ISSN 1984-6029

O Comunicante

SUMÁRIO

ARTIGOS

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

VOLUME 7 - Nº 2

Junho 2017

ISSN 1984-6029

O Comunicante

SUMÁRIO

ARTIGOS

VOLUME 7
Nº 2
Junho 2017

ESCOLA DE COMUNICAÇÕES

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

"Em nossa carreira, precisamos estar sempre em movimento, para que nunca enferrujemos. Mudar sempre, sempre que possível para melhor, mas mudar. Não deixe nunca que as coisas fiquem paradas, porque a nossa profissão é essencialmente dinâmica."

Marechal Castello Branco

CORPO EDITORIAL

O COMUNICANTE

Revista Científica da Escola de Comunicações

Ano 7 - Nº 2
Junho 2017

ISSN 1968-6029
Escola de Comunicações - EsCom
Escola Coronel Higyno Corsetti

O Comunicante Revista Científica - Escola de Comunicações Volume 7, Nº2(Jun/2017)
Brasília-DF: Escola de Comunicações. 2017 34p; 29,7 cm X 21,0 cm

Publicação Quadrimestral
ISSN 1968-6029
Revista Científica da Escola de Comunicações
1. Escola de Comunicações 2. Defesa 3. Cibernética 4. Ciência & Tecnologia 5. Doutrina 6. Direito 7. Educação 8. Informática 9. Instrução Militar 10. Gestão 11. Meio Ambiente 12. Operações Militares Conjuntas e Singulares.

EXPEDIENTE

O COMUNICANTE

Revista Científica da Escola de Comunicações

A Revista Científica, O Comunicante, publicada pela Escola de Comunicações, busca incentivar pesquisas científicas nas áreas afetas à Defesa e que contribuam para o desenvolvimento da Arma de Comunicações.

OBJETIVOS

- Promover o viés científico em áreas do conhecimento que sejam de interesse da Arma de Comunicações e, consequentemente, do Exército Brasileiro.
- Manter um canal de relacionamento entre o meio acadêmico militar e civil.
- Trazer a reflexão temas que sejam de interesse da Força Terrestre e que contribuam para a Defesa.
- Publicar artigos inéditos e de qualidade.
- Aprofundar pesquisas e informações sobre assuntos da atualidade em proveito da Defesa e difundir aos Corpos de Tropa.

PÚBLICO-ALVO

A revista está voltada a um amplo espectro de pesquisadores, professores, estudantes, militares, bem como, todos profissionais que atuem nas áreas de Defesa, Cibernética, Ciência & Tecnologia, Direito Militar, Doutrina, Educação, Informática, Instrução Militar, Gestão, Meio Ambiente, Operações Militares Conjuntas e Singulares.

PUBLICAÇÃO DE ARTIGOS

Os artigos apresentados para submissão devem ser livres de embaraços. Caso o autor tenha submetido o Artigo a outra revista, ele deverá consultar a mesma a respeito da submissão do artigo a esta Revista Científica, cientificando-se de não estar ferindo direitos de publicação conferidos à revista anterior.

PROCESSO DE AVALIAÇÃO

Os artigos submetidos são avaliados pela Comissão Editorial no que se refere ao seu mérito científico e adequação às regras de apresentação de trabalhos científicos.

Em seguida, os textos são encaminhados aos pareceristas e os mesmos terão o prazo de 30 dias para fazerem a sua avaliação. Os pareceristas não são remunerados e, caso aceitem, terão seus nomes incluídos no Comitê de Avaliadores, publicados a cada volume da revista. A partir das avaliações dos pareceristas, o Comitê Editorial pode decidir editar ou não os artigos submetidos além de sugerir mudanças eventuais de modo a adequar os textos.

Todos os textos submetidos devem vir acompanhados de Carta de autorização para publicação que garantirá seu ineditismo ou, ainda, que apesar de estar concorrendo a publicação em outras revistas, não está ferindo direitos de publicação com terceiros para ser veiculado nesta revista.

Outrossim, nenhum dos organismos editoriais, organizações de ensino e pesquisa ou pessoas físicas envolvidas nos conselhos, comitês ou processo de editoração e gestão da revista se responsabilizam pelo conteúdo dos artigos seja sob forma de ideias, opiniões ou conceitos, devendo ser de inteira responsabilidade dos autores dos respectivos textos.

PERIODICIDADE

A Revista terá a periodicidade quadrimestral (Fevereiro, Junho e Outubro) e se reserva ao direito de realizar edições especiais, além das previstas.

Editorial

O mundo tem evoluído mais nos últimos 30 anos do que no século anterior. Televisões de alta resolução, mídias de armazenamento cada vez menores e com maior capacidade, processadores e chips mais complexos, velozes e funcionais, GPS, *Smartphones, notebooks, tablets,* transmissão de dados de alta velocidade sem fio e motores de busca são apenas algumas dentre inúmeras outras invenções que podem ser citadas.

A celeridade dos eventos que nos cercam tem tornado, mesmo o melhor e mais imbuído estudante, um ser desinformado, em algum campo do conhecimento que seja. O simples fato de dominar somente a tecnologia de emprego de um equipamento pode nos conduz invariavelmente à obsolescência.

Assim, é necessária uma consciência situacional, que nos permita compreender que o presente século nos obriga ao autoaperfeiçoamento constante, não pelo simples receio de sermos ultrapassados, mas pela certeza de que temos muito a dominar no que diz respeito às fronteiras tecnológicas.

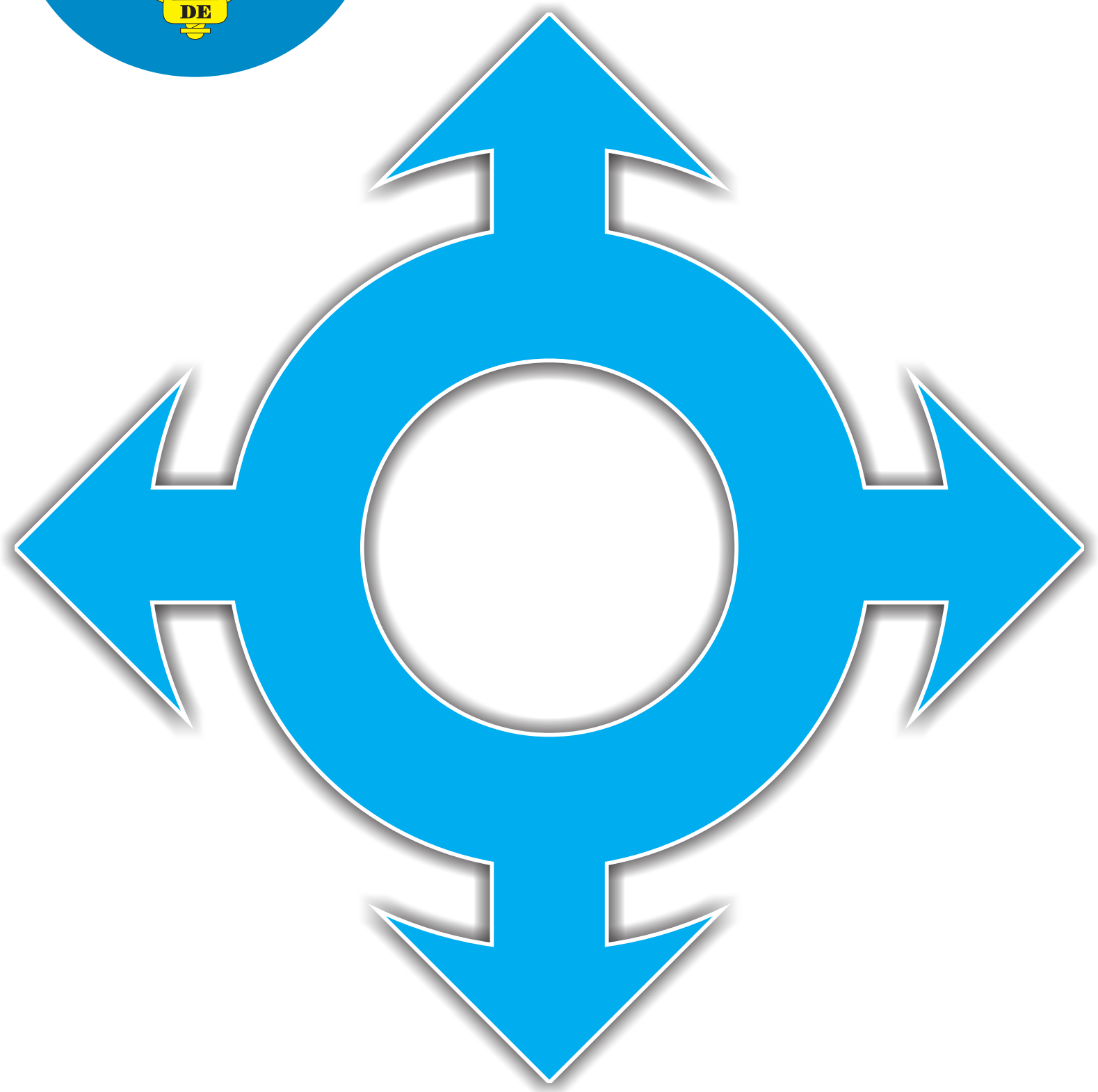
Nesse sentido, é mister aproveitar as oportunidades que surgem, como, por exemplo, a inclusão da Defesa como área de conhecimento no rol das ciências estudadas no Brasil, pelo Ministério da Educação, fato ocorrido em 4 de abril de 2017. Ações como essa tornam a Defesa tema acadêmico corrente no meio universitário, extensivo à sociedade, permitindo maior aproximação da caserna ao meio civil, aos pesquisadores e aos estudantes das instituições de ensino civis e militares. Este, o grande escopo da Revista Científica da Escola de Comunicações.

É nessa empreitada que a Revista se lança aos olhares inquiridores, buscando produzir artigos científicos que se dividam em duas grandes seções: a primeira, de caráter mais técnico, e a segunda, de natureza mais informativa. Ambas, porém, com o objetivo de aguçar e desenvolver o interesse de seus leitores, especialmente nas áreas de Cibernética, Ciência e Tecnologia, Doutrina, Direito, Educação, Informática, Instrução Militar, Gestão, Meio Ambiente e Operações Militares Conjuntas e Singulares.

Assim, reforçamos o compromisso da EsCom com a inovação, com o planejamento e com o autoaperfeiçoamento. Boa leitura a todos. Aguardamos suas inquirições e suas pesquisas.

ÂNDREI CLAUHS – Cel
Comandante da Escola de Comunicações

INFORMATIVO



SEGURANÇA EM NUVEM EM UMA REDE CORPORATIVA

RICARDO REBELO SILVA MELO
Pós-graduado, lato sensu, em Gestão de Segurança da Informação.

RESUMO: Este trabalho apresenta um estudo da tecnologia em segurança na computação em nuvem, desenvolvida por uma empresa de TI voltada para o mercado de virtualização de *Data Center*, que aplica a criação de toda a parte de infraestrutura de rede e segurança virtualizada como *switches, roteadores, firewalls* e além do mais servidores. Essa tecnologia engloba todas as sete camadas do modelo OSI, modelo de rede atualmente utilizada. A ferramenta escolhida para simular o modelo proposto neste trabalho é a VMWare NXS. O uso da ferramenta proporcionou mostrar a criação de dispositivos intermediários de redes criado por meio nova tendência tecnológica SDN *(Software Defined Network).*

Palavras-Chave: segurança em nuvem, SDN.

1 INTRODUÇÃO

No ano de 2008, a expressão Computação em Nuvem começou a ganhar força na área de TI, pois muitas empresas queriam reduzir custos, principalmente, na construção de *Data Center* para armazenamento de dispositivos intermediários.

A computação em nuvem veio para solucionar problemas como utilização de memória e das capacidades de armazenamento de dados em computadores e servidores compartilhados e interligados por meio da Internet.

A computação em nuvem surgiu para que fosse dada mais flexibilidade de provisionamento de serviços escaláveis, aproveitando os avanços da conectividade e as tecnologias de virtualizações, além de mudar a forma de negócios de TI.

A virtualização faz com que os *hardwares* sejam utilizados com mais eficiência e possibilita desacoplar o ambiente de *software* do de *hardware.* Ela permite que os servidores existam como se fosse um único arquivo, uma máquina virtual.

Computação em nuvem vem atingindo fortemente a virtualização em *Data Center.* Esse recurso vem sendo utilizado em *pool,* diversidade geográfica e conectividade universal. Sendo assim, esse tipo de tecnologia facilita o fornecimento de software hospedado, plataforma e infraestrutura como um serviço.

A tecnologia em nuvem pode ser considerada uma nova plataforma tecnológica e uma nova arquitetura para TI.

A computação em nuvens tem algumas características que vão além de acesso a aplicativos via *Internet,* sem que estejam instalados em computadores ou dispositivos específicos (ALECRIM, 2015). Outras características relevantes são:

a) Acesso a aplicativos independente do sistema operacional ou dispositivo utilizado;
b) O usuário não precisa se preocupar com a estrutura para executar a aplicação – *hardware, backup* e outros recursos;
c) Compartilhamento de dados e recursos de infraestrutura de armazenamento se tornam mais fáceis, pois os usuários acessam aplicativos e os dados no mesmo lugar: na nuvem; e
d) Controle e redução de custo, pois o usuário pode pagar por um determinado recurso temporário, saindo da licença integral, que é feito no meio tradicional de fornecimento de *software.*
e) Dependendo do fornecedor, o usuário pode contar com alta disponibilidade do serviço, ou seja, caso um servidor pare de funcionar, outros servidores que fazem parte desta estrutura continuam a oferecer o serviço.
f) Utilização de recursos de infraestrutura de redes e segurança que estão voltadas para virtualização, conhecido com SDN (*Software Defined Network*).

Com todas essas características relacionadas, as empresas começaram a corrida pela tecnologia como o caso da IBM, *Amazon, Google* e *Microsoft* que foram as primeiras empresas a lançarem serviços na nuvem, junto com VMWare e *Openstack* que utilizaram a tecnologia SDN.

Algumas dessas empresas, durante a corrida pelo serviço em nuvem, deixaram de tratar uma preocupação muito importante dessa nova arquitetura: a segurança em computação em nuvem.

A segurança da computação em nuvem vem sendo um grande desafio das empresas para que possa ter interesse em implementar a sua gestão nuvem.

2. SURGIMENTO DA COMPUTAÇÃO EM NUVEM ATRAVÉS DA TI

A Tecnologia da Informação está ligada a diversas áreas, além disso existem diversas definições e nenhuma delas pode ser considerada completa. Portanto, segundo Emerson Alecrim (2013), “a TI pode ser definida conjunto de todas as atividades e soluções

providas por recursos computacionais que visam permitir a obtenção, o armazenamento, o acesso, o gerenciamento e o uso da informação."

A TI possui um legado de conjunto de aplicativos que se comunicam de forma precária e com dados duplicados. Romper esse tipo de tecnologia é um ato considerado muitas vezes inteligente, mas não tão simples, pois as organizações estão em pleno funcionamento e qualquer migração de sistema se torna complexo, com o risco de perda de dados e *downtime* de aplicativos. Pode ocorrer também a falta de recursos para o novo projeto. A infraestrutura precisa ser repensada, pois com o surgimento de aplicativos que podem ser acessados em qualquer lugar do mundo, deixa a antiga infraestrutura de acesso, quase que exclusivamente local, não ser mais utilizada.

A TI é dividida em quatro partes: Sistema de informação, arquitetura, infraestrutura e gestão (VERAS, 2012).

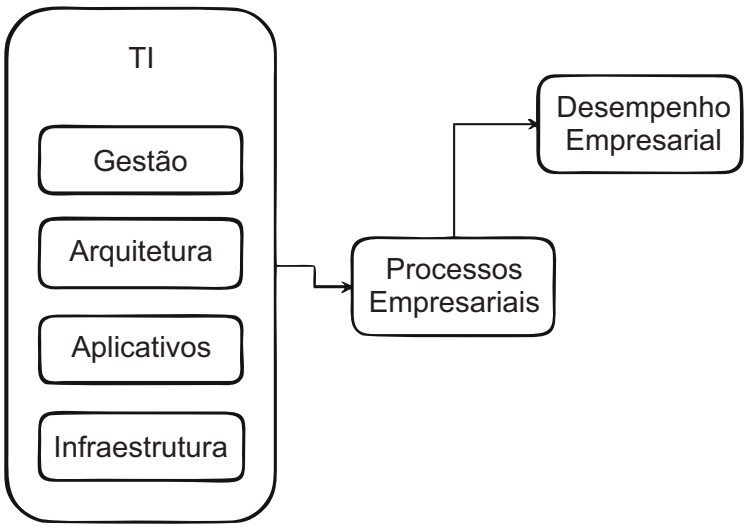
A arquitetura de TI é dividida em duas partes: arquitetura de aplicativos e arquitetura de infraestrutura.

