptografado;
- Encriptação: transforma o texto legível em um texto cifrado, por meio de um algoritmo;
- Utiliza-se no processo de transformação uma chave (simétrica) ou duas chaves (uma publica e uma privada no caso assimétrico), presença da função de resumo (***Hash***), para verificar a integridade da mensagem;
- Decriptação: transformar texto cifrado em texto legível.

Segundo (CERT.BR, 2017) a função de resumo (***Hash***) é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado ***hash***. Sendo utilizada para verificar a integridade de um arquivo. Exemplos de métodos de *hash* são: SHA-1, SHA-256 e *Message-Digest algorithm 5* (MD5) de 128 *bits*.

A criptografia é utilizada de varias formas:

- Tráfego *Web*: *Hyper Text Transfer Protocol Secure* (HTTPS) - protocolo de transferência de hipertexto seguro;
- Tráfego *Wirless*: IEEE802.11 *Wi-Fi Protected Access 2* (WPA2) - é um protocolo de comunicação via rádio e *Wired Equivalent Privacy* (WEP), Sistema Global para Comunicações Móveis (GSM), *Bluetooth*;
- Arquivos em discos, protegendo os dados sigilosos armazenados no computador;
- Proteção de conteúdo (DVDs, *Blu-ray*);
- Autenticação de usuários;
- Proteger backups contra acesso indevido;
- Proteger comunicações realizadas pela Internet;
- Assinatura digital, é usada uma chave privada que permite comprovar a autenticidade e a integridade de uma informação;

- Certificado digital, é um registro eletrônico (conjunto de dados que associa a uma chave pública). Sendo emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um *site Web*).
- E infelizmente temos também os usos indevidos, do tipo para cobrir rastos ou provas de criminosos em discos rígidos criptografados.

Com a o auxilio da **criptoanálise**, a criptografia pode ser quebrada por meio de ataque por força bruta, onde são testadas todas as chaves possíveis. Sendo assim o objetivo da criptografia é fazer com que o custo ou tempo sejam elevados, para que o tempo e recurso de quebra do código sejam extremamente demorados tornando assim inviável a quebra. A criptografia a ser usada depende da aplicação e do nível de segurança exigido, por exemplo, uma criptografia de 128 bits é muito mais segura do que uma de 56 bits.

As evoluções das criptografias utilizadas hoje, partem das de 128 bits que é tido como referência de segurança muito usadas por serviços como *WhatsApp*, *Signal*, *Messenger*, *Gmail*, *Facebook*. Esses aplicativos de mensagens oferecem a criptografia assimétrica de ponta-a-ponta, dando proteção e confidenciabilidade nas mensagens (ou conteúdos) trocadas entre os usuários envolvidos na conversa, onde cada usuário dentro dessas redes possui uma chave de criptografia específica que é combinada com a de seus contatos durante a troca de mensagens realizada dentro dos aplicativos.

3.2.1 Criptografia de chave simétrica e de chaves assimétricas

A Criptografia de chave simétrica, utiliza uma única chave tanto para encriptar como para decriptar informações, tem como prioridade garantir a confidencialidade dos dados e a vantagem de processo rápido, no entanto, as chaves devem ser trocadas antes da comunicação (riscos de interceptações), não garante a identidade de quem enviou ou recebeu a mensagem (autenticidade e não-repúdio) e caso um número n de pessoas quiserem se comunicar usando uma chave secreta, serão necessárias muitas chaves (escalabilidade).

Alguns exemplos de métodos criptográficos que usam chave simétrica são: *Advanced Encryption Standard* (AES), Blowfish (cifra simétrica de blocos), *Rivest Cipher 4* (RC4), *3 Data Encryption Standard* (3DES) - usa 3 chaves de 64 bits, onde 56 bits de chave + 8 bits de paridade e *International Data Encryption Algorithm* (IDEA) - chaves 128 bits. Como observado na Figura 8.

Conforme (CERT.BR, 2017) a criptografia de chaves assimétricas, utiliza duas chaves distintas: uma pública (livremente divulgada), e uma privada (mantida em segredo por seu dono). Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio.

Figura 8 – Alguns algoritmos criptográficos de chave simétrica comuns

Cifra	Autor	Comprimento da chave	Comentários
Blowfish	Bruce Schneier	1 a 448 bits	Velho e lento
DES	IBM	56 bits	Muito fraco para usar agora
IDEA	Massey e Xuejia	128 bits	Bom, mas patenteado
RC4	Ronald Rivest	1 a 2048 bits	Atenção: algumas chaves são fracas
RC5	Ronald Rivest	128 a 256 bits	Bom, mas patenteado
Rijndael	Daemen e Rijmen	128 a 256 bits	Melhor escolha
Serpent	Anderson, Biham, Knudsen	128 a 256 bits	Muito forte
DES triplo	IBM	168 bits	Segunda melhor escolha
Twofish	Bruce Schneier	128 a 256 bits	Muito forte; amplamente utilizado

Fonte: TANENBAUM (2015)

A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token*. Exemplos de métodos criptográficos que usam chaves assimétricas são: *Rivest Shamir Adleman* (RSA), Criptografia de Curvas Elípticas (ECC), Diffie-Hellman e *Secure Shell* (SSH) - protocolo de rede criptográfico para operação de serviços de rede em segurança.

3.2.2 *Cryptomalware*

Atualmente enfrentamos esse novo uso de criptografia, chamado de ***cryptomalware***, onde segundo (KASPERSKY, 2017) este ano de 2017 já vimos três ataques em grande escala do *Ransomware*, que é um tipo de ***cryptomalware*** pedindo resgate das informação criptografadas por *malware*. Até agora foram localizados e registrados três tipos de *malware* utilizados nesse tipo de ataque, são eles: o ***WannaCry***, o ***ExPetr*** e o ***Bad Rabbit***.

O primeiro foi ***WannaCry***, conforme (KASPERSKY, 2017) uma das principais razões pelas quais o *Trojan ransomware* que afeta usuários domésticos e empresas, entrou em erupção tão rapidamente que se transmite usando um *exploit*, entrando através de uma vulnerabilidade conhecida do *Windows* sem a necessidade de intervenção do usuário. E uma vez que um computador é infectado, o *malware* tenta se espalhar para todos os outros sistemas na rede local.

O segundo ***ExPetr*** (também conhecido como *Petya*, *PetrWrap* e *NotPetya*), de acordo (KASPERSKY, 2017) é uma variação de *cryptomalware*, *ransomware* os criminosos escolheram o alvo com bastante precisão: a maioria são empresas, não consumidores. A pior, infraestruturas críticas estão entre as vítimas. Por exemplo, alguns voos atrasaram no aeroporto de *Boryspil* em *Kiev* por conta do ataque. Ainda pior – o sistema de monitoramento da infame usina de *Chernobyl* parou temporariamente pelo mesmo motivo. Esses sistemas de infraestrutura crítica continuam sendo atingidos por *malware*, por

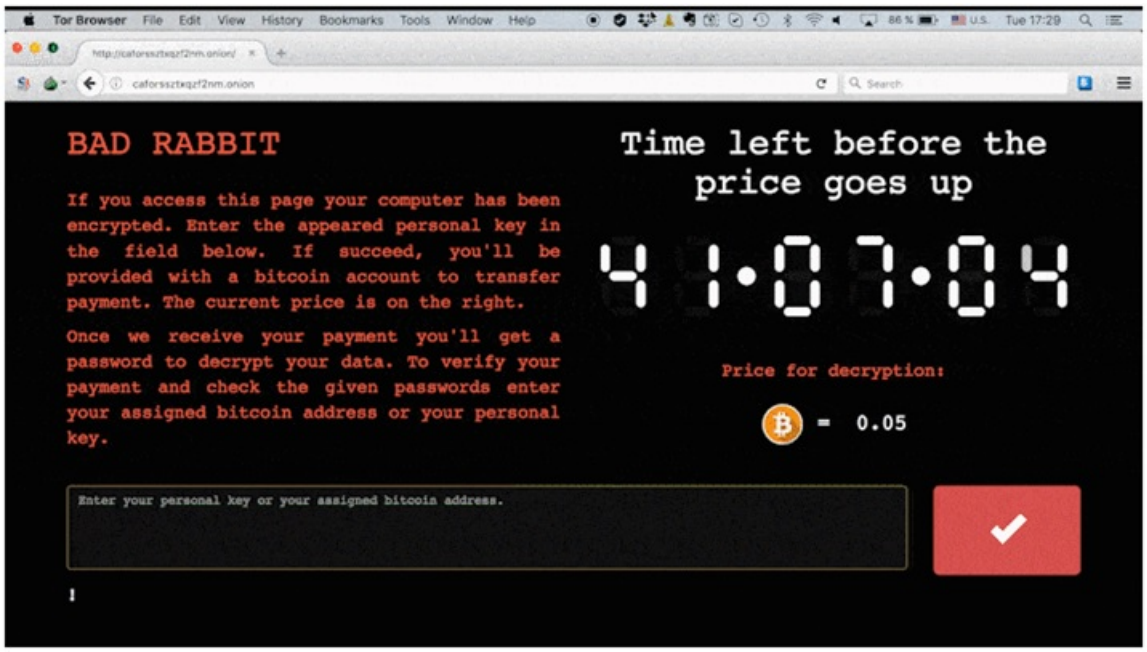
estarem diretamente conectados com a rede corporativa ou possuírem acesso à internet.

Primeiro, usa pelo menos dois *exploits*: um *EternalBlue* modificado (também usado pelo *WannaCry*) e o *EternalRomance* (outro *exploit* do *Transmission Control Protocol* (TCP) port 445). Segundo, quando um sistema é infectado no qual o usuário possui privilégios de administrador, começa a se disseminar usando a tecnologia do Windows Management Instrumentation ou com a ferramenta de controle de sistema remoto o PsExec. Temos a penetração inicial do malware na infraestrutura da empresa e sua proliferação interna.

Em alguns casos, por meio de sites maliciosos (infecção drive-by); usuários recebem o malware disfarçado de uma atualização no sistema. Em outros, a ameaça se espalhava como novas versões de softwares de terceiros – por exemplo, o M.E. Doc de contabilidade ucraniano. Em outras palavras, não há uma única forma de prever que entrada proteger.

Um terceiro o ***malware Bad Rabbit***, como mostrado pelo (KASPERSKY, 2017), o ***Bad Rabbit***, é um ataque direcionado contra redes corporativas e que infectou grandes meios de comunicação russos (as agências de notícias Interfax e Fontanka.ru). O Aeroporto Internacional de Odessa (Ucrânia), informou sobre um ataque cibernético em seu sistema de informação.

Figura 9 – Ataque Bad Rabbit, exigindo 0,05 Bitcoin como resgate



Fonte: Kaspersky (2017)

Outros ataques semelhantes, porém em menor escala ocorreram na Ucrânia, Turquia e Alemanha. Dessa vez, o ataque não ussou *exploits* (há uma diferença: ao contrário do

ExPetr, o ***Bad Rabbit*** não usa o *EternalBlue* – ou qualquer outro *exploit*). É um ataque drive-by: as vítimas baixam um falso instalador do *Adobe Flash* de sites russos infectados (de notícias ou de mídia) *hackeados* e iniciam manualmente o arquivo .exe, infectando-se assim. Alguns dos códigos usados no ***Bad Rabbit*** foram vistos no ***ExPetr***. Os criminosos por trás do ataque ***Bad Rabbit*** estão exigindo 0,05 *bitcoin* como resgate – aproximadamente US$ 280 à taxa de câmbio atual, como observado da Figura 9.

Segundo (KASPERSKY, 2017) para evitar ser uma vítima do cryptomalware, são recomendadas algumas medidas de seguranças, como:

- Devemos orientar aos funcionários a nunca abrir anexos suspeitos ou clicar em links recebidos por *e-mail*;
- Garanta que todos os sistemas conectados à internet estão equipados com soluções de segurança atualizadas que incorporem análise comportamental de componentes;
- Verifique se todos os componentes criticamente importantes da solução de segurança estão habilitados (por exemplo, antivírus);
- Atualize soluções de segurança regularmente;
- Empregue ferramentas para controlar e monitorar soluções de segurança de um único dispositivo com permissões de administrador – não permita que funcionários brinquem com as configurações;
- Monitoramento de portas usando o *firewall*;
- Bloqueie a execução dos arquivos *c:\windows\ infpub.dat* e *c:\Windows\cscc.dat*.
- Desative o serviço do Instrumentação de Gerenciamento do Windows (WMI) (se for possível) para impedir que o *malware* se espalhe pela sua rede.
- Faça *backup* dos dados sempre.
- Não pague o resgate. Pois ainda não se sabe se é possível recuperar arquivos criptografados por ***Bad Rabbit*** (seja pagando o resgate ou usando alguma falha no código do ***ransomware***).

3.3 Controle de Informações em Sistemas

Os Projetos e Avanços que podem impactar na Segurança Digital, relacionados ao controle de informações em nossos sistemas é uma preocupação constante. Devido ao custo e a complexidade do gerenciamento de volumes crescentes de dados e de conteúdo, combinados com a necessidade de fornecer informações confiáveis para todos os usuários em todas as transações, onde requer:

- Criação de políticas e práticas para gerenciamento e proteção das informações;
- Definir a infra-estrutura e a tecnologia para controle;
- Estabelecer definições comuns e padrão do domínio da informação;
- Definir os processos e pontos de controle;
- Desenvolver padrões de arquitetura;
- Monitorar e aprimorar a qualidade dos dados;
- Capacitar e treinar diretores, administradores, executivos e pessoal envolvido;
- Estabelecer e supervisionar as políticas organizacionais necessárias.

3.4 Backup

Em Sistemas de Informação, ***Backup*** é a cópia de dados que é feita de um dispositivo de armazenamento para outro, de maneira continua para que possam ser restaurados em caso da perda dos dados ou informações originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Meios difundidos de cópias de segurança incluem *Compact Disc Read-Only Memory* (CD-ROM), *Digital Versatile Disc* (DVD), disco rígido, disco rígido externo (uso de *Universal Serial Bus* (USB)), fitas magnéticas e a cópia de segurança externa (online ou em nuvem) que transporta os dados por uma rede como a Internet para outro ambiente, geralmente para equipamentos mais sofisticados, de grande porte e alta segurança.

Outra forma pouco difundida de cópia de segurança é feita via rede. Na própria rede local de computadores, o administrador ou o responsável pela cópia de segurança grava os dados em um formato de arquivo, processa e distribui as partes constituintes da cópia nos computadores da rede, de forma segura (arquivos são protegidos), criptografada (para não haver extração ou acesso aos dados na forma original) e oculta (na maioria das vezes o arquivo é ocultado).

Normalmente essas cópias de segurança são feitas em horários de menor pico de funcionamento da empresa, e são guardados em outros locais fora da empresa ou dentro de cofres a prova de incêndios e roubos, com acesso restrito apenas a pessoas autorizadas.

As arquiteturas *Redundant Array of Independent Disk* (RAID) utilizadas alocam uma porção de sua capacidade para armazenamento de códigos redundantes, que permitem a recuperação dos dados originais, no caso de falha de algum disco da arquitetura, a partir dos dados presentes nos demais discos (SCHULZE et al., 1989).

As arquiteturas *Redundant Array of Independent Disk* (RAID) podem ser classificadas em sete níveis segundo (HENNESSY; PATTERSON, 1990):

- **RAID 0**: não contém nenhum tipo de redundância ou de paridade dos dados, ocorrendo apenas o entrelaçamento ou distribuição dos dados em diversos discos;
- **RAID 1**: nesta classe de redundância de discos, é feito o espelhamento dos dados em um ou mais discos distintos;
- **RAID 2**: consiste na implementação do armazenamento dos dados através de Códigos de *Hamming*, que possibilitam a correção de erros, de acordo com o nível de redundância utilizado;
- **RAID 3**: nesta classe de redundância, há um disco exclusivamente dedicado ao armazenamento da paridade dos dados, calculada em todos os demais discos da matriz redundante;
- **RAID 4**: realiza-se o armazenamento de blocos de dados de forma entrelaçada entre os diversos discos da arquitetura, sendo que um dos discos continua reservado ao armazenamento do *bit* de paridade;
- **RAID 5**: nesta classe também se realiza o armazenamento de blocos de dados de forma entrelaçada entre os diversos discos da arquitetura, bem como o armazenamento da paridade também é distribuído entre os diversos discos;
- **RAID 6**: tem as mesmas características do RAID nível 5, além de apresentar também redundância de dados.

Como o foco deste trabalho é o que temos de mais avançados mecanismos de preservar todas as informações em Sistema de Informação, daremos preferência de implementação a partir do **RAID 5**, pois a paridade é distribuída entre os diversos discos.

3.4.1 *Cloud Storage*

O ***Cloud storage*** ou **armazenamento na nuvem** é considerada como uma das maneiras mais modernas de Backup atualmente, pois garante a integridade dos Bancos de dados. As cópias de segurança ou backup são salvos na nuvem, o que basicamente consiste em enviar os dados para uma empresa terceirizada ou outra filial em um outro local através da Internet.

Caso ocorra a perda de acesso aos dados, uma cópia estará disponível por esse serviço de backup na nuvem, ou seja, os dados não ficam armazenados exclusivamente em um dispositivo, pois, os mesmos podem ser acessados, guardados e compartilhados de qualquer lugar do mundo, bastando apenas ter uma boa conexão de Internet.

A utilização de *Cloud Storage* para *backup* e sincronização de arquivos vem a ser uma ferramenta de grande valia tanto pra empresas ou indivíduos comuns. Os mecanismos de armazenamento na nuvem podem proporcionar mais agilidade (acesso rápido as informações), organização, otimização do espaço físico (terceirização do serviço) e até mesmo a escalabilidade com custos reduzidos (*upgrade* do serviço para obter mais espaço).

Como um outro exemplo de uso em nuvem temos a própria construção deste estudo, no qual foi utilizada uma plataforma online de implementação de códigos *LaTex* para geração deste documento.

Segundo (WEBLINK, 2017) as principais ferramentas que oferecem o serviço de armazenamento em nuvem, são:

- **One Drive**: Essa é a ferramenta de armazenamento em nuvem da *Microsoft* e já vem pré-instalada no *Windows* 10. Além disso, a ferramenta permite o trabalho colaborativo com outras ferramentas como o *Word*, *Excel*, *Power Point* e *OneNote* a partir de qualquer dispositivo ou pela *web*. A plataforma oferece planos gratuitos com 5GB ou planos pagos de até 5TB que podem conter os programas que compõem o *Office 365*. Além disso, também existem os planos empresariais que contam com soluções para equipes com espaço de armazenamento ilimitado.

- ***Google Drive***: Esta é a plataforma de armazenamento em nuvem da ***Google*** e conta com 15GB gratuitos para guardar qualquer tipo de arquivo, basta ter uma conta de *e-mail*. Os planos pagos disponibilizam de 100 GB até 30TB de espaço de armazenamento. Porém, se a sua necessidade for ainda mais profissional você também pode optar pelo *Google Drive for Work* onde cada usuário conta com espaço de armazenamento ilimitado e recursos avançados.

- ***Dropbox***: O *Dropbox* é bem famoso quando se fala em armazenamento em nuvem pela sua facilidade de uso. Oferece plano básico de 2GB gratuitos. Os valores são cobrados somente em dólares. Um dos grandes diferenciais do *Dropbox* é a preocupação com a segurança das informações armazenadas, pois todos os planos contam com recursos avançados que garantem a proteção dos dados. Os valores dos planos começam a partir de U$ 9,99/mês e o espaço de armazenamento é disponibilizado a partir de 1TB. Já para empresas e equipes o espaço é ilimitado e pode ser customizado de acordo com cada necessidade.

- ***Resilio***: é uma ferramenta desenvolvida por ex-colaboradores da *BiTorrent* e oferece serviços de armazenamento de dados de alto desempenho. A ferramenta promete sincronizar todos os dados em todos os dispositivos, além de disponibilizar recursos avançados para gestão de dados. Sincronização seletiva: onde o usuário pode escolher baixar apenas os arquivos que precisa sem ter que replicar pastas inteiras em todos os

seus dispositivos. Envio de arquivos grandes: um serviço onde a plataforma ignora a nuvem e encontra o caminho mais curto entre os dispositivos ao transferir dados. Com isso é possível enviar arquivos sem limites de tamanho, sincronizar e compartilhar facilmente pastas que contenham *gigabytes* (ou até *terabytes*) de dados. Os planos e valores do *Resilio* são um tanto diferenciados, começando por U$59,99 pagos uma única vez para uso pessoal e U$99,99 para até 5 usuários. Para uso empresarial a plataforma custa a partir U$ 29,00 por mês.