Arquitetura de aplicativos trata de desenhos dos aplicativos, da forma de construção e do seu reaproveitamento, aumentando a eficiência da TI (VERAS, 2012).

A arquitetura de infraestrutura é o alicerce para os aplicativos e sustenta o modelo operacional, modelo que define como os processos serão integrados e padronizados.

A figura 1 mostra que o desempenho empresarial depende exclusivamente do processo empresarial que está diretamente ligado às quatros partes da TI.

FIGURA 1 - TI e desempenho empresarial



Fonte: VERAS, 2012.

A governança de TI está ligada diretamente a gestão da TI. Ela tem como responsabilidade a definição, o provisionamento e a precificação dos serviços compartilhados de TI, que decorrem da infraestrutura, buscando o alinhamento dos níveis destes serviços com as recomendações definidas na estratégia de TI para as aplicações (VERAS, 2012). A governança de TI deve estar de acordo com a estratégia da organização.

2.1. MODELOS DE SERVIÇOS

A computação em nuvem possui sete tipos de serviços em nuvem que podem ser utilizadas por usuários ou organizações:

- IaaS (*Infrastructure as a Service*) – Esse tipo de serviço funciona como aluguel de equipamentos de infraestrutura como: servidores, *rack,* roteadores, *switches* e outras caixas de *hardware.* O usuário não tem muito controle da infraestrutura física, mas sim o controle de virtualização das máquinas virtuais, armazenamentos, aplicativos instalados e recursos da rede. A tarifação desse serviço se dá conforme as quantidades de servidores que serão utilizados ou outros serviços de infraestrutura. Empresas para esse tipo de serviço são: IBM, *Amazon* EC2, *OpenStack, CloudForms* da *Red Hat* e *VmwareIaaS*.
- SaaS (*Software as a Service*) – Esse tipo de serviço funciona com aluguel de *software* e não está relacionado à compra de licença, ou seja, utiliza o *software* e paga por sua utilização. Empresas que fornecem esse tipo de serviço são a *Skype* da *Microsoft* e *Citrix.* O *Skype* é software utilizado para comunicação via telefone VoIP e imagem e sua tarifação ocorre de acordo com que é utilizado e não através de uma licença.
- PaaS (*Platform as a Service*) – Esse tipo de serviço funciona como um meio termo entre o SaaS e o IaaS, é uma plataforma mais robusta e flexível para a utilização de muitos recursos tecnológicos, onde é possível utilizar recurso de *software* e utilizar a infraestrutura necessária para atender à solicitação de um usuário ou uma organização. As empresas que fornecem esse tipo de serviço são *AppEngine* do *Google, Windows Azure* da *Microsoft, CloudFoundry* e *OpenShift* da *Red Hat*.
- DevaaS (*Development as a Service*) – Esse tipo de serviço funciona como ferramenta de desenvolvimento.
- CaaS (*Communication as a Service*) – Esse tipo de serviço funciona como Comunicação

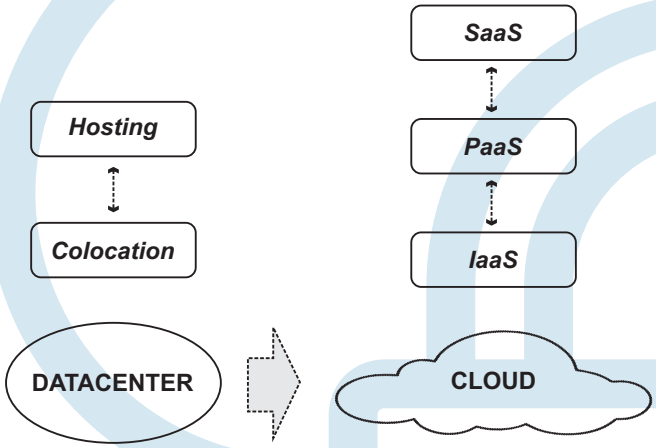
Unificada hospedada em *Data Center* do provedor ou fabricante.

- DBaaS (*Data Base as a Service*) – Esse tipo de serviço funciona como servidor de Banco de dados; e
- EaaS (*Everything as a Service*) – Esse tipo de serviço funciona como tudo, ou seja, engloba todos os tipos de serviço em nuvem.

Neste trabalho serão explicados os três serviços mais utilizados na computação em nuvem que são: IaaS, SaaS e PaaS, em que serão explanados maiores detalhes como comparação entre a arquitetura de computação em nuvem e os serviços tradicionais de *Data Centers*, como as empresas que utilizam esses serviços e o ponto de vista delas em relação ao modelo de serviço.

A figura 2 mostra a arquitetura dos serviços de computação em nuvem e os serviços tradicionais do *Data Center*.

FIGURA 2 - Arquitetura de serviço de computação em nuvem versus Data Center



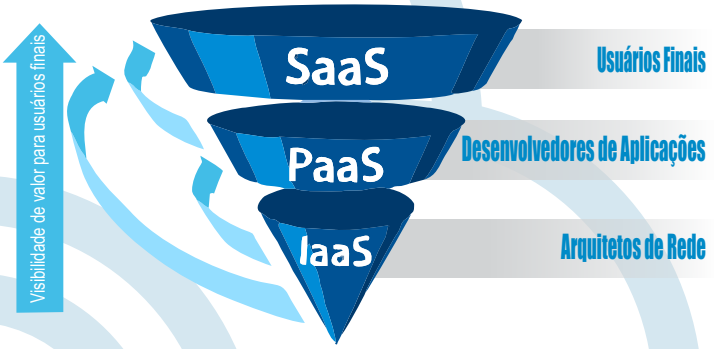
Fonte: VERAS, 2012.

Na arquitetura de serviço do *DataCenter* se destacam dois tipos de serviços que são *Colocation* e *Hosting.*

- *Colocation* – é um *Data Center* independente que oferece hospedagem compartilhada para múltiplos servidores de diversas organizações, ou seja, é um *Data Center* que aluga toda a infraestrutura para instalação do servidor. Normalmente são empresas de mobilidade de alojamento de *web.* Elas alugam a rede e dispositivo de armazenamento de dados, interconectado a vários provedores de serviços de telecomunicações e outros serviços em rede, além de utilizar para o bem próprio a infraestrutura.
- *Hosting* – é uma linha de serviço utilizada para oferecer às organizações um aperfeiçoamento de *hardware* e *software.* O serviço de *hosting* permite ao contratante utilizar a infraestrutura de *Data Center,* incluindo servidores, *Storage* e unidade de *backup,* além de contar com profissionais especializados do provedor para fornecer suporte ao serviço contratado (VERAS, 2012).

A computação em nuvem é um serviço muito mais simples que o *Colocation* e o *Hosting* do *Data Center,* por isso é interessante identificar os papéis desempenhados na arquitetura baseada em nuvem. A figura 3 mostra que consome e fornece o serviço. O IaaS suporta o serviço PaaS, que suporta o serviço Saa.

FIGURA 3 - Principais camadas de computação em nuvem

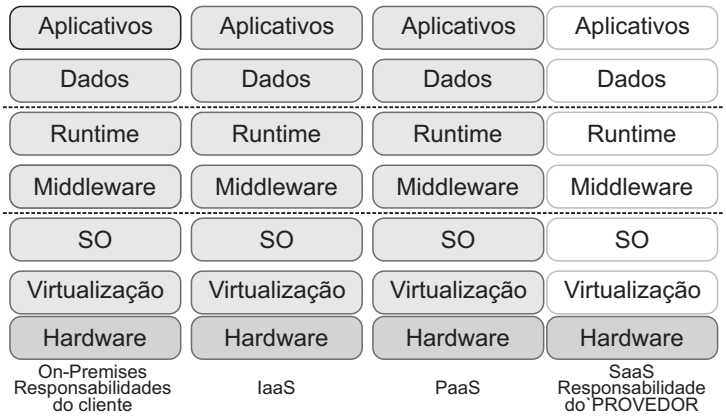


Fonte: BAZANA, 2013.

O provedor de serviço é responsável por gerenciar, disponibilizar e monitorar toda a estrutura da nuvem, deixando os desenvolvedores e usuários sem essa responsabilidade. Com isso o provedor deve possuir os três tipos de serviço e deixar que o usuário pague o que for utilizar. É importante ressaltar que o provedor de serviço não é obrigado a fornecer os três serviços e nem o cliente a contratar os três serviços também.

É interessante comparar os serviços de nuvem com os serviços internos. Os serviços internos possuem os *softwares* de *middleware* e *runtime.* O *middleware* é a designação genérica utilizada para se referir aos *softwares* que são executados entre as aplicações e os sistemas operacionais. O *runtime* é o *software* responsável pela execução dos programas (VERAS, 2012). Portanto, a figura 4 mostra uma relação entre os serviços internos e os serviços da computação em nuvem, em que o serviço de gerenciamento e segurança muda da esquerda para a direta.

FIGURA 4 - Responsabilidade do serviço interno e do serviço da computação em nuvem.

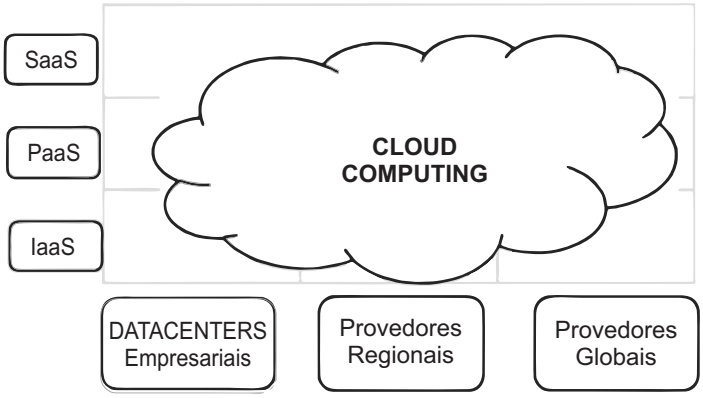


Fonte: VERAS, 2012.

Como pode ser visto na figura 4, o provedor tem total responsabilidade de gerenciamento e segurança pela pilha de TI, já no IaaS, o cliente é responsável pela implantação e pelo gerenciamento da segurança.

Outro aspecto importante é saber onde os serviços de computação em nuvem serão aplicados. Os serviços podem rodar internamente dentro da organização, podem rodar em provedores regionais e provedores globais. É importante destacar que onde os serviços vão rodar vai depender da latência das aplicações e aspectos institucionais. A latência normalmente define que aplicação vai ficar próxima do usuário e os aspectos institucionais definem onde os dados serão armazenados (VERAS, 2012). A figura 5 mostra os serviços de computação em nuvem versus localização.

FIGURA 5 - Serviço de computação em nuvem versus localização.



Fonte: VERAS, 2012.

3 SEGURANÇA NA COMPUTAÇÃO EM NUVEM

A segurança da informação possui alguns princípios que devem ser observados, são eles: disponibilidade, integridade, confidencialidade, autenticidade e não repúdio (BENEVENTO, 2015). Sendo que os princípios de confidencialidade e integridade dependem basicamente de medidas de segurança, tais como: *firewall* ativo como bloqueios e rotas definidas contra vírus, *worms, spyware* e qualquer outro tipo de dano ao sistema.

Como visto, os modelos de serviços em computação na nuvem possuem suas características e funções, com isso é necessário estabelecer algumas recomendações que vão variar de acordo com o modelo. Essas recomendações fazem parte da segurança na computação em nuvem.

Portanto, neste capítulo será abordada a segurança tradicional, disponibilidade, controle de dados por terceiros e as soluções que utilizam *Cloud Computing.*

TABELA 1 – Princípio da segurança em computação na nuvem.

PRINCÍPIOS DE SEGURANÇA	CENÁRIOS DE RISCO
Integridade	Manter os dados sem alteração, ou seja, o dado enviado da origem deve ser o mesmo dado recebido pelo destino. Violação das leis de proteção de dados.
Disponibilidade	Manter o caminho entre a origem e o destino sempre ativo.
Confidencialidade	Os dados transmitidos entre as aplicações de vários usuários utilizando o mesmo sistema de armazenamento.
Autenticação	Verificação do sistema das chaves autenticadoras, (privadas e públicas) entre entidades se comunicam.
Não-repúdio	Garantir que a pessoa não negue que tinha assinado a transmissão da mensagem ou arquivo.

Fonte: autor.

4 CONCLUSÃO

A nova era tecnológica de segurança corporativa em computação na nuvem tornou-se um centro de pesquisa ao longo dos anos para o crescimento das empresas. A segurança vem cada vez mais sofrendo grandes desafios e um destes é tornar a computação em nuvem um sistema com confidencialidade, integridade e disponibilidade.

Conclui-se que a computação em nuvem, mesmo diante de grandes desafios, torna-se uma tendência para se adquirir segurança em nuvem, baseada nas suas características, modelos de serviços e modelo de implantação.

CLOUD SECURITY IN A CORPORATE NETWORK

ABSTRACT

This paper presents a study of cloud computing security technology developed by an Information Technology (IT) company focused on the Data Center virtualization market that applies the creation of all the network infrastructure and virtualized security as switches , Routers, firewalls, and servers. This technology encompasses all seven layers of the OSI model, the currently used network model. Providing the creation of intermediate network devices created through the new technological trend SDN (Software Defined Network).

Keywords: Cloud security, SDN.

REFERÊNCIAS

ALECRIM, Emerson. **O que é cloud computing**. Disponível em: <http://www.infowester.com/cloudcomputing.php>. Acesso em: 02 fev. 2017.

CASTRO, Rita; SOUSA, Verônica. **Segurança em Cloud Computing**: Governança e Gerenciamento de Riscos de Segurança. 2010. 7f. Dissertação (Mestrado Profissional em Computação) – Instituto Federal de Educação, Ciência e Tecnologia do Ceará, Universidade Estadual do Ceará, Fortaleza, 2010.

SANTOS, Alfredo. (2013). **Segurança em Computação na Nuvem**, 1-16, ASIN: B00CR47PFU, Amazon Digital Services, Inc.,USA, May.

VERAS, Manoel. **Cloud Computing**: Nova Arquitetura de TI. 1.ed. Rio de Janeiro: Brasport, 2012. 211p.

O autor é graduado pela UniCeub e Pós-graduado pela Universidade de Brasília. É instrutor da Academia Cisco habilitado a tutoria dos Cursos CCNA1, CCNA2, CCNA3, CCNA 4, IT *Essencial*, IoE, IoT *Fundamentals* e *CiberSecurity*. Atualmente, exerce a função de instrutor da Escola de Comunicações e pode ser contactado pelo email rebelo.melo@eb.mil.br.

MINERAÇÃO DE DADOS EM FONTES ABERTAS: UMA FERRAMENTA DE APOIO AO PROCESSO DECISÓRIO

RAFAEL COSTA BARROS

Pós-graduado, lato sensu, em Gestão de Sistemas Táticos de Comando e Controle

RESUMO: A mineração de dados é fundamental no processo de tomada de decisão. Nos últimos 30 anos o processo de informatização cresceu exponencialmente. Estima-se que em 2020 o tráfego global de dados na *internet* será de 61,386 GBps. Esse crescimento teve como consequência o desenvolvimento da Ciência de Dados. Essa abrange uma grande gama de especialidades relacionadas com a exploração dos dados produzidos. Dentre essas áreas destacam-se: *Big Data*, *Machine Learning*, *Business Inteligence, Data Mining* (Mineração de Dados), *Knowledge Discovery in Databases* (KDD) e *Deep Learning*. Os padrões encontrados em um processo de mineração de dados têm sido utilizados nos mais variados ramos da sociedade: finanças, saúde, telecomunicações, direito, astronomia, biologia, engenharias e ciências da computação, como subsídio para tomada de decisão. Com a evolução do combate, temos um emprego crescente de satélites, aeronaves, *drones,* navios, sensores, radares, mídias sociais, *internet,* que geram um grande volume de dados, dessa forma a mineração de dados se estabelece como uma ferramenta muito útil, ao proporcionar uma análise oportuna dos dados gerados.

Palavras-chave: mineração de dados, processo decisório.

1 INTRODUÇÃO

A mineração apresenta-se como uma ferramenta essencial no processo decisório. O crescimento do volume de informação não é um fenômeno novo, é um processo contínuo ao longo dos anos. No entanto, com o avanço da tecnologia nas últimas décadas, o volume de informação gerado tem crescido cada vez mais rápido. A informação constitui a base do processo decisório. Dessa forma, o grau de êxito em uma decisão será proporcional à confiabilidade das informações obtidas, para a tomada de decisão.

A grande produção de informação tem sido explorada por diversas áreas do conhecimento, acompanhando essa tendência, as forças armadas de diversos países têm utilizado a mineração de dados em proveito do seu emprego, nos mais variados ambientes operacionais. O combate moderno tem acompanhado o avanço da tecnologia e, atualmente, os conflitos modernos caracterizam-se pelo conceito da Guerra Centrada em Redes (GCR), em que os agentes e os sistemas envolvidos no conflito utilizam meios informatizados.