- ***Icloud***: O *iCloud* é a plataforma de armazenamento em nuvem da *Apple* e com ela o usuário mantém todos os seus arquivos salvos e sincronizados em todos os seus dispositivos. Um dos diferenciais do *iCloud* é o compartilhamento familiar. Essa funcionalidade permite o compartilhamento de fotos, calendários, localizações e compras feitas no *App Store* por até 6 pessoas da família. Na plataforma, o usuário conta com 5GB espaço gratuitamente e pode expandir o plano para até 2TB. Porém, um ponto negativo é que os valores dos planos são cobrados em dólares e variam entre U$ 0,99 e 19,99 por mês. Além disso, a ferramenta funciona tanto em dispositivos da *Apple* como em computadores com o sistema operacional *Windows*.

- ***Owncloud***: é uma ferramenta *open source* e tem uma proposta um tanto diferente das outras plataformas de armazenamento em nuvem. Enquanto nos outros serviços você deixa a responsabilidade dos seus dados nas mãos de outras empresas, com o *Owncloud* você mesmo cria o seu servidor de armazenamento. Depois de instalá-lo em um servidor você pode acessar seus dados privados em uma interface *web* fácil de usar ou sincronizá-los com seus dispositivos, com sistemas *Android* e *iPhones*. Você pode armazenar seus contatos, calendário, bem como arquivos, armazenar senhas, músicas, filmes e assim por diante. Também permite que você compartilhe de forma segura com outras pessoas e colabore em documentos. A desvantagem do *Owncloud* é que você precisa configurá-lo antes de utilizar e para isso é preciso ter alguns conhecimentos sobre a área, porém nada muito difícil, tendo em vista que no próprio site há centenas de explicações junto com uma comunidade de desenvolvedores.

3.5 Programação Defensiva

Em relação aos projetos e avanços que podem impactar na Segurança Digital, a programação defensiva é resaponsável pela prevenção de falhas ou erros de software, verificação de hardware e ocorrência de entradas e saídas inválidas pelo usuário ou arquivos corrompidos, prevenção de interrupções de hardware e de software, tornando assim o sistema mais seguro possível.

As técnicas de programação defensiva baseiam-se na suposição de que o hardware e o software do sistema não são totalmente confiáveis e, portanto, podem vir a apresentar

comportamento não esperado (CHENG; DEUTSCH; DUTTON, 1990).

A Busca por defeitos e falhas de implementação e/ou especificação visando garantir a funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade dos sistemas e portais. De maneira a reduzir impactos na Segurança Digital.

Segundo (ALMEIDA et al., 2002) algumas das principais técnicas utilizadas na programação defensiva são:

- **Teste de Valores Válidos**: se estão dentro das faixas de valores considerados.
- **Teste de Sincronismo**: assegurando uma correta sequência de eventos.
- **Teste de Tempos de Execução**: se estão dentro de padrões pré-especificados.
- **Verificação da Capacidade**: a capacidade máxima não deve ser excedida.
- **Teste de *Time-outs***: Se o tempo de o fluxo de processamento.
- **Teste de Áreas de Memória**: assegurando acesso correto a dados ou ao código.
- **Tratamento de Exceções**: exceções consistem em condições de erro.
- **Verificação de Argumentos de Funções**: dentro de limites pré-determinados.
- **Códigos de Retorno de Erros**: os códigos de erros gerados.
- **Retorno de Sub-rotinas**: se está executando ações de forma incorreta.
- **Controle de Laços**: pra assegurar a correção das condições de controle do laço.
- **Testes de Entrada/Saída**: evitar a reentrância causada por desvios impróprios.

3.6 Redundância

Na arquitetura dos projetos e avanços que podem impactar na Segurança Digital, tem-se a tática de Redundância nos sistemas de informações. Sendo assim, podemos dizer que a forma mais utilizada para a prevenção dos efeitos de falhas em Sistemas é a utilização de **módulos redundantes**.

Há quatro formas para que se faça implementação de redundâncias em um Sistema, que são: a **redundância de *hardware***, **de *software***, **de informação** e **redundância temporal**.

3.6.1 Redundância de Hardware

A Redundância de *Hardware* de acordo com (JOHNSON, 1989) implica na inclusão de circuitos de *hardware* adicionais ao mínimo necessário para o funcionamento do sistema. A redundância de *hardware* pode ser implementada através de três formas básicas:

- **Redundância Estática**: utiliza o mascaramento de falhas como principal técnica e o projeto é feito de forma a não requerer ações específicas do sistema ou de sua operação em caso da ocorrência de falhas;
- **Redundância Dinâmica**: implica na detecção de falhas, caso em que o sistema deve tomar alguma ação para anular seus efeitos, o que normalmente envolve uma reconfiguração do sistema;
- **Redundância Híbrida**: consiste na combinação de técnicas estáticas com técnicas dinâmicas. Utiliza mascaramento de falhas para prevenir que erros se propaguem, detecção de falhas e reconfiguração para remover, do sistema, unidades com falha.

3.6.2 A Redundância de *Software*

A Redundância de *Software* segundo (JOHNSON, 1989) implica na geração de versões distintas do *software* do sistema ou de partes desse *software*, sempre se baseando em uma especificação comum.

3.6.2.1 *Software* para Sistemas Críticos

Conforme (JOHNSON, 1989) em função da dificuldade da comprovação da não existência de falhas na implementação de um *software*, em relação à sua especificação, são utilizadas técnicas de redundância de *software*, cujo objetivo é tornar o *software* mais robusto em relação à segurança, ou seja, tolerante a falhas porventura ainda existentes.

3.6.2.2 Processo de Desenvolvimento de *Software* para Sistemas Críticos

Nesses tipos de *software* devem ser implementadas todas as normas de seguranças nacionais e internacionais de prevenção, evitando condições perigosas, sem que para isso aumente a complexidade do sistema. As principais etapas no processo de desenvolvimento de um software para Sistemas Críticos são: especificação de requisitos, projeto da arquitetura, projeto dos módulos, testes, integração dos módulos e integração com o *hardware* do sistema.

3.6.3 Redundância de Informação

A Redundância de Informação segundo (JOHNSON, 1989) implica na inclusão de informação adicional àquela estritamente necessária ao funcionamento do sistema, como por exemplo bits de paridade, códigos de detecção e correção de erros e checksums, dentre outros.

3.6.4 Redundância Temporal

Por fim, a Redundância Temporal de acordo com (JOHNSON, 1989) consiste na repetição de cálculos e a comparação de seus resultados, possibilitando a detecção de possíveis falhas transientes e intermitentes no hardware.

3.7 Análises e Medidas a Serem Adotadas

Todos os projetos e avanços realizados até o presente momento são elaborados por meio de análises e medidas a serem adotadas observando cuidadosamente todos os possíveis impactos na Segurança Digital, com a finalidade de prevenção contra falhas, que permitiu a elaboração de um Manual de Normas e Procedimentos de Segurança Física e Lógicas em Sistemas de Informação, cujas regras básicas a serem adotadas são:

- **Definir responsabilidades e orientar**: a conduta dos profissionais e usuários do sistema na utilização dos recursos computacionais, visando proteger a integridade e confidencialidade das informações, e manter a continuidade operacional do sistema;
- **Direito à Propriedade**: Os programas homologados e instalados nos computadores e nos servidores de rede são propriedade exclusiva da instituição, sendo vetada sua cópia parcial ou integral.
- **São reconhecidos como usuários desse sistema**: os Funcionários devidamente registrados no quadro de empregados da instituição; os Estagiários (com a devida autorização da chefia).
- **Atribuição exclusiva do Departamento de Segurança da Informação (DSI)**: - Definir e divulgar as medidas de Segurança da Informação; - Instalar ou remover componentes, fazer manutenção e controlar *hardware* e *software*; - Homologar *hardware* e *software*; - Autorizar tecnicamente a aquisição de *hardware* e *software*; - Realizar auditorias de *hardware* e *software*, com finalidade de garantir a proteção dos recursos computacionais e seu uso exclusivo nas atividades da instituição; - Adquirir serviços de informática.

- **Atribuições do Usuário**: - Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho; - Responder pelo uso exclusivo e intransferível de suas senhas de acesso. Em caso de dúvidas, solicitar orientação ao DSI; - Adquirir conhecimento técnico necessário para a correta utilização dos recursos; - Relatar prontamente ao Representante do DSI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, vírus, acesso indevido ou desnecessário a pastas / diretórios de rede, acesso indevido à Internet, programas instalados sem conhecimento do DSI etc; - Não tentar obter acesso não autorizado a sistemas ou recursos de redes de computadores internas ou externas; - Assegurar que as informações e dados de propriedade da instituição não sejam disponibilizados a terceiros, a não ser com autorização por escrito de um Superintendente; - Relatar ao representante do DSI a possibilidade de instalação de um novo *software* ou aquisição de novo *Hardware* para a melhoria dos serviços prestados.

- **Atribuições dos Diretores e Gerentes**: - Zelar pelo cumprimento destas normas e procedimentos e notificar imediatamente ao DSI quaisquer vulnerabilidades e ameaças de quebra de segurança; - Educar os funcionários sobre os princípios / procedimentos de Segurança da Informação, bem como lhes assegurar treinamento para o uso correto dos recursos, visando evitar falhas e danos ao funcionamento dos sistemas; - Solicitar ao DSI autorização para acesso do usuário aos sistemas de informação, bem como atualizar as solicitações de autorização sempre que houver alterações nos sistemas ou funções nas áreas de atuação; - Advertir formalmente o usuário e aplicar as sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente fato ao DSI; - Antes de aprovar a solicitação de compra ou alteração de hardware e software, assegurar que o profissional responsável do DSI foi consultado e efetuou a autorização técnica;

- **Os *backups***: devem ser guardados em local seguro, separados dos equipamentos, para viabilizar a recuperação dos dados.

- **Todos os usuários receberão login e senha**: exclusivos para sua utilização e é obrigatório que todos os usuários tenham senhas individuais de difícil descoberta. Os usuários desligados terão suas contas bloqueadas imediatamente, assim como o acesso a qualquer recurso da empresa.

- **Todos os recursos de rede de computadores**: deverão ser utilizados exclusivamente para fins profissionais, que envolvam atividades relacionadas ao bom andamento dos serviços e processos da instituição.

- **Todos os computadores da instituição**: devem ter antivírus instalado e atualizado periodicamente, é proibido desinstalar e utilizar computadores sem antivírus

instalado.