No combate moderno é produzido um grande volume de dados através dos diversos sistemas utilizados, sendo fundamental a utilização de mecanismos que possam selecionar as informações úteis para determinada situação. Uma das soluções para esse fato é a utilização de mineração de dados, que através da análise de padrões dos dados produzidos, consegue selecionar dados de interesse que podem gerar conhecimento através de uma posterior interpretação e avaliação.

2 RESULTADOS E DISCUSSÃO

A partir dos anos 1990, com o advento da internet, a produção de dados cresceu de forma acelerada. Na tabela abaixo, podemos verificar um estudo realizado pela Cisco Systems, em que podemos constatar o crescimento do volume de dados a partir dos anos de 1990, e esse estabelece, ainda, perspectivas para o ano de 2020.

TABELA 1 - Cisco VNI Previsão / Histórico - *Internet*

ANO	TRÁFEGO GLOBAL NA *INTERNET*
1992	100 GB por dia
1997	100 GB por hora
2002	100 GBps
2007	2.000 GBps
2015	20.235 GBps
2020	61.386 GBps

Fonte: Adaptado de Cisco VNI, 2016.

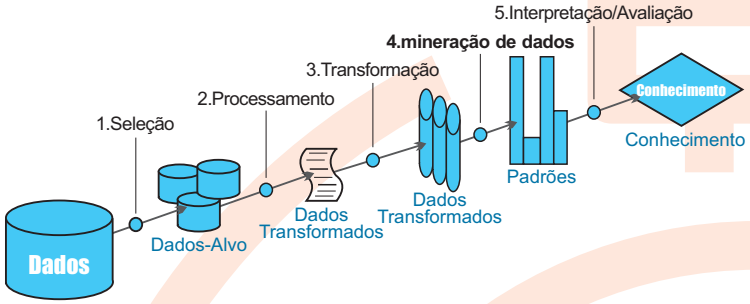
O grande volume de dados produzidos ao longo dos últimos 30 (trinta) anos estabeleceu uma vasta fonte de conhecimento existente na *internet.* Com o avanço da tecnologia, cada vez mais, os mais variados tipos de interações humanas estão sendo estabelecidos em redes informatizadas: atividades econômicas, culturais, sociais e políticas. Esse crescimento teve como consequência o desenvolvimento da Ciência de Dados.

A Ciência de Dados abrange diversas áreas relacionadas aos dados disponíveis na *internet,* dentre elas: *Big Data*, *Business Inteligence*, *Machine Learning*, *Data Mining* (Mineração de Dados), sendo fundamental a distinção entre essas áreas.

O *Knowledge Discovery in Databases* (KDD), descoberta de conhecimentos em base de dados refere-se ao processo completo de obtenção de conhecimento

desde a coleta de dados, a seleção, a transformação, a mineração de dados e a interpretação dos dados, com a finalidade de utilizar esse conhecimento obtido, para uma tomada de decisão. O KDD é o processo não trivial de identificação de padrões válidos, novos, potencialmente úteis e, finalmente, compreensíveis em dados (Fayyad, Piatetsky-Shapiro e Smyth, 1996, p.40).

FIGURA 1 - Descoberta do Conhecimento em Base de Dados



Fonte: Adaptado de (Fayyad, Piatetsky-Shapiro e Smyth, 1996).

A Fig.1 representa o processo de descoberta de conhecimento, em que um determinado volume de dados é submetido a diversas etapas. Após os dados serem coletados, selecionados, processados e transformados inicia-se a fase de mineração de dados, em que serão utilizados padrões, escritos em variadas linguagens de programação, para encontrar dados que atendam ao interesse proposto. Segundo Fayyad, Piatetsky-Shapiro e Smyth (1996, p. 41) a etapa de mineração de dados pode ser de dois tipos: verificação e descoberta. O primeiro consiste em verificação simples de um determinado padrão pré-estabelecido. O segundo possibilita a descoberta de variados padrões.

Os padrões encontrados em um processo de mineração de dados têm sido utilizados nos mais variados ramos da sociedade, como subsídio para tomada de decisão.

De acordo com Han, J Kamber, M Pei, J, (2012, p. 613):

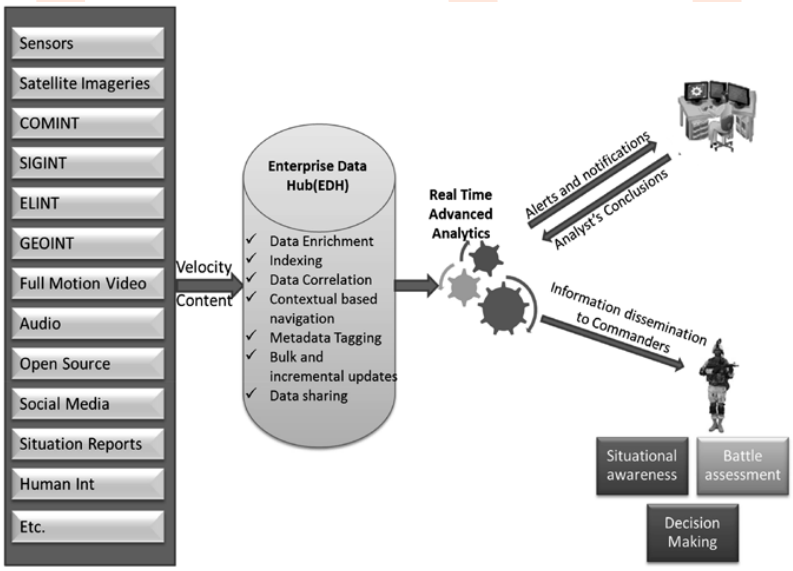
> Enormes quantidades de dados de comunicação humana são produzidas diariamente. Tal comunicação existe em muitas formas, incluindo notícias, blogs, artigos, páginas da *web,* discussões *on-line*, revisões de produtos, *twitters,* mensagens, propagandas e comunicações, na *internet* e em vários tipos de redes sociais. Com isso, a mineração de dados nas Ciências Sociais tornou-se cada vez mais popular. Além disso, os comentários de usuários ou leitores sobre produtos, discursos e artigos podem ser analisados para deduzir opiniões e sentimentos gerais sobre os pontos de vista daqueles na sociedade. Os resultados da análise podem ser utilizados para prever tendências, melhorar o trabalho e ajudar na tomada de decisões.

O combate no século XXI tem como característica o massivo emprego de sistemas informatizados, devido ao surgimento de novas ameaças. O inimigo tornou-se um elemento difuso, diferentemente dos conflitos do século XX, em que eram bem definidos, exigindo uma grande utilização de ferramentas para monitoramento: satélites, aeronaves, *drones,* navios, sensores, radares, mídias sociais, *internet.* Os conflitos modernos são marcados por emprego de *streaming* de vídeo. Todas essas ferramentas geram um grande volume de dados, que necessitam ser utilizados oportunamente. Sendo essencial a utilização de dispositivos que consigam analisar esses dados.

De acordo com Haridas, M, (2015, p.72):

> Hoje, os dados de máquina são gerados pelo movimento de navios, aeronaves e veículos, satélites no espaço, *drones,* veículos aéreos não tripulados, aeronaves de reconhecimento, sensores e radares de vigilância de campo de batalha. Os dados gerados por humanos incluem dados de sites de redes sociais, como *YouTube*, *Facebook, Tweeter,* etc. Os dados comerciais são gerados a partir de todas as transações de comércio eletrônico. Todos esses dados possuem inteligência, que não podemos desperdiçar. Análise de *Big Data* será utilizada para a coleta de informações em um futuro próximo, uma vez que os insumos para inteligência nacional e militar são obtidos continuamente durante a paz e a guerra, essa quantidade cresce exponencialmente durante as crises e as guerras. A análise humana deste volume de informação e dados de inteligência está muito além da capacidade física. Portanto, a grande inteligência baseada em análise de dados fornecerá o resultado necessário para a tomada de decisões e a condução das operações.

FIGURA 2 - Concepção do sistema de coleta de informações de aplicativos baseados em *Big Data*



Fonte: Adaptado de (HARIDAS, M. 2015).

3 CONCLUSÃO

Com o avanço da tecnologia, os processos envolvendo os diversos setores da sociedade tornaram-se informatizados, gerando um grande volume de dados. A mineração de dados em fontes abertas é uma ferramenta essencial em relação a produção de conhecimento em apoio ao processo decisório, pois vivemos em mundo que está amplamente interligado

através dos sistemas informatizados.

Esses produzem um grande volume de dados, que devem ser analisados de forma oportuna. A mineração de dados é uma ferramenta que tem sido utilizada nos mais variados setores da sociedade. Tem sido uma ferramenta muito útil nos conflitos modernos.

O processo de evolução do combate atual está diretamente ligado ao processo de evolução tecnológica. Forças Armadas de diversos países tem empregado equipamentos com alto valor tecnológico agregado e que geram uma expressiva quantidade de dados.

Com as perspectivas de crescimento do volume de dados em combate, é fundamental que as Forças Armadas possuam *expertises* para analisá-los em tempo oportuno, garantindo vantagem em uma situação de emprego.

DATA MINING IN OPEN SOURCES: A TOOL TO SUPPORT THE DECISION-MAKING PROCESS

ABSTRACT

Data Mining is fundamental in the decision-making process. In the last 30 years the informatization process has grown exponentially. It is estimated that by 2020 global data traffic on the internet will be 61,386 GBps. This growth resulted in the development of Data Science. This covers a wide range of specialties related to the exploitation of the data produced. Among these areas are: Big Data, Machine Learning, Business Intelligence, Data Mining, Knowledge Discovery in Databases (KDD) and Deep Learning. The patterns found in a data mining process have been used in the most varied branches of society: finance, health, telecommunications, law, astronomy, biology, engineering and computer science, as a basis for decision making. With the evolution of combat, we have a growing employment of satellites, aircraft, drones, ships, sensors, radars, social media, internet, which generate a large amount of data, with this data mining is established as a very useful tool, by providing timely analysis of the data generated.

Keywords: data mining, decision-making.

REFERÊNCIAS

The Zettabyte Era — Trends and Analysis – Cisco Disponível em <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html>. Acesso em: 27 maio 2017.

Fayyad, U. Piatetsky-Shapiro, G., Smyth P., **From Data Mining to Knowledge Discovery in Databases**, 1996, In: Advances in Knowledge Discovery and Data Mining , pp. 1–34.

Han, J Kamber, M Pei, J, **Data Mining Concepts and Techniques**, Waltham, Elsevier, 3ª Ed, 2012.

HARIDAS, M, **Redefining Military Intelligence Using Big Data Analytics**, Claws: Scholar Warrior, 2015.

O autor é graduado pela Academia Militar das Agulhas Negras e Pós-graduado pela Escola de Comunicações, *lato sensu*, em Gestão de Sistemas Táticos de Comando e Controle. Atualmente, exerce a função de instrutor da Escola de Comunicações e pode ser contactado pelo email rafaelcostabarross@gmail.com.

O EMPREGO DO SISTEMA DE DETECÇÃO DE INTRUSÃO SNORT EM AMBIENTES COOPERATIVOS

RODRIGO ADÃO DA SILVA

Pós-graduado, lato sensu, em Guerra Eletrônica e em Sistemas de Comunicações e Defesa

RESUMO: Este artigo consiste em abordar o emprego do sistema de detecção de intrusão Snort em ambientes cooperativos. A detecção de intrusão é uma das áreas de maior expansão, pesquisa e investimento em segurança de rede de computadores. Com o crescimento da interligação de computadores em todo o mundo, houve um aumento nos tipos e números de ataques contra sistemas de computadores, produzindo uma complexidade muito alta para a capacidade dos mecanismos preventivos tradicionais. Para a maioria das aplicações atuais, a partir de redes corporativas simples para sistemas de *e-commerce* ou aplicações de banco, é praticamente impossível o simples uso de mecanismos para reduzir a probabilidade de ataques. Um ataque pode provocar a interrupção total de serviços, forçando a ocorrência de um lento e dispendioso processo de auditoria, e a restauração manual do sistema. Esse contexto justifica todo o investimento feito, a fim de criar dispositivos que superem a barreira de prevenção simples, garantindo aos sistemas uma operação contínua e correta, mesmo na presença de falhas de segurança. Assim, aparece o Sistema de Detecção de Intrusão ou *Intrusion Detection System* (IDS). Basicamente, o IDS é uma ferramenta inteligente (um sistema de configuração e regras) capaz de detectar intrusões em tempo real e capaz de verificar se um usuário está usando a rede corretamente, produzindo alertas quando detecta pacotes que podem ser parte de um possível ataque. Nesse contexto, aparece o *software* Snort, amplamente utilizado em ambientes cooperativos, como uma solução de aviso sobre a possibilidade de ataques e anomalias em redes de computadores.

Palavras-chave: snort, segurança, detecção de intrusão.

1 INTRODUÇÃO

Com o advento da globalização, cotidianamente, grandes uniões ocorrem nos setores econômico, social, político e cultural, atinentes à sociedade pós-moderna. Como consequência, surgem numerosos problemas relacionados à segurança no campo do tráfego de dados entre os diferentes agentes envolvidos neste processo.

Assim, o espaço permeado pela diversidade de conexões entre parceiros comerciais, clientes - fornecedores, matrizes - filiais, e indivíduos, no qual a rápida troca de informações é um fator determinante de sucesso, é denominado de ambiente cooperativo (NAKAMURA e GEUS, 2004, p. 22).

Ademais,

> o ambiente cooperativo é caracterizado pela integração dos mais diversos sistemas de diferentes organizações, nos quais as partes envolvidas cooperam entre si, na busca de um objetivo comum: velocidade e eficiência nos processos e nas realizações dos negócios (NAKAMURA e GEUS, 2004, p. 22).

Nesse contexto, a segurança é uma condição indelével para o êxito do objetivo acima colocado, o que provoca uma perene busca pela proteção dos ativos informacionais. E há de ressaltar que a aquisição de conhecimento, oportunamente, pode ser um fator de vantagem competitiva no mercado atual.

As informações, do ponto de vista do negócio, configuram-se como ativos de uma empresa, juntamente, com todo o ambiente por onde trafegam e em decorrência devem ser protegidas, conforme visão de Caruso e Steffen (1999, p. 23).

Logo, cresce de importância no âmbito das redes de computadores a adoção de *firewall,* associado com um IDS.

Nesse aspecto, Marçula e Filho fornecem a seguinte conceituação:

> Um *Firewall* é uma combinação de *hardware* e *software* usados para implementar uma política de segurança comandando o tráfego da rede entre duas ou mas redes, algumas das quais podem estar sob seu controle administrativo (por exemplo, redes da sua empresa) e algumas das quais podem estar fora de seu controle (por exemplo, a *Internet*). Um *firewall* normalmente serve como uma primeira linha de defesa contra ameaças externas ao sistema de computadores, redes e informações críticas de sua empresa. *Firewalls* podem também ser utilizados para particionar as redes internas de sua empresa, reduzindo o risco de ataques internos (FITHEN *et al*., 1999 *apud* MARÇULA e FILHO, 2009).

O IDS "é um serviço que monitora e analisa eventos de uma rede com o propósito de encontrar e providenciar alertas em tempo real e acessos não autorizados aos recursos de uma rede" (SANTOS, 2010, p. 801).

Ratificando o exposto acima, Nakamura e Geus afirmam que:

> um sistema de detecção de intrusão trabalha como uma câmera ou um alarme contra as intrusões, podendo realizar a detecção com base em algum tipo de conhecimento, como assinaturas de ataques, ou em desvios de comportamento […]. Ao reconhecer os primeiros sinais de um ataque, e por meio de uma resposta coerente, os perigos de um ataque real podem ser minimizados. Além disso, quando um dispositivo do ambiente computacional falha, devido a um erro de configuração ou um erro do usuário, o IDS pode reconhecer os problemas e notificar o responsável (NAKAMURA e GEUS, 2004, p. 253).

Com vistas a elucidar os próximos tópicos do presente artigo, Murini cita que:

> devemos ter uma diferenciação entre "Ataque" e "Intrusão", pois parecem ser a mesma coisa, mas tem algumas particularidades: ataque refere-se à tentativa de perturbação, já intrusão é um ataque realizado que obteve sucesso (foi bem sucedido), pois invadiu a rede (MURINI, 2014, p. 20).

E a intrusão trata-se de um conjunto de ações realizadas por um intruso, visando comprometer os elementos: integridade, confidencialidade e

disponibilidade, que constituem a estrutura básica de segurança da informação de um sistema (SILVA e SAMPAIO, 2006, *apud* MURINI, 2014, p. 19-20).