- **É expressamente vedado aos usuários**: a instalação ou remoção de programas de computador, componente e periféricos; é proibido aos usuários conectar computadores pessoais ou de terceiros à rede coorporativa da instituição.

- **O acesso a Internet**: disponibilizado na instituição para viabilizar a busca de informações ou agilizar determinados processos da empresa. Todo o acesso à Internet através da rede coorporativa da instituição será controlado com a realização de auditorias nas páginas consultadas. Serão desenvolvidos relatórios com nomes, páginas consultadas, tempo de consulta. Não é permitido enviar, baixar (*download*) ou manter arquivos de imagens, musicas, vídeo, arquivos executáveis em geral ou quaisquer outros de caráter pessoal. É proibido o acesso a sites do gênero relacionamento, dos qual fazem parte de redes sociais: *facebook*, etc.; Não é permitido o acesso a sites de Internet com conteúdo pornográfico, jogos, batepapo, *chat*, *blogger*, *cartoon*, relacionamento, música, *hacker* ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia, senhas ou outros eventos de segurança; É proibido o acesso a sites, a instalação e a utilização de programas de troca de mensagens instantâneas ou arquivos do tipo: *WhatsApp*, ICQ, *Messengers*, *Yahoo Messenger*, *BitTorrent*, *iMesh*, *AudioGalaxy*, Programas P2P tipo *Emule* (compartilhamentos de dados), *Napster* e outros. A utilização de sites do tipo *Proxy* é proibida e será considerada falta grave.

- **Penalidades**: - O DSI alerta todos os usuários que a instalação ou utilização de *software* não autorizados constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena de detenção e multa.

- **Todos os usuários são responsáveis**: pelo uso correto das ferramentas eletrônicas de propriedade dos sistemas críticos.

- **Todas as práticas que representam ameaça à segurança da informação**: serão tratadas com a aplicação de ações disciplinares e severas.

Portanto, na ocorrência de infrações a este Manual, ou às determinações constantes de comunicações externas ou internas, ou mesmo às ordens de superiores hierárquicos, quando for o caso, ficam os infratores sujeitos às seguintes penalidades: advertência verbal, advertência por escrito, suspensão, demissão sem ou com justa causa e/ou outras medidas judiciais cabíveis.

Todos os usuários de informática passam a receber uma cópia deste Manual, dando ciência de seu conteúdo. Os novos colaboradores/usuários receberão o mesmo material por ocasião de sua admissão na instituição. Sendo assim a instituição se reserva o direito de

atualizar, alterar, anular toda ou em parte as normas aqui contidas, a qualquer momento e sem aviso. Uma versão atualizada deste manual estará sempre disponível na Intranet o no quadro de avisos da instituição.

Esse tipo exemplificado de Manual de Normas prevê algumas medidas de segurança observadas, porém requer uma constante atualização de acordo com as novas formas de segurança da informação para evitar que esta possa ser violada.

3.8 Ferramenta para *PenTests* e Auditorias

Foram realizados estudos sobre analises e testes com softwares diversos relacionados à segurança da informação e foram coletados pontos chaves de informações sobre as melhores ferramentas e o modo como são efetuadas as auditorias digitais em livros, artigos e sites. Os levantamentos mais pertinentes ao contexto do trabalho são apresentados a seguir. As organizações utilizam diferentes tipos de avaliações de segurança para avaliar o nível de segurança em seus sistemas.

Cada tipo de avaliação requer um tipo especifico de aplicação. Tipos de ferramentas com funcionalidades do tipo:

- Aquisição de Informações;
- Análise de Tráfego;
- Análise de Senhas;
- *Wireless Hacking*;
- *Scanner* de Vulnerabilidades;
- *Scanner* de Aplicação *Web*;
- *Scanner* de rede.

De acordo com (UTO, 2013) para realizar qualquer teste de invasão, um conjunto mínimo de ferramentas deve estar disponível, independentemente de serem livres ou pagas. O ideal é que o auditor prepare um notebook, com bom processador e bastante memória, instalando uma ou mais ferramentas de cada classe, com as quais se sinta à vontade para trabalhar.

Conforme (SÊMOLA, 2014) realizar uma análise de segurança já é prioridade para a grande maioria das empresas, o que vem demonstrar a percepção da necessidade de diagnosticar os riscos.

Na **Aquisição de Informações** é a maneira usada pra encontrar os dados importantes nas maquinas ou usuários do sistema. Segundo (UTO, 2013), a fase de reconhecimento tem por objetivo levantar o máximo possível de informações da aplicação alvo, principalmente nos casos de teste caixa-preta, em que quase nada é fornecido de antemão ao analista de segurança.

Na **Análise de Tráfego** são utilizadas ferramentas capazes de fazer análises de tráfego em toda a rede, para obter informações das conexões das máquinas, usuários na rede e tipos de pacotes. De acordo com (REIS; GEUS, 2002), existem vários programas que podem ser usados para capturar o tráfego de rede, denominados *sniffers*.

Além de capturar os *datagramas* que trafegam na rede (não importando o endereço destino do *datagrama*), os *sniffers* podem decodificá-los e exibi-los em um formato mais legível, ou ainda executar operações mais complexas como reconstrução de sessão e recuperação de arquivos transferidos pela rede.

Tem-se as ferramentas de **Análise de Senhas**, sendo capazes analisar possíveis senhas salvas em maquinas ou aplicações usadas por diversos usuários. Segundo (WEIDMAN, 2014) é possível provavelmente encontrar credenciais de trabalho mais facilmente por meio da alimentação de suposições sobre as senhas corretas em uma ferramenta de login automatizada.

Foram pesquisadas as ferramentas ***Wireless Hacking*** que são capazes de testar o quanto a rede sem fio esta segura a possíveis ataques. Segundo (DUARTE, 2003), as análises baseiam-se no protocolo das redes sem fio e nas possíveis configurações dos dispositivos.

Para o ***Scanner* de Vulnerabilidade** temos as ferramentas capazes de enxergar as vulnerabilidades de toda a rede, das portas, das máquinas e usuários nela existente. Já o ***Scanner* de Aplicação *Web*** são utilizadas essas ferramentas capazes de varrer as aplicações *Web*, em busca de possíveis vulnerabilidades. Segundo (UTO, 2013), estas ferramentas têm por objetivo encontrar, de maneira automatizada, o maior número possível de vulnerabilidades em um ativo. O mecanismo básico de funcionamento consiste no envio de requisições e análise das respostas obtidas, em busca de evidências de que uma dada vulnerabilidade está presente.

E, por fim, ***Scanner* de Rede** são utilizadas ferramentas que são capazes de varrer toda a rede, para ganhar a dimensão total das máquinas, usuários nela existentes e portas. De acordo com (REIS; GEUS, 2002), o estado da rede provê informações valiosas acerca das conexões de rede em andamento e dos processos aguardando uma conexão.

Na Tabela 2 da próxima página, temos alguns exemplos de ferramentas utilizadas para realização de *PenTests* classificando-as de acordo com suas funcionalidades principais.

Tabela 2 – Exemplos de Ferramenta para *PenTests*.

Funcionalidades	**Ferramentas**	**Fornecedores**
Aquisição de Informações	- *Everest Ultimate Engineer* - *Produkey*	<http://www.solvusoft.com> <http://www.nirsoft.net>
Análise de Tráfego	- *NetConnectChoose* - *Wireshark*	<http://www.nirsoft.net> <https://www.wireshark.org/>
Análise de Senhas	- *WebBrowserPassView*	<http://www.nirsoft.net>
Wireless Hacking	- *Dumpper* - *Wireless Network Watcher*	<https://sourceforge.net> <http://www.nirsoft.net>
Scanner de Vulnerabilidades	- *Nessus* - *Metasploit*	<https://www.tenable.com> <https://www.metasploit.com/>
Scanner de Aplicação *Web*	- *WebSiteSniffer* - *Burp Suite*	<http://www.nirsoft.net> <https://portswigger.net>
Scanner de rede	- *SoftPerfect Network Scanner* - *Nmap* - *CurrPorts*	<https://www.softperfect.com> <https://nmap.org/> <http://www.nirsoft.net>

3.9 Certificações

Com a onda crescente de ataques cibernéticos, as constantes falhas de segurança dos sistemas, muitos vazamentos de informações sigilosas ocasionadas por invasores ou funcionários insatisfeitos, muitas empresas e pessoas estão sendo *hackeadas* tendo seus arquivos criptografados e pedindo resgate pelas informações ou vendendo os dados a terceiros para uso indevido.

Atualmente, os usuários se tornam cada vez mais dependentes dos avanços tecnológicos, o que acarreta no aumento em relação a preocupação das pessoas e empresas em relação à segurança da informação. Consequentemente, se torna crescente a necessidade de profissionais altamente qualificados a desenvolver projetos e avanços tecnológicos na área de Segurança Digital.

Sendo assim serão abordadas as principais Certificações de Segurança, que os profissionais da área deverão se aperfeiçoar e assim, se torna um especialista no ramo de segurança.

Segundo (PACE, 2017), as cinco certificações de segurança mais exigidas no ano de 2017 aos profissionais atuantes na nessa área, foram:

- ***Certified Information Systems Security Professional*** **(CISSP)**: é considerada como uma das Certificações de Segurança mais reconhecida mundialmente. Tem destaque por ser reconhecida pelas maiores e melhores empresas do mundo de tecnologias. A prova composta por 250 questões para ser respondida em 6h de duração, após passar na prova deverá ainda comprova a experiência prévia em Segurança da Informação, para começar valer a certificação.

- ***Certified Information Systems Auditor* (CISA)**: é uma Certificação de Segurança oferecida pela *Information Systems Audit and Control Association* (ISACA) tem como foco o controle, auditoria e monitoramento de segurança dos ambientes de tecnologia da informação. Realiza um exame fazendo mais de 450 pontos (de um total 800 pontos) e comprovar no mínimo 5 anos de experiência na área de segurança. Assim estará apto a trabalhar com auditoria de sistemas de informação, em qualquer lugar do mundo.

- ***Certified Information Security Manager* (CISM)**: é uma Certificação de Segurança oferecida pela *Information Systems Audit and Control Association* (ISACA), tem como foco no gerenciamento da segurança da informação dentro das empresas. A prova tem 200 questões que vão medir as habilidades do candidato no desenvolvimento e gerenciamento de programas de segurança da informação, além de sua capacidade de gestão de respostas a incidentes de segurança que venham a ocorrer. Deve comprovar 5 anos de experiência na área. Assim estará apto a trabalhar como executivo ou estratégico na empresa quando o assunto for Segurança da informação.