Por fim, existem vários tipos de ferramentas de IDS para diferentes plataformas, mas o IDS opera basicamente da mesma forma, analisando os pacotes que viajam numa rede e comparando-os com as assinaturas de ataques, com vistas a alertar sobre vicissitudes indesejáveis.

2 DESENVOLVIMENTO

2.1 CARACTERÍSTICAS DE UM IDS

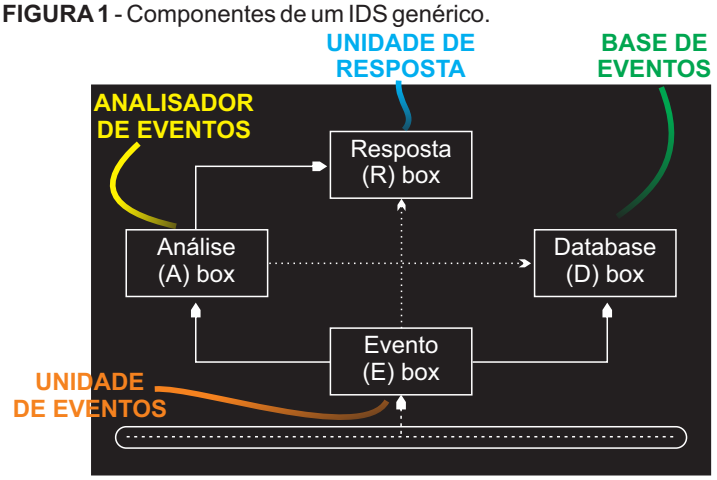
De acordo com Santos (2010, p. 801), um IDS deve possuir algumas características, como:

a) funcionar continuamente, operando normalmente em segundo plano;
b) ser tolerante a falhas;
c) ter a capacidade de monitorar a si próprio;
d) detectar mudanças no funcionamento normal da rede;
e) detectar o menor número de falsos positivos – que é a classificação de uma ação legal como uma possível invasão;
f) não deve permitir falso negativo – que ocorre quando uma intrusão real acontece, mas o sistema a classifica como legítima;
g) não deve permitir a subversão – que ocorre quando o intruso modifica a operação de ferramenta IDS para forçar a ocorrência de falso negativo;
h) deve avisar o administrador de rede ou de sistema, em tempo real, sobre uma possível invasão e, quando configurado, ativar automaticamente alarmes e mecanismos de segurança;
i) colher informações de intrusos para a sua captura; e
j) diagnosticar e corrigir eventuais falhas de segurança.

2.2 ARQUITETURA GENÉRICA DE UM IDS

Devido a ampla variedade de sistemas IDS, inicialmente foi proposto um modelo genérico denominado de *Common Intrusion Detection Framework* (CIDF), o qual reúne um conjunto de ferramentas que definem a configuração de um IDS, conforme figura a seguir:

FIGURA 1 - Componentes de um IDS genérico.



Fonte: Confeccionada pelo autor.

O objetivo do CIDF era promover a intercomunicação entre dispositivos de comunicação de intrusos e sistemas de respostas, como os *firewalls,* por intermédio de uma linguagem chamada de *Common Intrusion Specification Language* (CISL), na visão de Militelli (2006, p. 12).

Balizando-se pela figura 1, percebe-se que o modelo CIDF é composto pelos seguintes blocos: Unidade de Eventos (*E-box*), Analisador de Eventos (*A-box*), Unidade de Resposta (*R-box*) e Base de Eventos (*D-box*). Nesse contexto, Militelli (2006, p.12-13) afirma que estas unidades são responsáveis, respectivamente, pelas funções de:

a) gerar eventos e segurança que poderão se tornar alertas, a partir da informação proveniente de uma fonte de dados. Em se tratando de um meio físico, o *E-box* é o responsável por reconstruir o pacote de dados e repassar para análise;
b) realizar toda a análise e correlacionamento dos eventos, além da interação direta com o módulo e resposta;
c) promover as respostas no sistema IDS; e
d) armazenar o histórico de eventos conforme a ocorrência.

Posteriormente, em 1998 foi criado o *Intrusion Detection Exchange Format Working Group* (IDWG), grupo que se balizou nos conceitos contidos no CIDF e padronizou requisitos e novos protocolos de comunicação entre dispositivos envolvidos no sistema de detecção de intrusos, como o IAP e o IDXP.

E como aperfeiçoamento do IDXP, foi idealizado o *Secure Components Exchange Protocol* (SCXP), com o objetivo de promover um protocolo único de comunicação no escopo do IDS (YANG; CHANG; CHU, 2003 *apud* MILITELLI, 2006, p. 17).

2.3 CLASSIFICAÇÃO E TIPOS DE IDS

O IDS pode ser classificado em sistema de detecção por: assinatura (ou conhecimento) e por anomalias (ou comportamento). E segundo Nakamura e Geus (2004, p. 256) pode ser tipificado em três categorias: IDS baseado em máquina – *Host Based Intrusion Detection System* (HIDS), em rede – *Network Basead Intrusion Detection System* (NIDS) e híbrido – *Hybrid*. Vale ressaltar que este último aproveita as melhores características do HIDS e do NIDS.

2.4 SNORT

2.4.1 Características Técnicas

O Snort é um *software* livre desenvolvido por Martin Roesch, bastante popular por sua flexibilidade nas configurações de regras e constante atualização frente as novas ferramentas de invasão. Ele se baseia em assinaturas, ao monitorar tentativas de ataques contra uma rede e gera arquivos com as ocorrências diagnosticadas. Por isso, é classificado como um IDS baseado em rede.

Também é capaz de realizar análises em tempo real com suporte a diversos protocolos em nível de rede e aplicação, sobre o conteúdo hexadecimal e ASCII (GONÇALVES, 2015, p. 199). Pode ser usado para detectar uma variedade de ataques, como: *buffer overflows*, *stealth port scans*, ataques CGI, SMB *probes,* OS *fingerprinting*, dentre outros.

Essa ferramenta é compatível com arquiteturas RISC e CISC, e com distintas plataformas, como: distribuições *Linux* (*Red Hat, Debian, Slackware, Ubuntu*, etc.), sistemas operacionais (SO) da *Microsoft – Windows* e *Apple* – MAC OS.

O código fonte está calcado em linguagem de programação C e as documentações afetas ao seu emprego e funcionamento são de domínio público.

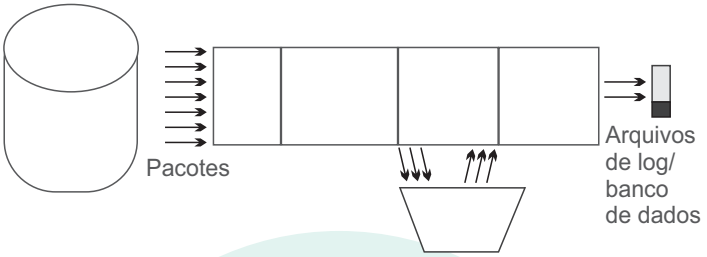
No Brasil, existe o projeto Snort-BR, um esforço para a criação de uma comunidade de usuários que podem usar um IDS de código aberto no país.

2.4.2 Arquitetura do Snort

Caswell e outros (2003) afirmam que a arquitetura do Snort é composta por quatro blocos, a saber:

a) o farejador de pacotes;
b) o pré-processador;
c) o mecanismo de detecção; e
d) o mecanismo de alerta/registro.

FIGURA 2 - Arquitetura do Snort



Fonte: Caswell et al., 2003, p.26.

2.4.2.1 Farejador de Pacotes

Os farejadores de pacotes são dispositivos de *hardware* ou de *software* utilizados na escuta das redes, capturando todos os dados trafegados.

Segundo Caswell *et al.* (2003), farejadores de pacotes podem ser utilizados para:

- análise de diagnóstico e solução de problemas na rede;
- análise e comparativo de desempenho; e
- intromissão para obter senhas em texto puro e outros dados interessantes.

A criptografia de tráfego da rede pode impedir que os dados sejam analisados por um farejador, o que se configura como uma desvantagem para o Snort.

2.4.2.2 Pré-Processador

De acordo com Caswell *et al*. (2003), este componente pega os pacotes brutos e verifica em relação a certos *plug-ins*, determinando assim o comportamento do pacote analisado. Uma vez detectado o comportamento particular do pacote, o mesmo é encaminhado para o mecanismo de detecção. A grande vantagem de trabalhar com *plug-ins*, é a possibilidade de ativar e desativar alguns deles de acordo com a necessidade e o perfil da rede onde o IDS está sendo configurado. Em suma, o pré-processador classifica os pacotes oriundos do farejador.

2.4.2.3 Mecanismo de Detecção

Na visão de Caswell *et al.* (2003), este é o bloco mais importante do IDS Snort. Os dados vindos do mecanismo de pré-processamento são recebidos pelo mecanismo de detecção e comparados com um conjunto de regras de assinatura de ataques conhecidos. Uma vez que os dados dos pacotes correspondam com as informações de alguma regra, estes são enviados para o processador de alerta.

Em se tratando do Snort, as regras são conjuntos de requisitos que geram um alerta. E para a criação de regras, é de vital importância ter conhecimento sobre os arquivos *snort.conf*, *threshold.conf* e *community.rules*,

que podem ser editados por intermédio de um editor de texto, como o *wordpad* (para o SO *Windows*).
O *download* das regras é feito do sítio eletrônico www.snort.org. Depois estas são descomprimidas e inseridas na pasta *rules* (*c:\snort\rules*), no caso do emprego do SO *Windows,* possibilitando que o mecanismo de detecção funcione de forma adequada.

2.4.2.4 Sistema de Alerta

Quando os dados que passam pelo mecanismo de detecção correspondem com alguma regra, então um alerta é disparado pelos *plug-ins* de saída. Sobre este evento, destaca-se a opinião de Caswell *et al.*(2003), ao afirmar que os *plug-ins* de saída fornecem aos administradores a capacidade de configurar *logs* e alertas de fácil compreensão. Ressalta-se que a análise de fluxo seria inútil sem eles para processar e formatar os dados analisados.

Os alertas podem ser enviados para um arquivo de *log* através de uma conexão de rede, por meio de soquetes UNIX ou *Windows Popup* e também podem ser armazenados num banco de dados. Existem muitas ferramentas adicionais que podem ser utilizadas para tratar os dados de saída do Snort como *plug-ins Perl* e PHP, além de servidores *Web* para exibir os dados processados.

2.4.3 Exemplificação da utilização do Snort

A representação do Serviço Federal de Processamento de Dados (SERPRO) em Recife tem adotado o Snort em suas redes internas, o que tem proporcionado uma economia da ordem de milhões de reais, caso fosse adquirida uma solução proprietária (BRASIL, [201-]).

3 CONCLUSÃO

O presente artigo busca dar uma visão panorâmica sobre o contexto de um Sistema de Detecção de Intrusão, abordando em particular o *software* Snort, um dos mais empregados no âmbito de sistemas cooperativos.

O emprego de um IDS, como o Snort, é de grande valia, tendo em vista que a solução já está consolidada no mercado de tecnologia da informação e possui atualizações constantes de regras, o que promove uma maior segurança numa rede de computadores.

Na visão de Gonçalves (2015, p. 199), seus módulos são capazes de analisar o conteúdo dos cabeçalhos tão quanto dos pacotes em redes *Internet Protocol* (IP), gerando elevada quantidade de informação sobre os ataques detectados. Ademais, uma das mais notórias características do seu funcionamento é a ampla possibilidade de tratamento dos alertas gerados, através de ações que vão desde mensagens ao administrador de rede a bloqueios de tráfego.

Outro detalhe que favorece a adoção do Snort é a característica do sistema ser baseado em assinaturas, trabalhando somente em comparação com seu banco de regras, ao contrário dos sistemas de detecção por anomalias.

Gonçalves (2015, p. 199) afirma que estes IDS possuem alguns inconvenientes, como: falsos positivos equivocadamente sinalizados como intrusão em relação a atividades anômalas, porém não intrusivas e falsos negativos, por não produzirem alguma anomalia perceptível, possibilitando que intrusões não sejam detectadas.

Assim, espera-se que o trabalho possa contribuir na difusão do emprego do Snort, visando elevar os níveis de segurança no universo das redes de computadores e *gadgets* que circundam o cotidiano da sociedade pós-moderna.

EL EMPLEO DEL SISTEMA DE DETECCIÓN DE INTRUSOS SNORT EN AMBIENTES COOPERATIVOS

RESUMEN

El presente trabajo científico consiste en abordar el “empleo del sistema de detección de intrusos en ambientes cooperativos”. La detección de intrusión es una de las áreas de mayor expansión, investigación e inversión en seguridad de redes de ordenadores. Con el crecimiento de la interconexión de ordenadores alrededor del mundo, por intermedio de internet, ocurrió un aumento en los tipos y números de ataques a los sistemas informáticos, produciendo una complejidad muy elevada para la capacidad de los tradicionales mecanismos de prevención. Para la mayoría de las aplicaciones actuales, a partir de redes corporativas simples hasta los sistemas de comercio electrónico o aplicaciones de banco, es prácticamente imposible el simple uso de mecanismos para reducir la probabilidad de ataques. Un ataque puede, en casos extremos, causar una interrupción total de los servicios, forzando la ocurrencia de un lento y costoso proceso de auditoría, y una restauración manual del sistema. Este contexto justifica toda la inversión realizada con el fin de crear dispositivos que superen la barrera de la simple prevención, asegurando a los sistemas una operación continua y correcta, mismo en la presencia de fallos de seguridad. Así, aparecen lo Sistema de Detección de Intrusos o Intrusion Detection System (IDS). Básicamente, el IDS es una herramienta inteligente (un sistema de configuración y reglas) capaz de detectar los intentos de intrusión en tiempo real y capaz de verificar si un usuario está usando la red correctamente, produciendo alertas cuando detecta paquetes que pueden ser parte de un posible ataque. En este contexto, se presenta el software Snort, ampliamente utilizado en

ambientes cooperativos, como una solución de aviso sobre la posibilidad de ataques y anomalías en redes de ordenadores.

Palabras-clave: snort, seguridad, detección de intrusos.

REFERÊNCIAS

BRASIL. **Snort**: ferramenta livre garante segurança na rede Serpro, [201-]. Disponível em: < http://www.softwarelivre.gov.br/noticias/snort-ferramenta-livre-garante-seguranca-na-rede-serpro/>. Acesso em: 06 jun. 2017.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações**. 2. ed. São Paulo: SENAC, 1999.

CARVALHO, João Antônio. **Informática para concursos**: teoria e questões. Rio de Janeiro: Elsevier, 2013.

CASWELL, Brian et al. **Snort 2**: sistema de detecção de intrusão. Rio de Janeiro: Alta Books, 2003.

GONCALVES, Denis Pohlmann. **Utilização de sistema de detecção e prevenção de intrusos modo NIDS**. In: ENCONTRO ANUAL DE TECNOLOGIA DA INFORMAÇÃO. 2015, Frederico Westphalen. Anais... Frederico Westphalen: IFF FARROUPILHA, ano 5, n. 1, nov. 2015. Disponível em: < http://eati.info/eati/2015/assets/anais/Longos/L24.pdf>. Acesso em: 06 jun. 2017.

KAHN, C.; PORRAS, P. A.; STANIFORD-CHEN, S.; B., A **Common Intrusion Detection Framework**. Journal of Computer Security, Julho, 1998.

LEMKE, Alexandre; SANTOS, Vagner. **Ferramenta Snort**. Disponível em: <http://olaria.ucpel.tche.br/rii/lib/exe/fetch.php?media=texto-trabalhosnortfinal.pdf>. Acesso em: 06 jun. 2017.

MARÇULA, Marcelo; FILHO, Pio Armando Benini Filho. **Informática**: conceitos e aplicações. 3. ed. São Paulo: Érica, 2009.

MILITELLI, Leonardo Cavallari. **Proposta de um agente de aplicação para detecção, prevenção e contenção de ataques em ambientes computacionais.** 2006. Dissertação (Mestrado em Engenharia Elétrica) – Escola Politécnica da Universidade de São Paulo, 2006. Disponível em: < http://www.lsi.usp.br/~volnys/academic/trabalhos-orientados/Agente-de-aplicacao-para-IDS.pdf>. Acesso em: 06 jun. 2017.

MURINI, Cléber Taschetto. **Análise dos sistemas de detecção de intrusão em redes: snort e suricata comparando com dados da DARPA.** 2014. Trabalho de Conclusão de Curso (Tecnólogo em Redes de Computadores) – Universidade Federal de Santa Maria, 2014. Disponível em: <http://www.redes.ufsm.br/docs/tccs/CleberMurini.pdf>. Acesso em: 06 jun. 2017.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. 2. ed. São Paulo: Futura, 2004.

SANTOS, André Alencar dos. **Informática descomplicada:** teoria e exercícios para concursos públicos. 5. ed. Brasília: Gran Cursos, 2010.

SILVA, Edelberto Franco; JULIO, Eduardo Pagani. **Sistema de detecção de intrusão** – artigo Revista Infra Magazine 1. Disponível em: <http://www.devmedia.com.br/sistema- de-deteccao-de-intrusao-artigo-revista-infra-magazine-1/20819>. Acesso em: 05 jun. 2017.

SNORT. Site of Snort Community. Disponível em: <https://www.snort.org/>. Acesso em: 05 jun. 2017.

_____. Snort Uses Manual 2.9.9. [S. l.]. 2016. Disponível em: < http://manual-snort-org.s3-website-us-east-1.amazonaws.com/>. Acesso em: 05 jun. 2017.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Capitão da Arma de Comunicações do Exército Brasileiro, possui especialização nas áreas de Manutenção de Comunicações e Guerra Eletrônica. Concluiu com aproveitamento o curso de Manutenção de Comunicações da Escola de Comunicações, o curso Básico de Guerra Eletrônica, no Centro de Instrução de Guerra Eletrônica (CIGE) e o curso Expedito de Guerra Eletrônica para Oficiais, no Centro de Adestramento Almirante Marques Leão da Marinha do Brasil. É pós-graduado em Guerra Eletrônica pelo CIGE e em Sistemas de Comunicações e Defesa, pela Universidade Politécnica de Madri. Atualmente, exerce a função de Instrutor na Escola de Comunicações e pode ser contactado pelo email adao.silva@eb.mil.br.

INTERNET OF THINGS - INTERNET DAS COISAS: SOLUÇÕES INOVADORAS PARA PROBLEMAS ANTIGOS.

RICARDO INACIO DONDONI
Pós-Graduado, lato sensu, em Operações Militares

RESUMO: Desde a primeira vez que o termo "Internet de Todas as Coisas" foi cunhado até o presente momento, seus braços tem unificado pesquisadores e cientistas. Estes enxergam possibilidades infinitas de aplicação para essa, que é a evolução mais significativa da rede mundial de computadores até o presente momento. No entanto, há um abismo entre a sociedade acadêmica/científica e o cidadão comum, de modo que é pertinente a pergunta: como atrair este cidadão ao universo da IoT? Nesse sentido, este artigo tem por finalidade exemplificar uma dentre inúmeras aplicações que podem servir de chamariz para atrair ao mundo que se abre diante da IoT. Para isso, foi empregado no presente artigo a metodologia da pesquisa acadêmica, quantitava e teórica, por meio de leitura de artigos, periódicos e revistas, objetivando informar os alcances da IoT, suas definições e possibilidades de aplicação. Com o tempo, a sociedade atual será transportada completamente para a realidade dos objetos conectados e a grande pergunta que deve-se fazer é: como se inserir neste universo? Passageiros ou condutores? Por fim, o presente estudo se encerra, ao conduzir o leitor às portas do conhecimento, rumo aos estudos introdutórios ao universo IoT.

Palavra-chave: IoT, dispositivos inteligentes, segurança, aplicações

1 INTRODUÇÃO

1.1 ORIGENS

Nos idos de 1999, ocorreram os primeiros estudos sobre a IoT, atingindo popularidade ao designar a integração de objetos que colaboravam digitalmente, provendo dados que pudessem ser processados para fins específicos (SANTOS *e Col.*, 2015). Nesse sentido, Santos e Sales (2016) prestam sua colaboração ao lembrar que a *Internet of Things*, ou Internet das Coisas, é cunhada pela primeira vez por Ashton (2009), haja vista a expressividade de suas pesquisas na área, no entanto, naquele momento ainda não havia uma definição que fosse amplamente aceita. Galegale explica que:

> para Singer (2012) a simples definição de Internet das Coisas enquanto rede mundial de objetos conectados, que trocam informação entre si é muito ampla. Segundo pesquisa da autora, o termo IoT parece bem aceito na Europa, enquanto nos Estados Unidos as pesquisas estão mais concentradas em torno de termos como objetos inteligentes ou computação em nuvem (GALEGALE e Col., 2016).

Dos dados iniciais resta que o grupo intitulado *Auto ID-Center* teve expressiva participação no surgimento da arquitetura IoT, pelo incentivo a pesquisa e desenvolvimento tecnológico (P&D), enquanto trabalhavam uma solução de identificação de radiofrequência em rede (RFID) juntamente com as tecnologias sensoras emergentes (EVANS, 2011).

Evans(2011) afirma que é notório o impacto causado pela *internet* na sociedade global em todas as áreas do conhecimento humano, das ciências, quer sejam exatas ou não, das relações sociais e comerciais. Sendo a IoT, a mais nova evolução da *internet,* quão mais notório será o impacto causado por ela?

1.2 CONCEITO E POSSIBILIDADES

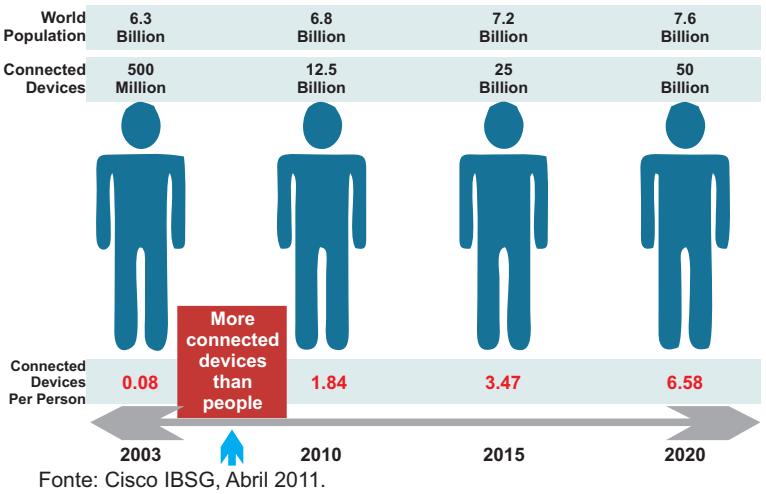
O termo IoT ganhou uma definição expressiva e amplamente aceita, cunhada pelo Cisco Business Solutions Group (IBSG) que define o termo como sendo o ponto no tempo no qual teremos mais objetos conectados do que pessoas (EVANS, 2011).

Em 2002, os pesquisadores já demonstravam expressiva preocupação com o avanço acelerado das pesquisas acerca da IoT, alertando que "tudo o que se veste ou se usa terá *microchips* que irão rastrear todo o comportamento do homem" (SCHOENBERGER, 2012, *apud* GALEGALE e *Col.*, 2016). Galegale comenta que:

> este cenário promove um ambiente interessante para incentivar o desenvolvimento de P&D com base em tecnologia radical ou incremental com a IoT, como também condiciona a necessidade de investimentos nas áreas de Engenharia Mecatrônica, Biotecnologia e Nanotecnologia, para produção de sensores miniaturizados de baixo consumo de energia dotados de endereço IP, pois a IoT não prescinde desses dispositivos para tornar-se onipresente e atender à crescente demanda (GALEGALE e *Col.*, 2016).

Em termos de inovação, a IoT interage em ambas vertentes, radical e incremental. A primeira diz respeito a apresentação e introdução de algo plenamente novo, sem precedentes, a segunda diz respeito as melhorias e aperfeiçoamentos que lhe são introduzidas, causando um processo de melhoramento constante (GONÇALVES, 2012).

FIGURA 1 - População mundial X Dispositivos conectados por pessoas



Fonte: Cisco IBSG, Abril 2011.

Os dados anteriores alarmam e evidenciam que a IoT, além de possibilitar a inovação incremental, obriga seus pesquisadores e desenvolvedores a pensarem em soluções radicais de conexão, de custo energético e de taxa de transmissão que integrem cinquenta bilhões de dispositivos sem perda das conectividades até agora alcançadas. Longe do temor que se espera, diante do desafio, o mundo globalizado está irremediavelmente focado na solução desse problema.

2 FAZENDO USO DO IoT NO DIA A DIA

Santos e colaboradores (2012) apontam que nem sempre a IoT traz algo, de fato, novo. Às vezes, resolve-se velhos problemas de forma mais prática, rápida e precisa, por fazer uso da capacidade de conectividade constante de compartilhamento de dados, do controle à distância, no qual estes dispositivos inteligentes interagem (PEOPLES, 2013, *apud* SANTOS e Col., 2012).

Nessa ótica, a IoT avulta sua importância, pois por intermédio de "dispositivos conectados e identificados, torna-se possível perceber eventos e alterações dentro do chamado ambiente inteligente" (CHABRIDON, *e Col.*, 2014 *apud* SANTOS, 2016). Nesse universo de conexões, Pang alerta que:

> o impacto social e organizacional que a IoT potencialmente provoca na utilização das TIC's pode reconfigurar a maneira como as pessoas lidam com as informações, como convivem, como recebem e fornecem serviços e como utilizam as tecnologias existentes (PANG e *Col.*, 2015 *apud* SANTOS, 2016).

Diante desse cenário disruptivo, a tecnologia empregada na IoT empreende esforços para superar as restrições, limitações e impedimentos das tecnologias vigentes, a fim de integrar à rede mundial de computadores, mais de cinquenta bilhões de objetos inteligentes até meados de 2020.

Mais e mais, os objetos do dia a dia estão sendo inseridos no ambiente IoT e, em pouco tempo, a tecnologia vigente nesta década será superada e substituída, dando lugar a essa nova realidade onde já se tem mais dispositivos do que pessoas conectadas à rede.

A solução IoT tem inúmeras aplicabilidades para cada um dos setores da sociedade. Quando se trata de IoT, as possibilidades são infinitas e limitam-se apenas ao imaginário do pensamento humano.

2.1 PROBLEMAS ANTIGOS

Ao longo do tempo, cada geração empreendeu esforços na solução dos problemas que afligiram seu cotidiano. Com o advento da *internet,* as soluções foram maximizadas de forma sem precedentes.

Tais soluções têm sido exponenciadas pela sinergia existente entre Ciência & Tecnologia, no exercício contínuo do domínio teórico e prático das artes, ciências e técnicas, resultando em inovações incrementais e radicais, apresentadas com celeridade difícil de acompanhar.

O grande resultado é que o avanço tecnológico está alcançando inúmeras áreas do conhecimento ao mesmo tempo, produzindo novas soluções para problemas antigos.

Por exemplo, a segurança física das instalações, em qualquer época, sempre foi um problema a ser dimensionado. Aliás, privacidade e segurança são bens desejáveis e de difícil manutenção.

Para gerir aquilo que é privativo, Wang e Kobsa (2008) identificam onze princípios fundamentais da privacidade, dos quais se destacam os quatro princípios abaixo elencados pelo relacionamento com o tema segurança de instalações (WANG e KOBSA, 2008, *apud* SANTOS e SALES, 2015).

QUADRO 1 - Princípios e descrições de privacidade elencados por WANG e KOBSA

a consciência de utilização	Baseado em declarações claras e bem detalhadas das políticas de privacidade.
a limitação de uso	Defini-se a fim de evitar que dados sejam usados ou divulgados para fins que não tenham sido especificados no momento da coleta.
a segurança	Garantia de que os dados estão fora de risco de perda, acesso não autorizado, uso indevido, modificação ou divulgação não autorizada
a aplicação	Preocupa-se diretamente com a existência de mecanismos que façam cumprir princípios de privacidade

Fonte: (WANG e KOBSA, 2008, *apud* SANTOS e SALES, 2015).

No século passado, tais princípios eram tidos como boas práticas relacionadas a provimento de segurança de instalações. Nos dias atuais, definir as políticas de privacidade, restrições de acesso ao ambiente e à informação, enquanto gerencia a execução dos procedimentos estabelecidos, são apenas a base rudimentar de qualquer esforço para o estabelecimento da segurança.

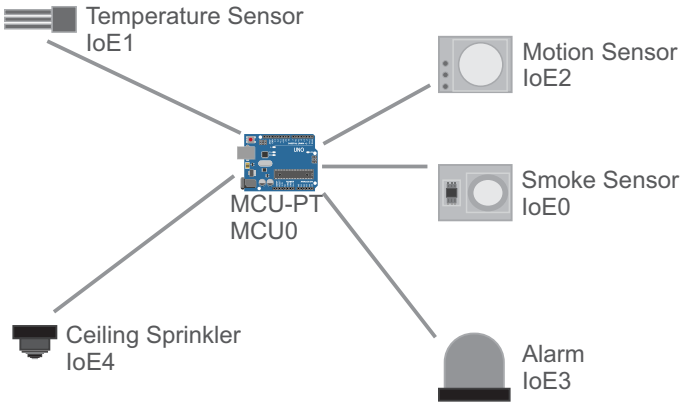
Nesse sentido, o ambiente estabelecido pela tecnologia IoT permite dar um passo além do usual, ao encontro daquilo que é dinâmico, preciso, flexível e eficaz.

2.2 SOLUÇÕES NA ÁREA DE SEGURANÇA

Os objetos inteligentes que integram o sistema IoT perfazem acréscimo ao nível de segurança já implantado. Ele não substitui os sistemas, protocolos e rotinas, mas amplifica suas potencialidades automatizando processos e tornando mais rápida a resposta aos eventos de segurança.

Uma das grandes marcas da tecnologia IoT é a capacidade de integrar sensores, atuadores e controladores, por meio de pequenas rotinas programáveis, que interagem com os equipamentos em resposta a sensores ativos ou, ainda, a intervenção pontual do gerente do sistema.

FIGURA 2 - Controlador e sensores conectados



Fonte: (Packet Tracer 7.0, adaptado pelo autor, 2017).

Imaginemos uma sala que, pela natureza do material que nela exista, necessite de um controle diferenciado, como por exemplo, uma reserva de material ou armaria. Além de uma fiscalização física de ambiente, feita por intermédio de ronda em período não padronizados, uma solução IoT poderia adicionar mais uma linha de segurança ao sistema vigente.

Por exemplo, uma placa de arduíno trabalhando em conjunto com um *Raspberry Pi* poderia agrupar sensores analógicos e digitais, aliados a atuadores controlados remotamente.

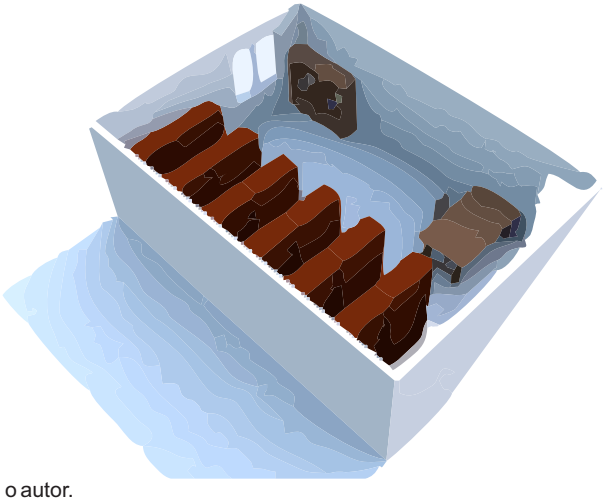
Em termos de sensores, poderiam ser utilizados para implementar a segurança, sensores de temperatura, de pressão, de umidade, de fumaça, de movimento, de alarme, entre outros.

Em termos de atuadores, são aplicáveis em tal ambiente, ventiladores, câmeras de visão noturna, trancas automáticas, sistema contraincêndio, *plug* 4G para conexão *internet,* entre outros passíveis de uso.

Uma vez instalada a solução IoT, que atenda as necessidades dimensionadas, pode-se, numa situação de arrombamento, ter o sensor de pressão identificado que a porta foi forçada, acarretando o envio de mensagem ao controlador, que por sua vez acionará a câmera que fotografará o ocorrido. O controlador, por intermédio do chip 4G, enviará a imagem para o celular funcional dos elementos de serviço que, de posse da informação, terão a oportunidade de analisar e processar o evento registrado, dimensionando a resposta de maneira eficaz. Além disso, o controlador poderia acionar o alarme, enviar mensagem pre-estabelecida para o comandante da unidade entre outras funcionalidades passíveis de implementação.

No caso de incêndio, uma gama de sensores e atuadores poderia ser programada para dar uma pronta resposta. Por exemplo: o sensor de fumaça

FIGURA 3 - Cômodo mobiliado



Fonte: o autor.

sensibilizaria o controlador indicando que o nível de fumaça no ambiente está prejudicial à saúde e como pronta resposta do sistema, as janelas conectadas ao dispositivo IoT seriam abertas e o ventilador acionado. Caso os sensores de temperatura acusassem o aumento exponencial da temperatura no ambiente, o sistema de incêndio poderia ser acionado. No caso do sensor de movimento indicar a presença de pessoas no recinto, o corpo de bombeiro poderia ser acionado remotamente por intermédio da programação realizada na placa, a fim de prestar os primeiros socorros àqueles que inalaram grandes quantidades de monóxido de carbono. O sistema pode ser programado para que uma vez restabelecidos os níveis de temperatura e fumaça, as seguranças sejam restabelecidas e os sistemas inicialmente desativados sejam, por sua vez, reativados. Outras rotinas poderiam ser amplamente empregadas.