- ***Certified Ethical Hacker* (CEH)**: é uma Certificação de Segurança oferecida pela *International Council of Electronic Commerce Consultants* (EC-Council). A prova tem 125 questões. E deve comprovar, no mínimo, 2 anos de experiência prévia em Segurança da Informação. Esses profissionais possuem o conhecimento operacional das técnicas e ferramentas de *hacking* para trabalhar do lado legal da segurança. São capazes de encontrar vulnerabilidades, explorar sites e encontrar fraquezas para prevenir as empresas de ataques maliciosos externos (ou internos).

- ***CompTIA Security+***: é uma Certificação de Segurança oferecida pela *Computing Technology Industry Association* (CompTIA). Reconhecida no mercado mundial. Os profissionais com este certificado tem conhecimento gerais da segurança como um todo, cobrindo o essencial da segurança de rede, gestão de riscos, criptografia, gerenciamento de identidades, segurança de sistemas e de sistemas organizacionais.

Na Figura 10 da próxima página são mostrados resultados de uma pesquisa informal realizada pelo (STRONG SECURITY, 2016). Onde os dados indicam o número de postos de trabalho em todo o país *United States of America* (USA) em que nossas certificações existentes foram mencionados em um determinado dia. Os dados devem dar uma ideia da popularidade relativa de cada certificação.

Observa-se que na pesquisa realizada no ano de 2016 temos como exemplo também da certificação *GIAC Security Essentials* (GSEC) entre as já citadas anteriomente pelo outro autor.

Figura 10 – Melhores Certificações de Segurança da Informação em 2016

	SimplyHired	Indeed	Dice	LinkedIn	TechCareers	JustTechJobs	Total
CEH	3,789	2,364	288	1,197	2,354	234	10,226
CISM	69,997	3,965	645	1,447	8,689	366	85,109
CISSP	66,939	13,271	2,014	6,013	12,755	1,401	10,2393
GSEC	2,101	1,581	218	651	266	177	4,994
Security+	3,497	2,772	226	999	468	328	8,290

Fonte: Strong Security (2016)

GIAC Security Essentials **(GSEC)**: é uma Certificação de Segurança para profissionais qualificados para aplicações de tarefas de segurança relacionadas a uma ampla gama de sistemas de tecnologia de informação.

Quanto as certificações que impactam na Segurança Digital nas empresas:

- **Certificação ISO/IEC 27001**: em Gestão de Segurança da Informação, que segundo (BSI, 2017) tem como objetivo manter as informações confidenciais, a integridade e a disponibilidade de informações e proteger as informações das partes interessadas, incluindo os seus clientes, colaboradores, parceiros de negócios e as necessidades da sociedade em geral; com um sistema certificado pela ISO/IEC 27001 e mostrando que mantém os riscos de segurança da informação sob controle. A conformidade com normas de nível mundial pode ajudá as empresas a conquistar a confiança dos clientes e novas oportunidades de negócios. A instituição passa por uma auditoria formal, caso não encontre vulnerabilidades receberá um certificado ISO/IEC 27001, válido por três anos. O auditor manterá contato durante este período, visitando-o regularmente, para averiguar a continuidade da Certificação.

Observações: *International Organization for Standardization* (ISO) - Organização Internacional de Normalização, sendo uma entidade de padronização/normalização em vários países. Já a Comissão Eletrotécnica Internacional (IEC) - é uma organização internacional de padronização de tecnologias elétricas, eletrônicas e áreas relacionadas, gerando padrões em conjunto com outras organizações.

3.10 Normas técnicas de segurança digitais mais conhecidas: brasileiras e internacionais

Conforme (ANYCONSULTING, 2017) As normas técnicas determinam regras, diretrizes e características mínimas para atividades ou resultados. Elas são aprovadas por um organismo reconhecido e as empresas que atendem suas exigências podem receber uma comprovação de excelência quando auditadas.

Em muitos casos, clientes exigem que as companhias possuam determinadas certificações para fecharem negócios, já que assim eles garantem que serviços e produtos sejam oferecidos de acordo com boas práticas internacionais, que podem ser de gestão, segurança, inovação ou processo. Seu principal objetivo é garantir confidencialidade, integridade e disponibilidades da informação, fatores esses essenciais para um sistema corporativo seguro.

Ainda segundo (ANYCONSULTING, 2017) para que as instituições sejam certificadas, elas passam por auditorias realizadas por entidades certificadoras, que checam todos os processos e conformidades. O processo de obtenção do certificado pode variar de acordo com o serviço, produto ou o porte da companhia, mas geralmente inclui aplicação das diretrizes da norma, análise de documentação, realização de auditorias internas para verificação de inconformidades, adequação e auditorias externas.

A partir de 2005, começaram a ser publicadas as normas da série 27000, que serão abordadas neste capitulo, anfatizando as normas mais conhecidas e seguidas como modelo de segurança digital.

A ISO/IEC 27001 segundo a (BSI, 2017) é a norma internacional de gestão de segurança da informação. É aprovada pelos órgãos reguladores *International Organization for Standardization* (ISO) e pela Comissão Eletrotécnica Internacional (IEC) para utilização internacional. Ela descreve como colocar em prática um sistema de gestão de segurança da informação avaliado e certificado de forma independente.

Isso permite que o usuário proteja todos os dados financeiros e confidenciais de maneira mais eficiente, minimizando a probabilidade de serem acessados ilegalmente ou sem permissão. Com a norma ISO/IEC 27001, o usuário poderá demonstrar compromisso e conformidade com as melhores práticas globais, provando a clientes, fornecedores e partes interessadas que segurança é fundamental na operação de sua empresa.

Os benefícios da norma ISO/IEC 27001 em Gestão de Segurança da Informação segundo a (BSI, 2017), são:

- Identificação de riscos e definição de controles para gerenciá-los ou eliminá-los;
- Flexibilidade para adaptar os controles a todas as áreas ou a áreas selecionadas de

sua empresa;

- Ganhe a confiança das partes interessadas e dos clientes, que sabem que seus dados estão protegidos;
- Demonstre conformidade e obtenha o status de fornecedor preferencial;
- Atenda às expectativas mais sensíveis, demonstrando conformidade;

De acordo com (LRQA, 2017) a publicação da ISO/IEC 27009 fornece um modelo no qual a ISO/IEC 27001 ou a ISO/IEC 27002 podem ser aprimoradas ou refinadas para incluir os requisitos específicos do setor ou em relação ao qual os requisitos podem ser interpretados para garantir a sua implementação consistente e facilmente compreensível.

Esta abordagem se baseará nas normas do setor, de tecnologia e de riscos específicos existentes, como a ISO/IEC 27011 (telecomunicações), ISO/IEC 27017 (computação em nuvem) ou ISO/IEC 27032 (cibersegurança) minimizando o risco de duplicação ou confusão. Isso representa uma fase importante para a otimização e racionalização em todos os setores da indústria.

Em (ABNT, 2017), Associação Brasileira de Normas Técnicas (ABNT), publicou a norma ABNT NBR ISO/IEC 27004:2017 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Monitoramento, medição, análise e avaliação, que revisa a norma ABNT NBR ISO/IEC 27004:2010, elaborada pelo Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-021).

Este documento fornece orientações que têm como objetivo auxiliar as organizações a avaliarem o desempenho da segurança da informação e a eficácia do Sistema de Gestão em Segurança da Informação (SGSI) a fim de atender aos requisitos da ABNT NBR ISO/IEC 27001:2013, Norma Brasileira (NBR).

Como auxiliadoras das normas técnicas há as melhores práticas que impactam na Segurança Digital e tratam de temas contemplados na Governança de Tecnologia da Informação (GTI), onde destacam-se o **CobIT** e o **ITIL**:

***Control Objectives for Information and Related Technology* (CobIT)**: é um *framework* de controle dirigido para a governança e gestão de tecnologia da informação. Recomendado pela *Information Systems Audit and Control Association* (ISACA), o CobIT possui recursos que são aplicados como um modelo de referência para a gestão da Tecnologia da Informação (TI).

Aplica um padrão das melhores praticas a partir de uma matriz de domínios, processos e atividades estruturados de forma lógica e gerenciável. Auxiliando na associação entre: os riscos do negócio, as necessidades de controle e aspectos tecnológicos. Os componentes inter-relacionados do COBIT podem ser representados em um cubo.

Atualmente na versão 5.0, lançada em 2012, a ISACA oferece aos profissionais que dominam o conteúdo do COBIT 5, exame para adquirir a Certificação. O exame consiste em 50 questões de múltipla escolha e exige uma pontuação de 50% ou mais para passar.

Benefícios do CobiT:

- Um melhor alinhamento baseado no foco nos requisitos de negócio;
- A orientação a processos;
- Ser baseado em controles;
- Ser direcionado por métricas;
- Uma visão clara para os executivos sobre o que a TI faz;
- Uma clara divisão das responsabilidades baseada na orientação para processos;
- Aceitação geral por terceiros e órgãos reguladores;
- Entendimento compreendido entre todas as partes interessadas, baseado em uma linguagem comum.

Information Technology Infrastructured Library **(ITIL)**: é uma biblioteca composta pelas melhores práticas usadas para o gerenciamento de serviços de tecnologia da informação. Composta por 5 livros principais: **Estratégia de Serviços, Projeto de Serviço, Transição de serviço, Operação dos Serviços e Melhoria Contínua do Serviço**. Também existe certificação para profissional que domina o uso da plataforma ITIL. A prova é aplicada por instituições autorizadas, com duração de 60 minutos durante os quais você deverá responder 40 perguntas do tipo teste. A nota mínima de aprovação é de 65% das questões.

Benefícios do ITIL:

- Maior controle nos processos com menor incidência dos riscos envolvidos;
- Torna os processos de gerenciamento dos serviços de TI mensuráveis;
- Atuação na causa raiz dos problemas, com foco no negócio;
- Definição clara e transparente de funções e responsabilidades;
- Eliminação de redundância de tarefas e ações;
- Maior qualidade nos serviços prestados;
- Elevação dos níveis de satisfação dos usuários internos e clientes com relação à disponibilidade e qualidade dos serviços de TI;

- Redução de custos de TI e aumento do *Return of Investment* (ROI);
- Flexibilidade e menores impactos na gestão de mudanças;
- Processos mais ágeis e organizados;
- Melhor relacionamento com os fornecedores e com os serviços prestados.