Imagine as possibilidades de programação de pronta resposta para inúmeras ações que a componente humana deveria tomar uma a uma, sendo processadas automaticamente, por intermédio de rotinas pré-estabelecidas, todas efetuadas de uma só vez. A automatização dos processos, libera a componente

humana para focar sua atenção em inúmeras outras ações prioritárias até então depreciadas em favor da urgência das primeiras.

3 CONCLUSÃO

A automatização dos processos pelo IoT é viável, eficaz e capaz de fornecer redundância de segurança aos sistemas críticos da Organização Militar (OM).

Como ainda estamos no alvorecer dos fatos, em termos de tecnologia e conhecimento, faz-se necessário que cada Organização empreenda esforços em formar quadros capazes de atuar com IoT, o que reverterá em grandes benefícios para a OM, bem como, para o próprio militar, que estará na vanguarda do conhecimento tecnológico mundial.

Afinal, estamos vivenciando a nova onda evolucionária da *internet,* com aplicação dual, emprego civil e militar. Tecnologia, essa, de ampla ligação com a rede 5G, que possui preocupações reais quanto à integração desses dispositivos inteligentes na rede de dados mundial.

Pensando em todo esse certame, a *Net Academy Cisco* implantou em suas academias os cursos IoT Fundamentos: Conectando Coisas e IoT Fundamentos: *Big Data* com vistas a preparar seus discentes para o universo que se abre a esta nova geração.

Afinal de contas, de tudo que se pode falar sobre IoT, pode-se concluir que: A IoT não é algo efêmero e quem não estiver preparado para exercer domínio sobre essa nova tecnologia será conduzido por aqueles que se capacitarem ao exercício dela.

Dito isso, ressalta-se que a Escola de Comunicações é uma Academia Cisco reconhecida internacionalmente e possui instrutores habilitados a ministrarem os cursos IoT da Cisco.

A implantação de soluções inovadoras para problemas antigos é realidade palpável e passível de materialização por meio da IoT. Basta, no entanto, romper as amarras da solução tradicional, empreendendo criatividade, esforço e dedicação. Uma vez vencida a inércia e lançado rumo ao horizonte de possibilidades, quem lhe imporá os limites?

INTERNET OF THINGS: CONVERTING OLD PROBLEMS IN NEW SOLUTIONS.

ABSTRACT

From the first time the term "Internet of All Things" has been coined to date, its arms have unified researchers and scientists. All researchers see endless possibilities of application for what is the most significant evolution of the world's However, there is an abyss between academic / scientific society and contemporary society, so the question is: How to attract the citizen to the IoT universe? In this sense, this article aims to exemplify one of many applications That can serve as a decoy to attract us to the world that opens before the IoT.For this, the Methodology of Academic, Qualitative and Theory Research was used in this article, through reading Articles, Periodicals and Magazines, aiming to inform the scopes IoT, its definitions, possibilities of application. Over time, the current society will be transported completely The reality of the connected objects and the great question that we must ask is how we want to be inserted in this universe? Passengers or drivers? Finally, the present study ends, by leading the reader to the doors of knowledge, towards the introductory studies of the IoT universe.

Keywords: IoT, Devices, Smart, Security.

REFERÊNCIAS

ALVES, Maria Bernardete Martins; ARRUDA, Suzana Margret de. **Como elaborar um Artigo Científico**. Disponível em: <http://www.bu.ufsc.br/design/ ArtigoCientifico.pdf>. Acesso em: 18 maio 2017.

EVANS, Dave. The Internet of Things. **How the Next Evolution of the Internet is Changing Everything**. Cisco Internet Business Solutions Group (IBSG). April, 2011. Disponível em: <http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> Acesso em: 18 maio 2017.

GALEGALE, Gustavo Perri e Col. **Internet das Coisas aplicada a negócios** - Um estudo bibliométrico. Revista de Gestão da Tecnologia e Sistemas de Informação. v. 13, nº 3, Set/Dez., 2016, pp. 423-438. Disponível em: <http://www.jistem.fea.usp.br/index.php/jistem/article/viewFile/10.4301%25S1807-17752016000300004/616>. Acesso em: 18 maio 2017.

GONÇALVES, Adriana Aguillera. **A proteção do conhecimento e a inovação na Universidade Estadual de Londrina.** 2012. Dissertação (Mestrado em Gestão da Informação) - Universidade Estadual de Londrina, Londrina. Disponível em: <http://repositorio.utfpr.edu.br/jspui/handle/1/337>. Acesso em: 18 maio 2017.

KRANENBURG, Rob Van; BASSI, Alex. **IoT Challenges**. Communications in Mobile Computing 2012. Disponível em: <https://muxjournal.springeropen.com/articles/10.1186/2192-1121-1-9>. Acesso em: 18 maio 2017.

SANTOS, Carlos Cesar; SALES, Jefferson David de Araújo. **O desafio da privacidade na Internet das Coisas.** Revista Gestão.Org, v. 13, Edição Especial, 2015. pp. 282-290. Disponível em: < http://www.revista.ufpe.br/gestaoorg/index.php/gestao/article/download/780/484> . Acesso em: 18 maio 2017.

SANTOS, G. A. e Col. Internet of Things (IoT): **Um cenário Guiado por Patentes Industriais.** Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 271-281. Disponível em: <http://www.revista.ufpe.br/gestaoorg/index.php/gestao/article/download/800/483 >. Acesso em: 18 maio 2017.

WRIGHT, Alex. **Mapping the Internet of Things:** Researchers are discovering surprising new risks across the fast-growing IoT. Communications of the ACM. v. 60. nº 1. 2017. pp. 16-18. Disponível em: <https://cacm.acm.org/magazines/2017/1/211101-mapping-the-internet-of-things/fulltext>. Acesso em: 18 maio 2017.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (2002) e pós-graduado pela Escola de Aperfeiçoamento de Oficiais (2010). É instrutor na plataforma *Net Academy Cisco* habilitado a tutoria do *IT Essencial*, CCNA1, *IoE, IoT Fundamentals: Conecting Things, Introduction to Cybersecurity.* Atualmente, é Instrutor na Escola de Comunicações e pode ser contactado pelo email dondoni.ricardo@eb.mil.br

UTILIZANDO GOOGLE HACKING PARA ENCONTRAR VULNERABILIDADES EM SITES

BRUNO RODRIGO BARBOSA CORTES

Pós-Graduado, lato sensu, em Guerra Cibernética e Análise e Desenvolvimento de Sistemas aplicados a Gestão Empresarial

RESUMO: Este artigo apresenta uma análise de como a configuração indevida de um servidor pode expor informações sensíveis de uma empresa na base de dados do *Google* e demonstra as técnicas utilizadas pelos *hackers* para explorar estas falhas, *Google Hacking.* Estar bem classificado nas pesquisas do *Google* é um dos principais objetivos de uma empresa que busca visibilidade na *internet,* entretanto, o mecanismo de indexação do *Google* poderá registrar informações sensíveis de sua empresa e abrir uma porta para a ação de *hackers* maliciosos. O trabalho realiza a exposição do método utilizado por *hackers* para obtenção de informações sensíveis e a descoberta de possíveis alvos que utilizam softwares vulneráveis.

Palavras-Chave: *google hacking,* segurança da informação, ataques cibernéticos.

1 INTRODUÇÃO

Com o advento da *internet* e sua constante expansão, tornou-se fundamental a presença das empresas na rede mundial de computadores, seja para expor trabalhos, atrair clientes, fornecer serviços e atividades de comércio *online* (*e-commerce*), quanto para outras muitas finalidades que tornam as empresas cada vez mais dependentes das facilidades providas pela conectividade da *internet.*

Entretanto, publicar um *site* ou serviço *web* não é o suficiente para atrair visitantes, é necessário ter visibilidade, ou seja, ser visto por seu público-alvo. Diante desta demanda, surgiram os *sites* para busca de conteúdo *web,* que tem por objetivo retornar o conteúdo relacionado a demanda de um usuário.

Dentre este universo, o *Google* é, atualmente, o buscador mais usado, estando à frente de outros concorrentes como *Ask, Yahoo* e *Bing.* O buscador *Google* se destaca dos demais por sua eficiente atualização e classificação de informações. Sua base de informações é diariamente atualizada por meio de seu *crawler,* o *Googlebot,* um "robô" que varre a rede mundial de computadores em busca de informações novas.

Entretanto, as facilidades providas pelos buscadores de conteúdo *web* também são o pivô para uma série de ataques cibernéticos, pois, assim como são eficientes ferramentas para pesquisa de conteúdo, possibilitam a *hackers* maliciosos encontrar vulnerabilidades conhecidas e realizar ataques a diversos alvos pela rede.

Neste artigo, será exposto como os criminosos utilizam o *Google* para obter acesso a informações sensíveis e encontrar alvos para vulnerabilidades conhecidas, bem como, será apresentado alternativas para proteção desta exposição indevida.

2 MATERIAL E MÉTODOS

Conforme Paiva (2015), a pesquisa no *Google* não se fundamenta especificamente na busca por informações sensíveis como usuários e senhas, mas se fundamenta no que é procurado, buscando usar essas informações para seus próprios objetivos.

Encontrar informações sensíveis faz parte da rotina de um *Google Hacker*, que pode utilizar o *Google* na busca de servidores negligenciados, diretórios expostos, relatórios de segurança expostos e na busca de informações pessoais e documentos compartilhados por engano na *Internet* como: planilhas, tabelas, vídeos, documentos do *Word,* fotos, bancos de dados e outros arquivos que possuam alguma informação relevante.

Segundo Long (2004), o *Google* permite o uso de certos operadores para ajudar a refinar as pesquisas. A utilização de técnicas avançadas com operadores é muito simples, desde que seja dada atenção à sintaxe.

Com o emprego de algumas técnicas, é possível otimizar as pesquisas feitas no *Google.* Os operadores de busca nada mais são que convenções definidas pelo próprio buscador para auxiliar quem procura por resultados avançados. A pesquisa é feita na tradicional caixa de busca do *Google,* porém, com alguns códigos adicionais inseridos antes dos termos utilizados. Um dos recursos mais poderosos do *Google,* e ao mesmo tempo desconhecidos pela maioria dos usuários, são os ditos "operadores avançados". Na confecção deste artigo foram levantados os principais operadores avançados nas obras de Johhny *Long The Google Hacker's Guide. Understanding and Defending Against the Google Hacker*, de 2004, e *Google Hacking for Penetration Testers. Google Hacking:* Teste de Invasão, de 2007. Os principais exemplos de operadores, neste contexto, são:

a. Subtrair resultado

Deve-se adicionar um traço (-) antes de uma palavra ou um site para excluir todos os resultados que incluem essa palavra. Isso é útil especialmente para diferenciar palavras com vários significados.

Exemplo: Eleições –governador, Gol –carro

b. Pesquisa exata

Usam-se aspas para pesquisar uma palavra exata ou um conjunto de palavras em uma página da *web.* Termos entre aspas filtram a busca somente para resultados exatos, ou seja, exatamente como o pesquisador está procurando. Deve ser usado somente se estiver procurando uma palavra ou frase exata. Caso contrário, a busca excluirá muitos resultados úteis por engano.

Exemplo: “Luiz Fernando da Costa” 34

c. Curingas

Usa-se um asterisco em uma pesquisa como um marcador para termos desconhecidos ou caracteres coringa. Aspas podem ser usadas para encontrar variações da frase exata ou para lembrar palavras no meio de uma frase.

Exemplo: “Forças * revolucionárias da *"

d. Busca alternativa

Usa-se *“OR”* quando se deseja pesquisar páginas que contenham apenas uma entre várias palavras, deve-se incluir *“OR”* (em maiúsculas) entre as palavras. Sem o *“OR”,* os resultados normalmente mostram somente páginas correspondentes a ambos os termos.

Exemplo: Brasil OR *Brazil*

e. Restringindo pesquisa a *site* específico

Se o pesquisador incluir o operador *“site”* em sua consulta, o *Google* irá restringir os resultados da pesquisa do *site* ou domínio que o pesquisador especificar. Por exemplo, é possível encontrar todas as referências a "terrorismo" no *website* da *BBC.*

Exemplos: terrorismo *site:bbc.co.uk/portuguese*

f. Buscando por cache

Caso o pesquisador utilize o operador *“cache”,* será exibida a versão de uma página *web* em cache do *Google* correspondente ao termo buscado. Este operador permite visualizar como estava a página na última vez que o *Google* rastreou o *site.*

Exemplo: cache:www.mpl.org.br

g. Buscando por tipo de arquivo

Caso o pesquisador utilize o operador *“filetype”* este se trata de um recurso empregado para selecionar o tipo de arquivo que se deseja em uma pesquisa. Busca apenas em arquivos de um tipo específico. Este operador instrui o *Google* para pesquisar apenas dentro do texto de um determinado tipo de arquivo. Este operador requer um argumento adicional da busca.

Exemplo: *download* Constituição Federal *filetype*:pdf

h. Buscando termos no texto de um documento

Caso o pesquisador utilize o operador *“intext”* os resultados serão restritos a documentos que contenham o termo no texto. O comando abaixo retornará documentos que mencionam a palavra "terremoto" no texto, e mencione os nomes "Missão”, “Paz” e “Haiti" em qualquer parte do documento (texto ou não).

Exemplo: Missão de Paz Haiti *intext:*terremoto

i. Buscando termos simultâneos em um texto

Caso o pesquisador utilize o operador *“allintext”* o *Google* restringirá os resultados para aqueles que contenham todos os termos da consulta que o pesquisador especificar no texto da página. O comando abaixo retornará somente as páginas em que as palavras "Exército", "fronteira" e "operação" aparecem no texto da página.

Exemplo: *allintext*:Exército fronteira operação

j. Buscando termo em um título de documento

Caso o pesquisador utilize o operador *“intitle”* restringirá os resultados a documentos que contenham o termo no título. Este comando faz com que o sistema de buscas foque somente no título das páginas dos *sites* indexados para encontrar os resultados relevantes para o pesquisador. O comando abaixo retornará documentos que mencionam a palavra "amazônia brasileira" em seus títulos, e mencione as palavras “garimpo” e “ilegal” em qualquer parte do documento.

Exemplo: garimpo ilegal intitle:amazônia brasileira

k. Buscando termos simultâneos em um título de um documento

Caso o pesquisador utilize o operador *“allintitle”* o *Google* restringirá os resultados para aqueles que contenham todos os termos da consulta que o pesquisador especificar no título. O comando abaixo retorna somente documentos que contenham as palavras "FARC" e "terrorismo" no título. Isso é equivalente a uma série de pesquisas *'intitle'* individuais.

Exemplo: *allintitle:*FARC terrorismo

l. Buscando termo em uma URL

Caso o pesquisador utilize o operador *“inurl”* em sua consulta, o *Google* irá restringir os resultados a documentos que contenham essa palavra na URL. Este operador instrui o *Google* a pesquisar somente dentro da URL ou endereço *web* de um documento.

Exemplo: *inurl:admin* senha

m. Buscando termos simultâneos em uma URL

Caso o pesquisador utilize o operador *“allinurl”* o *Google* restringirá os resultados para aqueles que

contenham todos os termos da consulta que o pesquisador especificar na URL. O comando abaixo mostrará somente documentos que contenham as palavras *"black"* e *"bloc"* na URL.
Exemplo: *allinurl:black bloc*

n. Buscando termo uma localidade especifica

Caso o pesquisador utilize o operador *"location"* em sua consulta no *Google,* apenas artigos do local que o pesquisador especificar serão devolvidos. O comando abaixo mostrará artigos que correspondam ao termo "eleições" de *sites* no Brasil.

Exemplo: eleições *location*:brasil

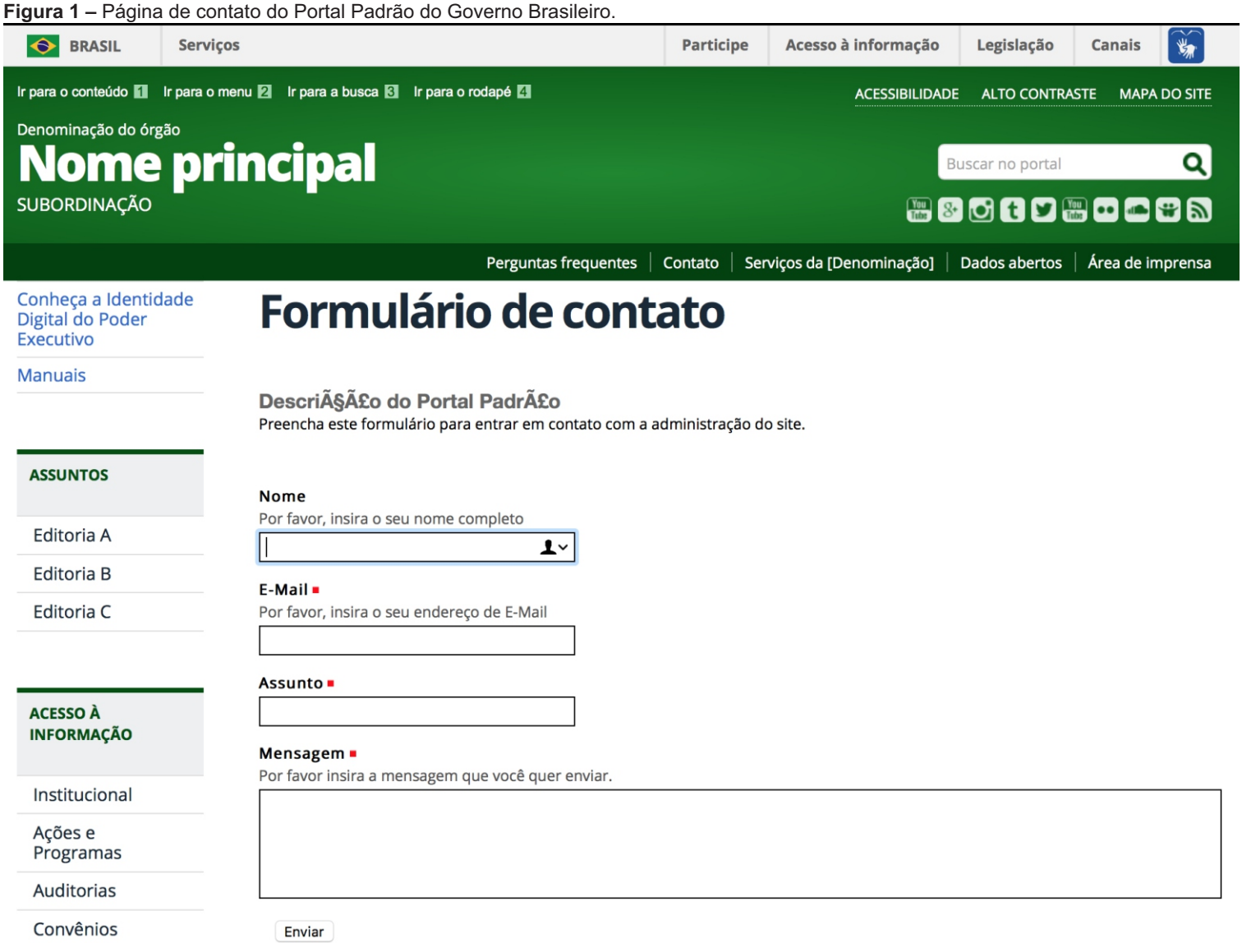
3 RESULTADOS E DISCUSSÃO

A fim de demonstração da técnica utilizada por *Hackers* na identificação de sistemas vulneráveis utilizando os serviços de busca do *Google,* considerei a situação hipotética de que um *hacker* encontrou uma vulnerabilidade no Portal Padrão adotado pelo Governo Brasileiro e deseja utilizar o *Google* para encontrar outros sites que adotam este sistema e possuem a vulnerabilidade encontrada.

A vulnerabilidade fictícia seria a possibilidade de SQL *Injection* (quando o atacante consegue inserir uma série de instruções SQL dentro de uma consulta através da manipulação das entradas de dados de uma aplicação) na página de contatos do Portal Padrão, disponível em: www.portalpadrao.gov.br/contact-info, conforme a figura 1:

Uma vez encontrada a vulnerabilidade, o *hacker* deverá construir uma *Dork,* combinação de termos e operadores avançados de pesquisas que retornará os *sites* vulneráveis a falha pesquisada. Neste exemplo, o *hacker* buscará por características da página que servirão como parâmetros de pesquisa para os operadores do *Google* a fim de filtrar os resultados encontrados para os *sites* que adotam o Portal Padrão

Figura 1 – Página de contato do Portal Padrão do Governo Brasileiro.



Fonte: o autor.

FIGURA 2 – Exemplo de pesquisa que retornaria páginas, hipoteticamente, vulneráveis.

Fonte: o autor.

do Governo Brasileiro e possuem a página de contato vulnerável.

Todas as páginas do Portal Padrão possuem, por padrão, o seguinte texto no rodapé "Desenvolvido com o CMS de código aberto *Plone"* o que possibilita a utilização do operador *intext* para procurar as páginas que possuem o trecho pesquisado. Entretanto, apenas este critério não será suficiente para encontrar as páginas vulneráveis, uma vez que outros *sites,* que não utilizam o Portal Padrão, também foram retornados na pesquisa.

Para direcionar a pesquisa aos resultados desejados, será adotado um segundo critério: a inclusão do operador *inurl* que irá filtrar os resultados para as páginas que, além do primeiro critério, possuem "*/contact-info*" em sua url. Desta maneira, o *Dork* utilizado para retornar o conteúdo desejado seria: *intext:*"Desenvolvido com o CMS de código aberto *Plone" inurl:/contact-info*.

Na Figura 2 podemos observar o retorno obtido com a utilização do *Dork* construído e exemplos de *sites* que estariam vulneráveis a falha encontrada.

Na *internet* estão disponíveis *sites* como o *Google Hacking Database (https://www.exploit-db.com/google-hacking-database/*) que possuem um banco de dados de *Dorks* pré-definidas para encontrar sistemas com vulnerabilidades conhecidas.

Desta maneira, pode-se observar como a ferramenta de pesquisa do *Google* torna-se um eficiente aliado aos *hackers* e criminosos cibernéticos. Para se proteger destas ameaças, torna-se necessário proteger a indexação de conteúdo pelos *Googlerobots,* o que

pode ser feito com a correta configuração do arquivo *robots.txt* na raiz da aplicação, documento que orienta o que deve e o que não deve ser indexado pelos *sites* de busca em seu sistema.

Além disto, deve-se buscar disfarçar características das tecnologias utilizadas, a fim de evitar a fácil identificação em buscas realizadas, por exemplo, no caso acima, os *sites* que utilizam o Portal Padrão e alteraram o texto exibido no rodapé não são exibidos nos resultados de pesquisa, entretanto, estariam igualmente vulneráveis.

4 CONSIDERAÇÕES FINAIS

Segurança da informação deve ser uma preocupação constante nos dias atuais, visto que, estão, cada vez mais constantes, ataques cibernéticos como, por exemplo, ataques de sequestro de dados, onde criminosos criptografam dados do usuário e solicitam um pagamento para liberação da senha de acesso, o que pode resultar em sérios prejuízos a uma empresa ou pessoa física.

Neste artigo, pode-se constatar a técnica utilizada por *hackers* para combinar buscadores de conteúdo *web,* como o *Google,* para identificação de sistemas vulneráveis e mal configurados.

Conclui-se que é importante manter atualizadas as tecnologias utilizadas nos sistemas, bem como, as configurações adequadas para se evitar a exposição de conteúdos indevidos na rede mundial de computadores.

USING GOOGLE HACKING TO FIND VULNERABILITIES ON SITES

ABSTRACT

This article presents an analysis of how improper configuration of a server can expose sensitive information of a company in the Google database and demonstrates the techniques used by hackers to exploit these flaws, Google Hacking. Being ranked well in Google searches is one of the top goals of a company that seeks visibility on the Internet, however, Google's indexing engine can record sensitive information from your company and open a door to malicious hacking. The work exposes the method used by hackers to obtain sensitive information and the discovery of possible targets that use vulnerable software.

Keywords: google hacking, information security, cyber security.

REFERÊNCIAS

DHANJANI, Nitesh; RIOS, Billy e HARDIN, Brett. Hacking: **A Próxima Geração**. Editora: Alta Books. Rio de Janeiro, 2011.

LONG, Johnny. 2007. **Google Hacking for Penetration Testers**. Google Hacking: Teste de Invasão. Rockland, Massachusetts, EUA: Syngress.

PAIVA, Newton. **Google Hacking**. Disponível em <http://blog.newtonpaiva.br/pos/wp-content/uploads/2013/04/PDF-E6-SI491.pdf>. Acesso em: 22 Set. 2015.

TOFFLER, Alvin. **The Third Wave** (A Terceira Onda): tradutor João Tavora, 4a Edição, Rio de Janeiro, RJ, Record, 1980.

TOFFLER, Alvin e TOFFLER, Heidi. **Guerra e antiguerra**: sobrevivência na aurora do terceiro milênio. Vol. 302. Tradução de Luiz Carlos do Nascimento Silva. Rio de Janeiro, RJ, Biblioteca do Exército, 1995.

O autor é Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Capitão da Arma de Infantaria do Exército Brasileiro. Pós-graduado em análise e desenvolvimento de sistemas pelo Instituto Federal do Triângulo Mineiro e em guerra cibernética pelo Centro de Instrução de Guerra Eletrônica (CIGE). Certificações que possui: GPEN e GCIH. Atualmente, exerce a função de Instrutor na Escola de Comunicações e pode ser contactado pelo email cortes.bruno@eb.mil.br.

A EVOLUÇÃO DO EMPREGO DA TECNOLOGIA CELULAR NO EXÉRCITO BRASILEIRO, SUAS VANTAGENS E LIMITAÇÕES

WASHINGTON RODRIGUES DA SILVA
Pós-graduado, lato sensu, em Operações Militares

RESUMO: O uso da tecnologia celular por militares do Exército Brasileiro vem aumentando nesta década. Especialmente com a criação dos *smartphones,* a empregabilidade deixou de restringir-se à voz e ganhou novas possibilidades, como meio de comunicação social ou mesmo de envios de mensagens de texto, voz, fotos e vídeos com aplicativos como o *WhatsApp Messenger,* aplicativo do Exército Brasileiro e *EBChat*. Entretanto, o uso dessa tecnologia ainda é limitada pela necessidade de infraestrutura de antenas para proporcionar a cobertura de sinal, o que torna mais eficaz o uso em zonas urbanas em razão da maior cobertura disponível.

Palavras-chave: tecnologia, *smartphones,* empregabilidade.

1 INTRODUÇÃO

Estudos de Silva (2006) propunham o uso de aparelhos de telefonia celular para transmissão de dados em operações urbanas de GLO em substituição aos, até então utilizados, rádios da faixa de frequência HF e VHF. Tal estudo proporciona a inferência de que nesse período não era incomum o uso de rádios em operações desse tipo.

O ambiente urbano apresenta a característica de ser economicamente favorável às empresas de telefonia móvel quando comparados ao rural. As razões são várias, das quais pode-se citar a maior facilidade de infraestrutura para instalação de Estações Rádio Base (ERB) como meios, logística, fontes de energia e o principal, sob a óptica dessas empresas, a elevada quantidade de clientes potenciais, o que permite a viabilidade do negócio de oferta de serviços de telefonia. Logo, não é difícil concluir que a disponibilidade de serviços de telefonia celular apresenta-se mais abundante nos ambientes urbanos, especialmente nas grandes cidades.

Os aparelhos de telefone celular deixaram de ser simples equipamentos de comunicação por voz ou mesmo de envio de mensagens de texto. Atualmente, os tradicionais telefones celulares estão cada vez mais em processo de substituição pelos chamados *smartphones.*

Barros (2012) define o *smartphone* como um híbrido de telefone celular com microcomputador, onde estão disponíveis tecnologias de comunicação como *internet, Global Positioning System* (GPS), correio eletrônico, *Short Message Service* (SMS), mensageiro instantâneo e aplicativos para variados fins, em um único equipamento.

Segundo Lopes e Vas (2016, p. 2), o aplicativo criado em 2009 por Brian Acton e Jan Koum com a finalidade de enviar mensagens instantâneas, o qual denominaram *WhatsApp Messenger,* caiu rapidamente no gosto dos usuários em geral. Tal ferramenta atraiu a atenção de grandes *players* do mercado da comunicação eletrônica, tanto que o *Facebook* a comprou por aproximadamente vinte e um bilhões de dólares em fevereiro de 2014.

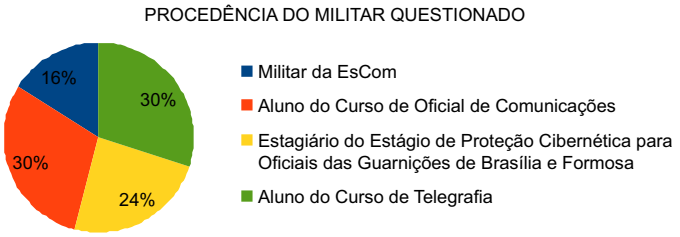
2 METODOLOGIA

O presente estudo utilizou pesquisa bibliográfica e questionários para obtenção de base de dados.

A amostra da pesquisa foi composta por cinquenta militares (oficiais intermediários ou subalternos, subtenentes e sargentos).

Os militares fazem parte de quatro perfis: militares da EsCom (capitães, tenentes, subtenentes e sargentos de carreira membros do corpo permanente da Escola de Comunicações do Exército Brasileiro); alunos do Curso de Oficial de Comunicações (tenentes de carreira das diversas Armas, Quadro e Serviço de Intendência) das cinco regiões do Brasil; participantes do Estágio de Proteção Cibernética para Oficiais da Guarnição de Brasília e Formosa (capitães e tenentes de carreira e temporários) e alunos do Curso de Telegrafia (sargentos de Comunicações de carreira), conforme o gráfico 1:

GRÁFICO 1 – Procedência dos militares que responderam o questionário



Fonte: o autor.

Os militares que compuseram a base de dados atualmente servem: 68% em unidades operacionais e 32% em unidades não-operacionais.

3 USOS ATUALMENTE NO EXÉRCITO BRASILEIRO

Os *smartphones* são utilizados de formas variadas

no âmbito do Exército Brasileiro (EB).

Com as possibilidades geradas pelos *smartphones,* vários outros usos tornaram-se possíveis. O EB criou aplicações voltadas para difusão de informações de comunicação social como o Aplicativo do Exército Brasileiro, disponível para plataformas *Android, Windows Phone* e iOS. Tal aplicação funciona como um canal de divulgação de variados meios de comunicação do Exército, como conteúdos da Revista Verde Oliva, Noticiário do Exército, Informex, entre outros. A figura 1 apresenta a página do Exército para *download* do aplicativo em pauta.

FIGURA 1 – Página para *download* do aplicativo do Exército Brasileiro

Fonte: Brasil, 2017.

Outro uso para os *smartphone* é para o emprego operacional. Segundo Brasil (2016), o *software* Pacificador possibilitou o acompanhamento em tempo real das operações no Jogos Olímpicos do Rio de Janeiro, em 2016, por meio do rastreamento do posicionamento dos *smartphones* com a versão móvel. A figura 2 mostra a visualização de diversas unidades móveis no terreno (inclusive de *smartphones* com a versão móvel do Pacificador), servindo como uma ferramenta adicional aos decisores para a obtenção de consciência situacional.

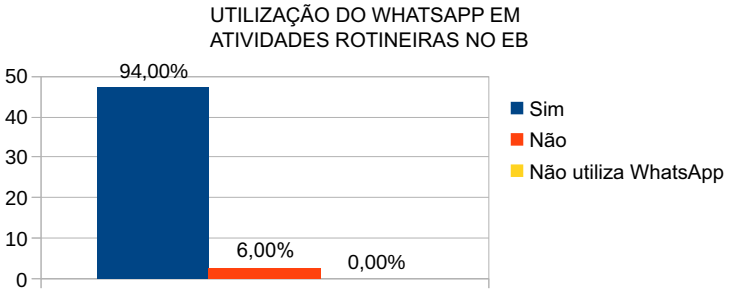
FIGURA 2 – Rastreamento de unidades móveis no *software* Pacificador.

Fonte: BRASIL, 2016.

O *WhatsApp Messenger* é o aplicativo utilizado com maior frequência e é o mais comum entre todos os usuários. No Exército não é diferente. A facilidade de envio de mensagens de texto, voz e, mais recentemente, vídeos e arquivos, torna cada vez mais prático seu emprego em situações diversas, desde trâmites de informações cotidianas até conteúdos com maior complexidade, como, por exemplo, o acionamento de um plano de chamada. Em ambos os casos, a possibilidade da confirmação do recebimento da mensagem pelo receptor, proporciona confiabilidade no processo de fluxo de informação.

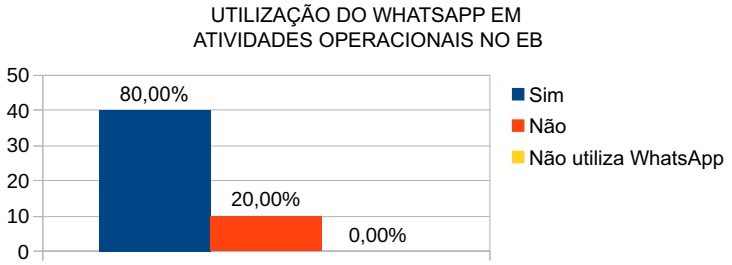
A pesquisa apontou o elevado uso de *smartphones* por militares do EB, verificou-se que 100% da amostra utiliza-os, o mesmo ocorrendo com o aplicativo *WhatsApp Messenger*. O uso do *WhatsApp Messenger* em atividades rotineiras de trabalho ocorre com 94% da amostra e 80% em atividades operacionais do EB, como podem ser vistos nos gráficos 2 e 3. Tais dados mostram que há elevada disseminação do uso dessas ferramentas entre o público considerado.