3.11 Os Projetos e Avanços das leis voltadas aos *Cybercrimes* no Brasil, que podem impactar na Segurança Digital

Cybercrime ou Crimes Digitais são termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, uma base de ataque ou como meio de crime.

Diante desta situação, surge a necessidade de elaboração de leis específicas para que seja possível punir os diversos crimes digitais ou também chamados de crimes cibernéticos ou informáticos que estão cada dia mais comuns.

O movimento responsável pelo enquadramento destes crimes em dispositivos legais específicos ficou conhecido a partir de 2014 como **Marco Civil da Internet** que estabelece princípios, garantias, direitos e deveres a quem utiliza a rede de computadores e as diretrizes de atuação do Estado.

Os *Cybercrime* indiretamente já podem ser enquadrados em crimes com penas previstas pela legislação existente, através do qual se consegue jugar, condenar e prender varias pessoas que os comete.

Alguns dos exemplos de Lei Federal e Código Penal (CP) brasileiro vigente que podem ser utilizadas aos *Cybercrimes*, são:

- Art. 153, §1-A, CP - Divulgação de Segredo, sem justa causa, informações sigilosas ou reservadas;
- Art. 2, V, da Lei no 8.137/1990 - Crimes Contra a Ordem Tributária;
- Arts. 13, 22 e 23 da Lei 7.170/83 - Crimes contra a segurança nacional;
- Art. 20 da Lei 8.081/90 - Discriminação ou preconceito de raça (Racismo), religião, etnia ou procedência nacional, muito comum de ocorrer pela internet;
- Arts. 33 e 34 da Lei 11.343/06 - Tráfico de drogas;
- Art. 62 da Lei 9.065/98 - Condutas e atividades lesivas ao meio ambiente;
- Art. 122, CP - Induzimento, instigação, auxilio ao suicídio;

- Art. 138, CP - Calúnia, crime contra a honra;
- Art. 139, CP - Difamação, crime contra a honra;
- Art. 140, CP - Injúria, crime contra a honra;
- Art. 147, CP - Crime de ameaça na internet;
- Art. 155, §4, II CP - Furto qualificado mediante fraude;
- Art. 158, CP - Extorsão;
- Art. 163, CP - Dano;
- Art. 168, CP - Apropriação indébita;
- Art. 171, CP - Estelionato;
- Art. 208, CP - Escárnio ou motivo de crença ou função religiosa;
- Art. 214, CP - Atentado violento ao pudor;
- Art. 216-A, CP - Assédio Sexual;
- Art. 228, CP - Favorecimento da prostituição;
- Art. 233, CP - Ato obsceno;
- Art. 234, CP - Escrito ou objeto obsceno;
- Art. 286, CP - Incitação ao crime;
- Art. 287, CP - Apologia de crime ou criminoso;
- Art. 288, CP - Quadrilha ou bando;
- Art. 297, CP - Falsificação de documento público;
- Art. 298, CP - Falsificação de documento particular;
- Art. 299, CP - Falsidade ideológica;
- Art. 307, CP - Falsa identidade;
- Art. 312, CP - Peculato;
- Art. 313-B, CP - Modificação ou alteração não autorizada de sistema de informações ou programa de informática;
- Art. 314, CP - Extravio, sonegação e inutilização de documento;

- Lei Federal nº. 9.970/2000 - Abuso e exploração sexual de menores - Crianças e Adolescentes;
- Art. 241 da Lei 8.069/90, Estatuto da Criança e do Adolescente (ECA) - Divulgação, aquisição e posse de pornografia infantil através da internet. "Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente"
- Art. 154-A, CP da Lei nº 12.737/2012 (conhecida como **Lei Carolina Dieckmann**, onde teve seu computador invadido e publicação de fotos íntimas na *web*) - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal (CP).

Nota-se que que mesmo não possuindo leis especificas para alguns casos específicos de *Cybercrimes*, os juízes podem enquadrar o flagrante delito em qualquer uma das leis já existentes que tenha sua devida relação através das jurisprudências.

Quanto aos tipos de *Cybercrimes* pode-se destacar: crimes comuns ou impuros, aqueles que já eram praticados anteriormente à popularização do computador e da Internet, por exemplo, quando alguém comercializa produtos contrabandeados pela Internet.

Em segundo temos os crimes puros ou crimes de alta tecnologia, que ocorre quando o alvo do criminoso é o próprio sistema de informação. Por exemplo, os ataques de negação de serviço contra sites e os acessos indevidos aos bancos de dados em empresas.

E por fim, os crimes mistos que não visam o sistema de informação, mas se utilizam dele como instrumento indispensável para a prática da infração. Esse tipo de *Cybercrimes* é muito comum em fraudes bancárias utilizando internet banking em alta nos últimos anos, e pode ser enquadrado no Art. 155, §4, II CP - Furto qualificado mediante fraude.

4 Resultados

Esta etapa do trabalho destinou-se às considerações gerais dos resultados sobre deste estudo, bem como, propor soluções ou melhorias aos principais problemas detectados na avaliação de risco, com base nas analises e discussões dos resultados obtidos. Identifica ainda, possíveis propostas de melhorias, sempre adequando à normas especificas a cada caso analisado e sendo satisfatório a defesa das informações.

Foi constatado que um dos principais problemas está no treinamento de profissionais que devem estar aptos a assumir os risco quanto ao desempenho das atividades pertinentes ao tema abordado, seguindo todas as instruções e mecanismos de segurança que evitem possíveis falhas.

Durante a implantação dos projetos e avanços outro problema constatado é o fator humano, pois ter um projeto ou sistema totalmente sem falhas não é o bastante quando se tem usuários ou funcionários vulnerareis, como por exemplo, a engenharia social. O fator humano pode ser considerado como um dos pontos mais vulnerável pois lida com as emoções, por isso deve-se ter treinamentos rotineiros de pessoal dando lhes mais instruções de segurança.

A Política de controle de acesso a informação é importantíssima tendo em vista que pessoas não autorizadas podem gerar muitos prejuízos à empresa. Por isso deve existir normativo interno para consistência entre controle de acesso e políticas de classificação da informação em diferentes sistemas e redes, sugere-se a divulgação deste em toda empresa e o cumprimento do que foi definido.

Foi constatada ainda, a necessidade de identificar as informações relacionadas às aplicações de negócios e os riscos a que estão expostas as empresas, classificando-os e disponibilizando-os corretamente em todos os segmentos da empresa.

Na politica de gerenciamento de acesso de usuário é necessário implementar uma rotina de remoção ou bloqueio imediato de acesso de usuários que mudaram de cargo, função ou deixaram a organização. E ter muito cuidado em lidar com funcionários insatisfeitos.

Quanto ao Controle de acesso à rede, nota-se que este deve ser muito rígido em relação ao que pode ser acessado na rede de computadores, tendo em vista que é inevitável o uso da internet nos dias atuais. Sendo assim recomenda-se que o ambiente de rede seja gerenciado exclusivamente apenas por empregado do Departamento de Segurança da Informação (DSI) e que seja implementada uma rotina para garantir o cumprimento da norma que regulamenta o acesso administrativo a usuários, em suas estações de trabalho.

E por fim, para que os principais problemas sejam detectados e melhorias sejam

adotadas deve-se ter uma constante avaliação de risco aos nossos projetos e avanços que podem impactar na Segurança Digital dos sistemas informativos.

5 Conclusão

O presente estudo abordou os principais projetos e avanços que podem impactar na Segurança Digital, com o intuito de propor uma gestão eficiente para as novas tecnologias em constante crescimento, por isso a necessidade de uma política de segurança da informação para esses dispositivos que manipulam informações importantíssimas voltadas aos usuários.

O desenvolvimento deste trabalho foi realizado com base nas melhores práticas de normas de segurança, objetivando contribuir em sua busca constate em governança de Tecnologias da Informação que detém grande importância na utilização para a empresa especializada nesse ramo de atuação.

Por meio de pesquisas aos meios de comunicação e aplicação de procedimentos aos envolvidos nesses sistemas informativos, verificou-se a necessidade de desenvolver uma política de segurança para os sistemas que disponibilizam informações voltadas ao funcionamento pleno e sem possíveis falhas do sistema uma vez que, além de possuírem tal política, devem existir definições de ações a serem implementadas no segmento estudado.

Os resultados apresentados por meio das pesquisas foram comparados com as analises de risco desses sistemas, verificando-se o grau de adequação com as normas nacionais e internacionais, possibilitando a apresentação das soluções e recomendações pertinentes. O desenvolvimento deste trabalho permitiu definir procedimentos de segurança aos sistemas evitando a parada de seu funcionamento por meio de falhas ou o uso de má fé por parte dos funcionários e ou terceiros.

O desenvolvimento desta monografia permitiu colocar em prática os conhecimentos adquiridos ao longo do curso de Sistemas de Informação (SI) e das pesquisas sobre o assunto abordado, ampliando significativamente os conhecimentos relacionados à segurança da informação. Constando-se assim que todas as empresas deve ser submetidas a avaliação de risco a fim de propor a segurança necessária ao sistema ou as pessoas autorizadas ao acesso.

Como pretensão em trabalhos futuros, espera-se dar continuidade aos estudos e pesquisas em segurança da informação aplicadas em projetos e avanços que podem impactar na Segurança Digital, com atenção especial a prevenção de vulnerabilidades em sistemas. Tal anseio será levado a diante, na medida em que nossos sistemas informativos se tornem mas modernos e avançados. Onde esses estudos forem aplicados a especialização em crimes e auditorias eletrônicas.

Referências

ABNT. *Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação*. ABNT - Associação Brasileira de Normas Técnicas, 2017. Disponível em: <http://www.abnt.org.br/noticias/5557-tecnologia-da-informacao-tecnicas-de-seguranca-sistemas-de-gestao-da-seguranca>. Acesso em: 13 de dezembro de 2017. Citado na página 66.

ALMEIDA, J. R. J. et al. Defensive programming for safety-critical systems. Rio de Janeiro, Brazil, October, p. 21–24, 2002. Citado na página 55.

ANYCONSULTING. *Quais são e para quê servem as normas de segurança da informação?* [S.l.], 2017. Disponível em: <http://www.anyconsulting.com.br/normas-de-seguranca-da-informacao/>. Acesso em: 13 de dezembro de 2017. Citado na página 65.

BBC - NOTÍCIAS. *Hacker invade babá eletrônica e grita palavrões para criança de 2 anos*. 2013. Disponível em: <http://www.bbc.com/portuguese/noticias/2013/08/130813_babaeletronica_hacer_pai>. Acesso em: 17 de dezembro de 2017. Citado na página 32.