GRÁFICO 2 – Utilização do *WhatsApp Messenger* em atividades rotineiras no EB.



Fonte: o autor.

GRÁFICO 3 – Utilização do *WhatsApp Messenger* em atividades operacionais no EB.



Fonte: o autor.

Figura 3 – Página para *download* do EBChat no *Google Play*.

Fonte: Google Play, 2017.

4 VANTAGENS, DESVANTAGENS E LIMITAÇÕES DO USO

A maior vantagem do uso de telefones celulares e *smartphones* é a flexibilidade, especialmente relacionada à mobilidade para comunicação em voz e/ou dados.

A área de cobertura para o uso do celular deve ser considerada para que haja efetivamente comunicação. Para isso é necessário haver disponibilidade de sinal de um provedor de telefonia móvel. Tal sinal é gerado em Estações Rádio-Base (ERB). As ERB geram o sinal em determinado raio ao redor de sua antena, tal raio é chamado de célula de cobertura. A união de várias células forma a chamada área de cobertura.

A disponibilidade de áreas de cobertura para o uso de telefonia celular nos centros urbanos é maior que nas zonas rurais. Dessa forma, pode-se inferir que o emprego de celular em localidades com pouca ou nenhuma cobertura de operadoras torna-se limitado ou mesmo inexistente.

Já para os *smartphones,* o conceito de área de cobertura está em evolução, principalmente pela possibilidade de manter a maior parcela de suas funcionalidades, independente de serem abrangidos pelas células de cobertura das operadoras, seja de voz ou dados (2G, 3G ou 4G), desde que esteja em uma área de cobertura de uma rede sem fio *Wi-Fi*, ou seja, em uma localidade com disponibilidade de internet fixa e um ponto de acesso *Wi-Fi* (*access point,* roteador sem fio, entre outros), é possível o uso dos *smartphones.*

O uso de *smartphone* como meio de propagação de conteúdos de comunicação social proporciona alcance global para usuários que estejam dispostos a baixar o aplicativo. Ademais possui a possibilidade de instalação de aplicativos como o *WhatsApp Messenger* e o EB*Chat* para transmissão de voz, textos, imagens e vídeos em tempo próximo ao real e com baixo custo (basicamente o de aquisição do *smartphone* e da disponibilidade de *internet* para o aparelho acessá-la).

A desvantagem identificada é que o Exército não possui o domínio das chaves criptográficas de aplicativos como o *WhatsApp Messenger*, o que não o garante a confidencialidade, apesar de o aplicativo afirmar que é seguro.

A limitação do emprego dos celulares está na necessidade de cobertura de sinal de telefonia móvel, o que o torna mais adequado para áreas urbanas, pois há maior quantidade de ERB, por consequência, maior disponibilidade de sinal.

5 CONCLUSÃO

Conclui-se que houve amplo crescimento do emprego do telefone celular no Exército Brasileiro desde o ano de 2006, quando propunha-se o seu uso em operações de garantia da lei e da ordem até os dias atuais, especialmente com o uso de *smartphones* com aplicações como o *WhatsApp Messenger*.

O uso de *smartphones* está amplamente difundido entre os militares do Exército Brasileiro e esses utilizam-os tanto em atividades rotineiras de trabalho quanto em operações militares. Tais militares utilizam o *WhatsApp Messenger* como meio de comunicação, o que apresenta flexibilidade, mobilidade e rapidez, entretanto não é conhecida a criptografia empregada. Por essa razão, foi criado um aplicativo semelhante, com criptografia própria, o EBChat.

Conclui-se, ainda, que a limitação dos celulares e *smartphones* está na necessidade de cobertura de sinal de telefonia, e no caso dos últimos, de sinal de *internet,* seja de operadoras de telefonia móvel, seja por *Wi-Fi*. Dessa forma, o emprego em áreas urbanas é mais eficiente devido à maior disponibilidade de cobertura.

RESUMEN

El uso de la tecnología celular por militares del Ejército Brasileño ha crecido en la última década. El empleo del celular no es restringido a la voz, especialmente después de la creación de los smartphones, ganando nuevas posibilidades como difusión de comunicación social,

transmisión de mensajes de texto, voz, fotos y videos en aplicaciones como WhatsApp Menseger, Aplicación del Ejército Brasileño y EBChat. Sin embargo, el uso de esa tecnología todavía es limitada por la necesidad de infraestructura de antenas para proveer disponibilidad de señal. Así su uso es más eficaz en zonas urbanas en razón de la cobertura más amplia.

Palabras-clave: tecnologia celular, Ejército Brasileño, aplicaciones.

REFERÊNCIAS

BARROS, Thiago. O que é smartphone e para que serve? **Artigo para sítio TechTudo.** Disponível em: < http://www.techtudo.com.br/artigos/noticia/2011/12/o-que-e-smartphone-e-para-que-serve.html >. 3 jan. 2012. Acesso em: 2 maio 2017.

BRASIL. Exército Brasileiro. **Sistema Pacificador garantiu segurança e defesa dos Jogos Rio 2016.** Brasília, 2016.Disponível em: <http://www.eb.mil.br/web/midia-impressa/noticiario-do-exercito/-/asset_publisher/IZ4bX6gegOtX/content/sistema-pacificador-garantiu-seguranca-e-defesa-dos-jogos-rio-2016 >. Acesso em: 2 maio 2017.

_____. _____. **Aplicativo do Exército Brasileiro**. Brasília, 2017. Disponível em: < http://www.eb.mil.br/aplicativos-mobile >. Acesso em: 8 maio 2017.

GOOGLE PLAY. **Página para download do EBChat no Google Play.** Disponível em: <aplicativo GOOGLE PLAY para smartphone Android>. Acesso em: 29 maio 2017.

LOPES, Cristiano Gomes e VAS, Braz Batista. **O ensino de história na palma da mão:** o whatsapp como ferramenta pedagógica para além da sala de aula. Simpósio Internacional de Educação a Distância. 2016. p. 2. Disponível em: < http://www.sied-enped2016.ead.ufscar.br/ojs/index.php/2016/article/view/1519 >. Acesso em: 8 maio 2017.

SILVA, Walbery Nogueira de Lima e. **O emprego da telefonia celular na transmissão de dados em operações urbanas de GLO**. EsAO, 2006.

O autor é graduado em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) e em Administração pela Universidade de Pernambuco (UPE). Pós-graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO), em Administração Financeira pela Universidade de Pernambuco (UPE), em Gestão de Sistemas Táticos de Comando e Controle pela Escola de Comunicações (EsCom) e em Guerra Eletrônica pelo Centro de Instrução de Guerra Eletrônica (CIGE). Atualmente, mestrando em Economia de Defesa pela Universidade de Brasília (UnB). É instrutor da Escola de Comunicações e pode ser contactado pelo email washington.rodrigues@eb.mil.br.

O SISTEMA DE GERENCIAMENTO DE CONTEÚDO JOOMLA

JAVAN DE OLIVEIRA CRUZ
Pós-graduado, lato sensu,em Operações Militares

RESUMO: Com o avanço da *internet* e a constante busca de informações em seu ambiente, há a necessidade de que os conteúdos nela disponibilizados estejam sempre atualizados, com informações relevantes sendo apresentadas aos leitores em tempo real. Empresas e instituições necessitam de *websites* que divulguem suas informações de forma atrativa e amigável, garantindo novas visitas, surgindo então a necessidade de gerir seus conteúdos de forma segura e eficaz. Assim, foram criados os Sistemas de Gerenciamento de Conteúdo, que são aplicações que fornecem uma plataforma capaz de gerenciar e publicar desde as páginas dos *websites* a produtos de uma loja *online.* O *Joomla* é um dos principais sistemas que cumprem esta finalidade, possuindo uma crescente comunidade de usuários mundialmente.

Palavras-chave: internet, conteúdo, gerenciamento, joomla.

1 INTRODUÇÃO

Atualmente, a *Internet* é um meio onde a informação pode ser divulgada com grande facilidade. Conteúdos sendo atualizados rapidamente e preços relativamente baixos, são atrativos para que empresas, instituições ou mesmo pessoas busquem ter o seu espaço no ambiente da *web.* Porém, nem todas as páginas que encontramos possuem informações atualizadas, além de não serem concebidas de modo que facilitem o acesso aos conteúdos mais relevantes nelas encontrados. Embora seja fácil construir um *website,* com ferramentas disponíveis sendo cada vez mais intuitivas, a concepção e manutenção de um *website* continua sendo uma tarefa trabalhosa e por muitas vezes complexa, sendo que nem sempre a eficiência pretendida é alcançada.

Conceitos com os utilizados em *blogs* surgiram para facilitar a atualização de conteúdos, que permitem que pessoas que possuem pouco conhecimento técnico na área de informática publiquem e atualizem informações em tempo real. Apesar de apresentarem uma estrutura linear, exibindo mensagens em ordem cronológica, os *blogs* tem como principal característica a facilidade para a sua atualização, por meio de qualquer computador ligado à *internet.* Porém, quando voltamos nossas atenções para instituições ou entidades que queiram distribuir conteúdos com regularidade, as demandas são maiores do que as capacidades fornecidas por um simples *blog.* Para atender a estas necessidades, é possível visualizar uma página sendo constituída não por um *blog,* mas por um conjunto de *blogs,* responsável por agrupar conteúdos categorizados por temas e que nem sempre serão agrupados de forma cronológica, possuindo ainda áreas de acesso restrito à apenas determinados usuários, de acordo com perfis preestabelecidos. A criação de um sistema com estas características que foram apresentadas pode ser uma tarefa complicada, porém existem soluções que tornam esta tarefa algo muito mais simples, não exigindo que os seus desenvolvedores sejam programadores ou técnicos especializados. A ferramenta utilizada para tal é o Sistema de Gerenciamento de Conteúdo (*Content Management System* – CMS).

2 DESENVOLVIMENTO

Um Sistema de Gerenciamento de Conteúdo é um aplicativo que deve ser utilizado para a criação, edição, gerenciamento e publicação de conteúdos de um *website,* possuindo características como flexibilidade, organização e eficiência.

Estes sistemas possuem uma área pública, que pode ser consultada pelos usuários que navegam pela *web,* o *site* propriamente dito, com características visuais e com o conteúdo que se deseja divulgar, conhecida como *Frontend,* bem como uma área restrita aos administradores, responsáveis por gerenciar o conteúdo a ser exposto, chamada de *Backend.*

Empresas com grandes capacidades financeiras ou que possuem técnicos da área de informática especializados em desenvolvimento optam, normalmente, pela construção de sistemas de gerenciamento de conteúdos proprietários, que permitam gerir as informações que produzem e pretendem disponibilizar na *Internet.* Essas soluções podem ser feitas de acordo com as demandas, ou adaptadas às necessidades efetivas da empresa ou instituição.

Porém, existem *softwares* disponibilizados gratuitamente, que permitem a gestão de conteúdos com grande eficiência e eficácia. Entre os projetos mais conhecidos de *software* para gestão de conteúdos encontra-se o *Wordpress,* o *Drupal,* o *Mambo3,* entre outros. Em Agosto de 2005, após uma ruptura dentro da equipe de desenvolvimento do *Mambo* e a empresa *Miro,* detentora dos direitos sobre o *Mambo,* surgiu um produto com um novo nome, porém com a mesma filosofia de funcionamento. Trata-se do *Joomla!*

O *Joomla* pode ser considerado, atualmente, o

CMS mais completo e complexo do mercado. A criação de *sites* em *Joomla* possibilita fazer praticamente tudo o que se deseja, desde a construção de simples *blogs* à implementação de portais com grande quantidade de informações. O *Joomla* é desenvolvido na linguagem PHP, sendo mantido por uma enorme comunidade de *webmasters,* dando continuidade à evolução do sistema.

É um dos CMS mais customizáveis existentes. Sua versão inicial do Joomla, conta com diversas funcionalidades dificilmente encontradas em outros gerenciadores de conteúdo. Permite a instalação de componentes, *plugins,* módulos, múltiplos idiomas, entre outras possibilidades, permitindo a divulgação de conteúdos de forma consistente e personalizável.

3 CONCLUSÃO

Com a grande necessidade de instituições e de pessoas divulgarem seus trabalhos e conteúdos, aliada a usuários que navegam pela *internet,* ávidos por informações, os Sistemas de Gerenciamento de Conteúdo surgem como uma solução de grande relevância. O *Joomla* é um CMS destacado, com ferramentas que permitem a gestão de conteúdos de forma competente, com grande personalização visual para a divulgação das informações, sendo produtivo para os administradores e atrativo aos usuários.

THE CONTENT MANAGEMENT SYSTEM JOOMLA

ABSTRACT

With the advancement of the internet and the constant search for information in its environment, there is a need for the contents made available to it to be always updated, with relevant information being presented to the readers in real time. Companies and institutions need websites that make their information attractive and friendly, guaranteeing new visits, and the need to manage their content in a safe and effective way. Thus, Content Management Systems were created, which are applications that provide a platform capable of managing and publishing from the pages of the websites to products of an online store. Joomla is one of the leading systems that serve this purpose, with a growing community of users worldwide.

Keywords: internet; content. management. Joomla

REFERÊNCIAS

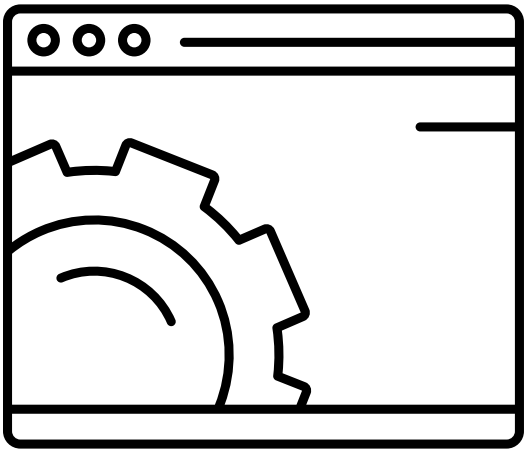
WIKIPEDIA, **Joomla**. Disponível em: <https://pt.wikipedia.org/wiki/Joomla>. Acesso em: 10 abr. 2017.

Estratégia Digital, **CMS:** para que serve um sistema de gestão de conteúdos?. Disponível em: <http://www.estrategiadigital.pt/cms/>. Acesso em: 12 abr. 2017.

Navega Bem, Joomla! O mais poderoso sistema de CMS. Disponível em: <https://www.navegabem.pt/joomla-o-mais-poderoso-sistema-de-cms.html>. Acesso em: 10 maio 2017.

Slideshare, **Joomla, o que é? Para que serve?**. Disponível em: <https://pt.slideshare.net/bullmkt/joomla-o-que-para-que-serve>. Acesso em: 10 maio 2017.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN), pós-graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO). Major da Arma de Comunicações do Exército Brasileiro, concluiu com aproveitamento o curso de Manutenção de Comunicações da Escola de Comunicações (EsCom). Possui os cursos de Programação em PHP com MySQL orientado a objetos, curso de ITIL V3 *Foundation* e o curso de Cobit 4.1. Atualmente, encontra-se cursando graduação em Análise e Desenvolvimento de Sistemas pela UNIGRAN. É instrutor na Escola de Comunicações e pode ser contactado pelo email cruz.javan@eb.mil.br.



License Type | Free for commercial use with attribution license

PREVIEW	DESCRIPTION	LICENSOR´S AUTHOR
	Content Management	Madebyoliver
	Cloud Computing	Freepik
	Footprint	Freepik
	Data	Freepik
	Mining	Smartline
	Management	Freepik
	Management	Freepik
	Search	Cole Bemis
	Internet	Made by Made
	Cloud Locked Symbol	Freepik
	Cell phone	Freepik
	Broken Zone	Freepik
	Fingerprint	Vectors Market
	Smartphone	Madebyoliver
	Smartphone	Madebyoliver
	Cloud Computing	Madebyoliver
	Spy	Made by Dondoni

Icons made by Freepik, Retinaicons, Gregor Cresnar from www.flaticon.com

ESCOM

Endereço: Estrada Parque do Contorno, Rodovia DF - 001, KM 5
Setor Habitacional Taquari - Lago Norte - Brasília - DF
CEP: 71559-902
Telefone: (0xx61) 3415-3000
(PABX) 3415-3131 (Voz/Fax)
Sitio: www.escom.ensino.eb.br