BONATO, C. da S.; NETO, R. M. F. Um breve estudo sobre biometria. Universidade Federal de Goiás (UFG) – Campus Catalão, 2010. Citado 2 vezes nas páginas 38 e 39.

BSI. *ISO/IEC 27001 Gestão de Segurança da Informação*. [S.l.], 2017. Disponível em: <https://www.bsigroup.com/pt-BR/ISO-IEC-27001-Seguranca-da-Informacao/>. Acesso em: 13 de dezembro de 2017. Citado 2 vezes nas páginas 64 e 65.

CERT.BR. *Estatísticas dos Incidentes Reportados ao CERT.br*. [S.l.], 2017. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 16 de janeiro de 2017. Citado 3 vezes nas páginas 20, 46 e 47.

CHENG, D. Y.; DEUTSCH, J. T.; DUTTON, R. W. 'defensive programming'in the rapid development of a parallel scientific program. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, IEEE, v. 9, n. 6, p. 665–669, 1990. Disponível em: <http://ieeexplore.ieee.org/abstract/document/55196/>. Citado na página 55.

DATACENTER DYNAMICS. *Como três tendências estratégicas vão impactar a Segurança da Informação*. DCD - Group, 2017. Disponível em: <http://www.datacenterdynamics.com.br/focus/archive/2017/02/como-tr%C3%AAs-tend%C3%AAncias-estrat%C3%A9gicas-v%C3%A3o-impactar-seguran%C3%A7a-da-informa%C3%A7%C3%A3o>. Acesso em: 17 de dezembro de 2017. Citado na página 27.

DIAS, C. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books, 2000. 42-44 p. Citado na página 18.

DUARTE, L. O. Análise de vulnerabilidades e ataques inerentes a redes sem fio 802.11 x. *UNESP–IBILCE–São José do Rio Preto*, p. 27, 2003. Citado na página 61.

HENNESSY, J. L.; PATTERSON, D. A. *Computer architecture: a quantitative approach*. [S.l.]: San Mateo, California: Morgan Kaufmann Publishing, 1990. Citado na página 52.

IBLISS DIGITAL SECURITY. *A IBLISS é referência em desenvolvimento e fornecimento de soluções estratégicas para a proteção de negócios e pessoas.* Três categorias: inteligência, digitalização e mesh. Para Leonardo Militelli, sócio-diretor da iBLISS Digital Security, 2017. Disponível em: <https://www.ibliss.digital>. Acesso em: 17 de dezembro de 2017. Citado na página 27.

IORJ - INSTITUTO DE OFTALMOLOGIA DO RIO DE JANEIRO. *O que é Retina.* Brasil, 2017. Disponível em: <http://www.iorj.med.br/o-que-e-retina/>. Acesso em: 30 Out. 2017. Citado na página 40.

ITGI. *COBIT Security Baseline — An Information Security Survival Kit.* ITGI - IT Governance Institute, 2017. Disponível em: <www.itgi.org>. Acesso em: 13 de dezembro de 2017. Citado na página 28.

JOHNSON, B. W. *Design & analysis of fault tolerant digital systems.* University of Virginia: Addison-Wesley Longman Publishing company, Inc., 1989. 584 p. Citado 2 vezes nas páginas 56 e 57.

KASPERSKY. *Bad Rabbit: nova epidemia de ransomware usa sites contaminados.* [S.l.], 2017. Disponível em: <https://www.kaspersky.com.br/blog/bad-rabbit-nova-epidemia-de-ransomware-usa-sites-contaminados/9783/>. Acesso em: 11 de dezembro de 2017. Citado 3 vezes nas páginas 48, 49 e 50.

KOTONYA, G.; SOMMERVILLE, I. *Requirements engineering: processes and techniques.* New York: Wiley Publishing, 1998. 282 p. Citado na página 33.

LRQA. *Atualização do LRQA sobre as Normas ISO: Incorporando as necessidades específicas dos setores aos sistemas de gestão de segurança da informação.* [S.l.], 2017. Disponível em: <http://www.lrqa.com.br/Noticias/2016/incorporando-as-necesidades-especificas-dos-setores.aspx>. Acesso em: 13 de dezembro de 2017. Citado na página 66.

NORSE CORP. *Registro dos Ataques Virtuais em Tempo Real.* [S.l.], 2017. Disponível em: <http://map.norsecorp.com/#/>. Acesso em: 25 de outubro de 2017. Citado na página 20.

O GLOBO. *Hacker consegue entrar em smart TV e filma casal fazendo sexo em sofá.* Por Fernando Moreira, 2016. Disponível em: <http://blogs.oglobo.globo.com/pagenotfound/post/hacker-consegue-entrar-em-smart-tv-e-filma-casal-fazendo-sexo-em-sofa.html>. Acesso em: 18 de dezembro de 2017. Citado na página 32.

OLHAR DIGITAL. *Veja como é um data center por dentro.* [S.l.], 2016. Disponível em: <https://olhardigital.com.br/pro/noticia/veja-como-e-um-data-center-por-dentro/60544>. Acesso em: 06 de dezembro de 2017. Citado 11 vezes nas páginas 16, 22, 32, 44, 78, 79, 80, 81, 82, 83 e 85.

PACE, R. *Top 5 Certificações de Segurança para 2017.* [S.l.], 2017. Disponível em: <http://formuladascertificacoes.com.br/blog/top-5-certificacoes-de-seguranca-2017/>. Acesso em: 13 de dezembro de 2017. Citado na página 62.

REIS, M. A. dos; GEUS, P. L. de. Análise forense de intrusões em sistemas computacionais: técnicas, procedimentos e ferramentas. Universidade Estadual de Campinas, 13083-970, Campinas - SP, p. 10, 2002. Citado 2 vezes nas páginas 25 e 61.

RIBEIRO, G. *Certificado Digital*. [S.l.]: Contábil Estoril - Consultoria e Assessoria Empresarial, 2015. Citado 3 vezes nas páginas 35, 36 e 37.

SCHULZE, M. et al. How reliable is a raid? In: *COMPCON*. San Francisco, CA, March 1: [s.n.], 1989. v. 89, p. 118–123. Citado na página 51.

SENAC. *Fundamentos de Segurança da Informação*. [S.l.], 2011. 45-47 p. Citado na página 45.

SÊMOLA, M. *Gestão da segurança da informação*. Elsevier Brasil, 2014. 133 p. Citado na página 60.

SPORTSLAB. *Dermatoglifia no Esporte*. Brasil, 2017. Disponível em: <http://sportslab.com.br/medicina-esportiva/servicos-produtos/dermatoglifia-no-esporte/>. Acesso em: 30 Out. 2017. Citado na página 40.

STRONG SECURITY. *Melhores Certificações de Segurança da Informação para 2016*. [S.l.], 2016. Disponível em: <https://www.strongsecurity.com.br/melhores-certificacoes-de-seguranca-da-informacao-para-2016/>. Acesso em: 13 de dezembro de 2017. Citado 2 vezes nas páginas 63 e 64.

SYMANTEC. *Internet das Coisas: Protegendo sistemas e dispositivos da IoT*. [S.l.], 2016. Disponível em: <https://www.symantec.com/pt/br/iot/>. Acesso em: 06 de dezembro de 2017. Citado na página 44.

TANENBAUM, A. S. *Redes de Computadores*. Vrije Universiteit Amsterdam, Holanda, 2015. 543-620 p. Citado na página 48.

UOL - CARROS. *Hackers invadem Jeep Cherokee e assumem volante à distância*. 2015. Disponível em: <https://carros.uol.com.br/noticias/redacao/2015/07/22/hackers-invadem-jeep-cherokee-e-assumem-volante-a-distancia.htm>. Acesso em: 17 de dezembro de 2017. Citado na página 32.

UTO, N. *Teste de Invasão de Aplicações Web*. Rio de Janeiro: RNP – Escola Superior de Redes, 2013. 42-65 p. Citado 2 vezes nas páginas 60 e 61.

WEATHERBY, E. *Summary Brief: IoT From the Beginning*. [S.l.], 2016. Disponível em: <https://yourdailytech.com/iot/iot-summary-brief-iot-from-the-beginning/>. Acesso em: 06 de dezembro de 2017. Citado na página 43.

WEBLINK. *Armazenamento em nuvem | Conheça as principais ferramentas*. [S.l.], 2017. Disponível em: <https://www.weblink.com.br/blog/tecnologia/armazenamento-em-nuvem-conheca-as-principais-ferramentas/>. Acesso em: 12 de dezembro de 2017. Citado na página 53.

WEIDMAN, G. *Testes de invasão: Uma introdução pratica ao hacking*. No Starch Press, San Francisco: Novatec Editora, 2014. 20, 29, 198 p. Citado na página 61.

WOOTTON, G. *Internet das Coisas. Uma visão ampla, humana e livre*. [S.l.]: Primeira edição. AURESIDE - Associação Brasileira de Automação Residencial e Predial., 2016. Citado na página 43.

Anexos

ANEXO A – Estudo de Caso: Veja como é um Data Center por Dentro

Este Anexo são materiais não elaborados pelo autor, está sendo utilizado para servirem de fundamentação, comprovação e ilustração. Trata-se de um Estudo de caso realizado pelo (OLHAR DIGITAL, 2016), onde fala em detalhes como é um Data Center por dentro, seus procedimentos de segurança do local, localizado em Cotia em um Data Center da empresa de tecnologia Level 3.

Figura 11 – Data Center Level 3 por Dentro

Fonte: Olhar Digital (2016)

A.1 Veja como é um data center por dentro

Segundo Gustavo Sumares 22/07/2016 17h30 big data computação na nuvem Computadores. Se você utiliza a internet com alguma frequência, com certeza já passou por um data center - mesmo sem saber. Boa parte dos sites, serviços e programas que usamos hoje em dia estão hospedados em máquinas nesses imensos centros de dados, e é em grande parte graças a eles que a internet funciona.

O Olhar Digital realizou ontem uma visita exclusiva a um data center da empresa de tecnologia Level 3, em Cotia. Abaixo, contamos para você para que servem espaços desse tipo, como eles são e como eles funcionam. Confira.

A.2 A empresa

A Level 3 mostrada na Figura 12 é uma empresa de tecnologia de rede voltada para empresas médias e grandes. Isso significa que ela oferece serviços de rede e conectividade para clientes com grandes volumes de dados e tráfegos. E isso significa que ela lida com volumes inacreditáveis de informação. Segundo a empresa, em todo o mundo, mais de 42 terabytes de dados passam por suas redes por segundo. Essas redes, por sua vez, contém mais de 320 mil quilômetros de cabos de fibra óptica.

Figura 12 – A empresa Level 3

Fonte: Olhar Digital (2016)

Cuidar desse tráfego todo exige muita energia. O data center de Cotia possui uma subestação própria capaz de gerenciar até 20 megawatts de potência. Segundo o Secretário de Energia do Estado de São Paulo, a cidade de cotia tem uma demanda agregada de 78MW, o que significa que o data center é responsável por mais de um quarto do consumo de energia da cidade.

Com essa rede imensa, a empresa presta diversos serviços. Clientes podem, no lado mais simples, apenas colocar os seus servidores nos data centers da Level 3. A vantagem disso é que eles se aproveitam da infraestrutura de energia, segurança e refrigeração da empresa. Por outro lado, a empresa também oferece serviços de distribuição de conteúdo, computação na nuvem e armazenamento e gerenciamento de dados na nuvem.

A Level 3 não pode revelar quais empresas são seus clientes por questões de segurança. No entanto, segundo Yuri Menck, gerente de marketing estratégico e comunicações da empresa, a lista inclui grandes empresas e até mesmo alguns games processados na nuvem.

Para atender às demandas desses clientes, no entanto, a Level 3 precisa garantir segurança e confiabilidade de seus serviços. Isso significa que o acesso aos seus servidores deve ser feito apenas por pessoas autorizadas, e que eles precisam garantir que as máquinas funcionem de maneira ininterrupta o dia inteiro, todos os dias do ano.

A.3 Segurança

A segurança já é visível desde a entrada do terreno do Data Center, que exige que todos os visitantes mostrem documentos com foto a seguranças armados. Uma vez liberada a sua entrada, os visitantes ainda precisam ser cadastrados novamente na portaria do Data Center. Nesse momento é decidido o nível de acesso que eles terão: esse nível determina quais áreas do espaço serão acessíveis com o crachá de visitante.

Figura 13 – Porta dupla que garante a passagem de uma única pessoa por vez

Fonte: Olhar Digital (2016)

Chegar nas salas dos servidores é ainda mais complicado. Além de passar por todas essas etapas, os visitantes ainda precisam ser acompanhados por um segurança. Isso porque a porta da sala dos servidores só pode ser aberta por meio de identificação biométrica de um segurança ou de pessoas com alto nível de acesso.

Antes dessa porta, porém, os visitantes (e o segurança que os acompanha) precisam passar por uma porta de acesso único. Trata-se de uma porta dupla Figura 13, que garante a passagem de uma única pessoa por vez. A primeira porta é aberta com o crachá do visitante. Em seguida, ela se fecha atrás dele. Para abrir a porta seguinte, o visitante posiciona seus pés em retângulos no chão e em seguida aperta um botão à sua frente.

Esse processo garante que ninguém pegue "carona" no crachá de outra pessoa, pois o sensor no piso detectaria a presença de mais de uma pessoa e não abriria a segunda porta. E depois dessa verificação ainda há a outra porta citada, que precisa ser aberta com a impressão digital do segurança. É atrás dela que fica a sala com os racks de servidores.

A.4 O Data Center

Se você já viu uma foto de uma sala de data center, você sabe mais ou menos o que imaginar: diversos racks cheios de computadores, servidores, roteadores, cabos e luzes piscantes. Essa também é a paisagem do Data Center VI do edifício da level 3, que foi o que visitamos. Essa Figura 14, no entanto, omite dois detalhes marcantes sobre o interior da sala. O primeiro deles é o frio: dentro do Data Center, a temperatura fica sempre a 17ºC a 20ºC de acordo com Daniel Falbi, gerente de operações em nuvem da Level 3 para América Latina. Isso tem a função de refrigerar as máquinas que operam na sala.

Figura 14 – Data Center

Fonte: Olhar Digital (2016)

Embora a temperatura seja relativamente homogênea, a sala tem corredores “frios” e “quentes”. Isso porque o ar condicionado passa pela frente das máquinas e sai por trás delas mais aquecido. Todo o fluxo de ar da sala é controlado para permitir que a refrigeração seja a mais eficiente possível.

Outro detalhe marcante que a fotografia não revela é o ruído: há muito barulho dentro de uma sala dessas. O principal culpado por isso é justamente o sistema de ventilação da sala. O ar condicionado e os ventiladores ficam ligados continuamente para garantir a refrigeração das máquians. Sem eles, a temperatura dos servidores se elevaria rapidamente, e as máquianas se desligariam para evitar danos.

Em um canto da sala também estavam alguns tanques vermelhos. Os tanques, na Figura 15, contém o gás FM-200, que é utilizado para suprimir incêndios o mais rápido possível caso eles aconteçam. Incêndios que ocorrem em data centers não podem ser apagados com água por conta da imensa quantidade de componentes elétricos envolvidos, daí a necessidade do gás.

Figura 15 – Os tanques contém o gás FM-200

Fonte: Olhar Digital (2016)

A.5 Racks

Os “armários” que lotam as salas dos Data Centers são chamados de “racks”, e são neles que ficam os servidores dos clientes de um data center, Figura 16. Essas máquinas podem conter desde dados empresariais até servidores de jogos online, passando também por diversos outros tipos de conteúdos como vídeos e músicas.

Em sua maioria, o espaço dos racks é ocupado por servidores: computadores especializados em cumprir determinadas tarefas de rede. Essas máquinas podem armazenar e gerenciar dados, por exemplo, e os dados contidos nelas podem ser acessados por usuários de fora. Vídeos do Youtube, posts do Facebook e séries da Netflix são exemplos de dados armazenados dessa maneira, e que podem ser acessados por usuários de fora.

Além de servidores, os racks também contém gerenciadores de carga. Essas máquinas se conectam a diversos servidores que prestam um mesmo serviço, e analisam o tráfego e a capacidade de processamento de cada uma. O trabalho delas é distribuir a carga de trabalho entre o conjunto de servidores, garantindo que nenhuma máquina fique sobrecarregada.

Figura 16 – Racks

Fonte: Olhar Digital (2016)

Também fica nos racks a “coluna dorsal” da rede do data center: os roteadores que ligam as máquinas umas nas outras. Os roteadores incluem dúzias de saídas e entradas

para cabos de rede e de energia. Impressiona a maneira como os cabos são organizados de maneira compacta, com braçadeiras para juntar cabos semelhantes. Mas essa organização é importante: cabos bem organizados facilitam o fluxo de ar, aumentando a eficiência da refrigeração e reduzindo os custos com energia.

Nenhum dos racks ou servidores é identificado pela empresa que os utiliza, apenas por códigos de letras e números. E cada empresa sabe apenas quais são as suas máquinas, mas não quem está utilizando as demais. Trata-se de uma medida de segurança: se por exemplo uma empresa soubesse que um servidor vizinho ao seu, no mesmo rack, estivesse sendo usado por uma concorrente, poderia acontecer um caso de sabotagem.

Muitas das máquinas também possuem painéis e avisos luminosos que informam os operadores sobre possíveis problemas antes mesmo de que eles ocorram. Essas luzes associadas ao ruído do ambiente ajudam a dar a ideia de toda a enorme movimentação de dados que acontece naquelas máquinas.

A.6 Infraestrutura

As salas de energia que alimentam o Data Center ficam atrás de portas trancadas, logo do lado dos racks. A entrada nelas, contudo, só é permitida a técnicos ou pessoas com alto nível de acesso ao ambiente.

Cada sala possui duas fontes de alimentação de energia diferente, embora apenas uma seja utilizada por vez. Isso é feito para garantir que sempre haja energia disponível para as máquinas. Caso uma das fontes apresente alguma falha, ela pode ser rapidamente substituída, sem perda para o funcionamento do Data Center.

Além disso, essa arquitetura redundante permite que as fontes de energia passem por reparos sem que seja necessário desligar as máquinas. Enquanto uma das fontes passa por manutenção, a outra alimenta os racks. A infraestrutura de rede possui uma organização semelhante, e o sistema de ar condicionado também, para garantir que nunca falte às máquinas refrigeração e acesso à rede. O Data Center VI que visitamos é apenas uma das nove salas do tipo, todas com 200m2 a 500m2 de área, contidas no edifício da Level 3. A empresa divide seus centros de dados em salas diferentes por diversos motivos. Primeiramente, esse desenho modular permite que a empresa atualize o equipamento de uma sala enquanto as outras se mantém funcionando.

Além disso, a empresa consegue organizar melhor a disposição dos seus clientes entre as salas para otimizar o consumo de energia. Como algumas tarefas demandam mais processamento e geram mais calor, elas consomem mais energia, e precisam ser melhor distribuídas pelos espaços.

A.7 Energia

Diferentemente das nossas casas, o data center da Level 3 recebe energia diretamente da rede de alta voltagem. Para poder utilizar essa energia, no entanto, o edifício possui também uma usina de transformação, que reduz a voltagem de cerca de 88 a 138 mil volts para tensões que possam ser usadas pelas máquinas, Figura 17.

Mesmo que a rede de energia do país inteira falhe, no entanto, o data center ainda consegue se manter funcionando por meio de geradores movidos a diesel. Os geradores contém combustível suficiente para manter o centro de dados operando por oito dias seguidos, e o acordo da Level 3 com o seu fornecedor de combustível garante que essas reservas possam ser reabastecidas em até quatro horas.

Energia é o grande custo que um data center tem, e por isso o seu gerenciamento é tão importante. Um aumento de 1% na conta de luz de um centro de dados pode ter um impacto imenso em suas finanças, o que motiva a empresa a buscar maneiras de utilizar a energia da forma mais eficiente possível.

Figura 17 – Usina de transformação, que reduz a voltagem de cerca de 88 a 138 mil volts para tensões que possam ser usadas pelas máquinas

Fonte: Olhar Digital (2016)

Além da energia necessária para alimentar as máquinas, a energia usada na refri-

geração é a segunda maior parcela do consumo do data center. Para garantir um bom uso de energia, as empresas desse ramo calculam um índice chamado PUE (Power Usage Efficiency, ou eficiência do uso de força).

Esse índice é calculado dividindo o consumo de energia total do data center pelo consumo de energia das máquinas. Segundo André Magno, o Diretor de Data Center e Segurança da Level 3 Brasil, o data center de Cotia consegue atingir um PUE de 1,8 no geral, com algumas salas específicas chegando a eficiências de até 1,5.